

Cisco Catalyst SD-WAN Command Reference

First Published: 2023-08-22

Last Modified: 2026-10-09

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

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

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

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

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

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

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

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

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

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

© 2019–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **CLI Configuration Commands** 3

CLI Operational Commands 3

CLI Overview 3

CHAPTER 3 **Configuration Commands** 15

Overview of Configuration Commands 23

aaa 24

aaa netconf-accounting 27

access-list 28

access-list 30

accounting-interval 31

acct-req-attr 32

action 34

action 48

address-family 50

address-pool 53

admin-auth-order 54

admin-state 55

admin-tech-on-failure 56

advertise 57

age-time 58

alarms 59

allow-local-exit 60

allow-same-site-tunnels 61

allow-service 63
api-key 65
app-probe-class 66
app-route-policy 67
app-visibility 69
applications 71
apply-policy 72
archive 75
area 77
arp 79
arp-timeout 80
auth-fail-vlan 81
auth-fallback 82
auth-order 84
auth-order 85
auth-reject-vlan 87
auth-req-attr 88
authentication 90
authentication-type 91
authentication-type 92
auto-cost reference-bandwidth 94
auto-sig-tunnel-probing 95
auto-rp 95
autonegotiate 96
bandwidth-downstream 97
bandwidth-upstream 99
banner login 101
banner motd 102
best-path 103
bfd app-route 105
bfd color 106
bfd app-route color 109
bgp 110
bind 112

block-icmp-error 113
block-non-source-ip 114
bridge 115
capability-negotiate 117
carrier 118
cellular 119
cflowd-template 121
channel 122
channel-bandwidth 124
cipher-suite 125
class-map 127
clear-dont-fragment 128
clock 129
cloud-qos 130
cloud-qos-service-side 132
cloudexpress 135
collector 136
color 137
community 139
compatible rfc1583 140
connections-limit 142
console-baud-rate 143
contact 144
container 145
control 145
control-connections 146
control-direction 147
control-policy 148
control-session-pps 149
controller-group-id 150
controller-group-list 151
controller-send-path-limit 152
cost 153
country 154

cpu-usage 156
crypto pki trustpoint 157
crypto pki authenticate 158
crypto pki enroll 160
crypto pki import 161
custom-eflow 162
das 163
data-policy 165
data-security 168
dead-interval 170
dead-peer-detection 171
default-action 172
default-information originate 175
default-vlan 176
description 178
device-groups 179
dhcp-helper 179
dhcp-server 181
dialer down-with-vInterface 182
direction 183
discard-rejected 184
disk-speed 185
disk-usage 186
distance 188
dns 189
domain-id 190
dot1x 191
duplex 195
ebgp-multihop 196
ecmp-hash-key 197
ecmp-limit 198
eco-friendly-mode 199
eigrp 200
elephant-flow 201

encapsulation 202
exclude 205
exclude-controller-group-list 207
flow-active-timeout 208
flow-control 209
flow-inactive-timeout 210
flow-sampling-interval 211
flow-visibility 212
gps-location 213
graceful-restart 214
group 215
group 217
group 218
guard-interval 219
guest-vlan 220
hello-interval 221
hello-interval 223
hello-interval 224
hello-tolerance 225
hold-time 227
host 228
host-mode 229
host-name 230
host-policer-pps 231
icmp-error-pps 232
icmp-redirect-disable 233
idle-timeout 234
igmp 235
ike 236
implicit-acl-logging 238
interface 239
interface 243
interface 246
interface 247

interface 248
interface 250
interface gre 251
interface ipsec 252
interface irb 255
interface ppp 256
integrity-type 258
ip address 259
ip address-list 260
ip dhcp-client 262
ip gre-route 264
ip ipsec-route 265
ip route 267
ip secondary-address 269
ipsec 270
ipsec 271
iptables-enable 272
ipv6 address 272
ipv6 dhcp-client 274
ipv6 route 275
join-group 277
join-prune-interval 278
keepalive 279
last-resort-circuit 281
lease-time 282
lists 283
local-interface-list 292
location 293
location 295
log-frequency 295
log-translations 297
logging disk 298
logging host 303
logging tls-profile 305

logging server 305
logs 308
low-bandwidth-link 309
mac-accounting 310
mac-address 311
mac-authentication-bypass 312
match 313
match 314
match 316
max-clients 328
max-control-connections 329
max-controllers 331
max-leases 331
max-macs 332
max-metric 333
max-omp-sessions 334
memory-usage 336
mgmt-security 337
mode 338
mtu 339
multicast-buffer-percent 340
multicast-replicator 341
name 342
name 343
nas-identifier 344
nas-ip-address 345
nat 346
nat-refresh-interval 348
natpool 349
neighbor 350
network 351
next-hop-self 352
node-type 353
nssa 354

ntp 356
offer-time 359
omp 360
on-demand enable 361
on-demand idle-timeout 361
options 362
organization-name 364
orgid 364
ospf 365
ospfv3 authentication 367
overlay-as 368
overload 369
parameter-map type umbrella global 371
parent 371
passive-interface 372
password 373
peer 374
perfect-forward-secrecy 376
pim 377
pmtu 378
policer 379
policy 382
policy ipv6 388
port-forward 390
port-hop 391
port-offset 393
port-scan 394
ppp 395
pppoe-client 397
priority 398
probe 399
probe-path branch 401
probe-path gateway 402
profile 403

profile 405
propagate-aspath 406
propagate-community 407
radius 407
radius-servers 411
range 414
reauthentication 415
redistribute 416
redistribute leaked routes 418
refresh 418
rekey 419
rekey 421
remote-as 422
replay-window 422
replay-window 423
replicator-selection 424
respond-to-ping 425
retransmit-interval 426
rewrite-rule 427
route-consistency-check 429
route-export 430
route-import 431
route-import-service (for route leak) 431
route-map 432
route-policy 433
router 435
router-id 437
router-id 438
secret 439
security 440
send-community 440
send-ext-community 441
send-path-limit 442
sense level 443

service 445
service-insertion appnav-controller-group appqoe 448
service-insertion service-node-group appqoe 449
set ip next-hop verify-availability 450
shaping-rate 451
shutdown 452
site-id 454
sla-class 455
snmp 456
sp-organization-name 457
speed 458
spt-threshold 459
ssid 460
static 462
static-ingress-qos 464
static-lease 465
stub 466
system 467
system-ip 470
system-tunnel-mtu 472
system patch-confirm 473
table-map 474
tacacs 474
tcp-mss-adjust 477
tcp-optimization 479
tcp-optimization-enabled 479
tcp-syn-flood-limit 480
tcp-timeout 481
technology 483
template-refresh 484
timeout inactivity 485
timer 486
tracker-dns-cache-timeout 488
timers 489

timers 490
timers 492
tloc-extension 494
tloc-extension-gre-from 496
tloc-extension-gre-to 497
track 499
track-default-gateway 500
track-interface-tag 501
track-list 503
track-transport 504
tracker 505
trap group 507
trap target 509
tunnel-destination 511
tunnel-destination 512
tunnel-interface 513
tunnel-source 514
tunnel-source 515
tunnel-source-interface 517
tunnel-source-interface 518
tunnel vrf multiplexing 519
udp-timeout 519
update-source 520
upgrade-confirm 521
usb-controller 523
user 524
user 525
usergroup 527
vbond 529
vbond-as-stun-server 532
view 533
vlan 535
vmanage-connection-preference 536
vpn 537

vpn-membership 541
vrrp 542
wake-on-lan 546
wlan 547
wpa-personal-key 549
zone 550
zone-based-policy 551
zone-pair 553
zone-to-nozone-internet 555

CHAPTER 4 **Operational Commands** 557
Overview of Operational Commands 565
clear aaa login 567
clear app cflowd flow-all 567
clear app cflowd flows 568
clear app cflowd statistics 570
clear app dpi all 570
clear app dpi apps 571
clear app dpi flows 573
clear app log flow-all 574
clear app log flows 575
clear arp 577
clear bfd transitions 578
clear bgp all 579
clear bgp neighbor 579
clear bridge mac 580
clear bridge statistics 581
clear cellular errors 581
clear cellular session statistics 582
clear cloudexpress computations 583
clear cloudinit data 584
clear control connections 584
clear control connections-history 585
clear control port-index 586

clear crash 586
clear dhcp server-bindings 587
clear dhcp state 588
clear dns cache 589
clear dot1x client 590
clear history 591
clear igmp interface 591
clear igmp protocol 592
clear igmp statistics 592
clear installed-certificates 593
clear interface statistics 595
clear ip leak routes vpn 596
clear ip mfib record 596
clear ip mfib stats 597
clear ip nat filter 597
clear ip nat statistics 598
clear ipv6 dhcp state 599
clear ipv6 neighbor 600
clear ipv6 policy 601
clear omp all 601
clear omp peer 602
clear omp routes 604
clear omp tlocs 604
clear orchestrator connections-history 605
clear ospf all 606
clear ospf database 607
clear pim interface 607
clear pim neighbor 608
clear pim protocol 609
clear pim rp-mapping 610
clear pim statistics 611
clear policer statistics 612
clear policy 613
clear policy zbfw filter-statistics 613

clear policy zbfw global-statistics 614
clear policy zbfw sessions 614
clear pppoe statistics 615
clear reverse-proxy context 616
clear system statistics 618
clear tunnel statistics 620
clear wlan radius-stats 620
clock 621
commit 622
complete-on-space 623
config 623
controller-mode 624
debug 625
debug packet-trace condition 632
debug platform condition mpls match-inner 633
debug-vdaemon 634
debug vdaemon peer 635
exit 636
file list 637
file show 637
help 638
history 639
idle-timeout 639
job stop 640
logout 641
monitor event-trace sdwan 641
monitor start 643
monitor stop 643
nslookup 644
paginate 645
ping 646
poweroff 648
prompt1 649
prompt2 651

quit 652
reboot 652
request aaa unlock-user 654
request admin-tech 655
request certificate 658
request container image install 659
request container image remove 660
request control-tunnel add 660
request control-tunnel delete 661
request controller add serial-num 661
request controller delete serial-num 662
request controller-upload serial-file 663
request csr upload 664
request daemon ncs restart 665
request device 665
request device-upload 666
request download 668
request execute 669
request firmware upgrade 670
request interface-reset 670
request ipsec ike-rekey 671
request ipsec ipsec-rekey 672
request nms all 672
request nms application-server 674
request nms cluster diagnostics 677
request nms cluster-orchestrator 679
request nms configuration-db 681
request nms coordination-server 683
request nms messaging-server 684
request nms olap-db 686
request nms statistics-db 687
request nms server-proxy 690
request nms server-proxy set ratelimit 691
request on-vbond-controller 692

request on-vbond-vsmart 692
request platform software sdwan bootstrap-config save 692
request port-hop 693
request reset configuration 694
request reset logs 697
request sla-dampening-reset color 698
request root-ca-crl 699
request root-cert-chain 700
request security ipsec-rekey 700
request software activate 701
request software install 702
request software install-image 704
request software remove 705
request software reset 706
request software secure-boot 707
request software set-default 708
request software upgrade-confirm 708
request software verify-image 710
request stream capture 711
request upload 712
request vedge 712
request vedge-cloud activate 713
request vsmart add serial-num 714
request vsmart delete serial-num 714
request vsmart-upload serial-file 715
screen-length 716
screen-width 716
set platform software trace 717
show aaa usergroup 718
show alarms 720
show app cflowd collector 722
show app cflowd flow-count 723
show app cflowd flows 724
show app cflowd statistics 726

show app cflowd template 727
show app dpi applications 728
show app dpi flows 729
show app dpi summary statistics 731
show app dpi supported-applications 732
show app log flow-count 738
show app log flows 739
show app tcp-opt 741
show app-route sla-class 742
show app-route stats 744
show arp 746
show bfd history 747
show bfd sessions 748
show bfd summary 750
show bfd tloc-summary-list 751
show bgp neighbor 753
show bgp routes 755
show bgp summary 758
show boot-partition 759
show bridge interface 760
show bridge mac 761
show bridge table 762
show cellular modem 763
show cellular network 764
show cellular profiles 765
show cellular radio 766
show cellular sessions 767
show cellular status 768
show certificate installed 769
show certificate reverse-proxy 771
show certificate root-ca-cert 772
show certificate root-ca-crl 774
show certificate serial 775
show certificate signing-request 776

show certificate validity 777
show cli 778
show clock 779
show cloudexpress applications 780
show cloudexpress gateway-exits 781
show cloudexpress local-exits 782
show configuration commit list 783
show container images 784
show container instances 785
show control affinity config 786
show control affinity status 787
show control connection-info 788
show control connections 788
show control connections-history 791
show control local-properties 794
show control statistics 799
show control summary 800
show control valid-vedges 801
show control valid-vsmarts 802
show crash 803
show crypto pki trustpoints status 804
show devices 805
show dhcp interface 806
show dhcp server 807
show dot1x clients 808
show dot1x interfaces 809
show dot1x radius 810
show hardware alarms 812
show hardware environment 813
show hardware inventory 816
show hardware poe 817
show hardware real time information 818
show hardware temperature-thresholds 820
show history 821

show igmp groups 822
show igmp interface 823
show igmp statistics 824
show igmp summary 826
show interface 827
show interface arp-stats 833
show interface description 835
show interface errors 836
show interface packet-sizes 840
show interface port-stats 841
show interface queue 843
show interface sfp detail 844
show interface sfp diagnostic 849
show interface statistics 851
show ip dns-snoop 853
show ip fib 854
show ip mfib oil 859
show ip mfib stats 860
show ip mfib summary 861
show ip nat filter 862
show ip nat interface 863
show ip nat interface-statistics 864
show ip routes 865
show ipsec ike inbound-connections 868
show ipsec ike outbound-connections 870
show ipsec ike sessions 872
show ipsec inbound-connections 873
show ipsec local-sa 874
show ipsec outbound-connections 875
show ipv6 dhcp interface 877
show ipv6 fib 878
show ipv6 interface 879
show ipv6 neighbor 882
show ipv6 policy access-list-associations 882

show ipv6 policy access-list-counters 883
show ipv6 policy access-list-names 884
show ipv6 policy access-list-policers 885
show ipv6 routes 885
show jobs 887
show licenses 888
show log 890
show logging 891
show logging process 892
show logging profile sdwan 893
show monitor event-trace sdwan 896
show multicast replicator 897
show multicast rpf 899
show multicast topology 900
show multicast tunnel 901
show nms-server running 902
show notification stream 903
show ntp associations 904
show ntp peer 905
show omp cloudexpress 906
show omp multicast-auto-discover 907
show omp multicast-routes 909
show omp peers 910
show omp routes 914
show omp services 919
show omp summary 921
show omp tlocs 924
show omp verify-routes 928
show orchestrator connections 930
show orchestrator connections-history 932
show orchestrator local-properties 935
show orchestrator reverse-proxy-mapping 937
show orchestrator statistics 937
show orchestrator summary 939

show orchestrator valid-vedges 940
show orchestrator valid-vmanage-id 941
show orchestrator valid-vsmarts 942
show ospf database 943
show ospf database-summary 944
show ospf interface 945
show ospf neighbor 947
show ospf process 948
show ospf routes 950
show packet-capture 952
show packet-trace 953
show parser dump 955
show pim interface 956
show pim neighbor 957
show pim rp-mapping 958
show pim statistics 959
show platform resources 960
show platform software trace level 961
show policer 963
show policy access-list-associations 964
show policy access-list-counters 965
show policy access-list-names 966
show policy access-list-policers 967
show policy data-policy-filter 968
show policy ef-stats 970
show policy from-vsmart 971
show policy service-path 973
show policy tunnel-path 974
show policy zbfw filter-statistics 975
show policy zbfw global-statistics 976
show policy zbfw sessions 980
show ppp interface 981
show pppoe session 981
show pppoe statistics 982

show reboot history 983
show running-config 984
show sdwan 987
show sdwan alarms detail 988
show sdwan alarms summary 989
show sdwan appqoe 990
show sdwan appqoe flow closed 994
show sdwan appqoe flow flow-id 995
show sdwan appqoe flow vpn-id 997
show sdwan cloudexpress applications 997
show sdwan cloudexpress gateway-exits 998
show sdwan cloudexpress local-exits 999
show sdwan cloudexpress service-area-applications 1000
show sdwan policy 1001
show sdwan policy service-path 1002
show sdwan policy tunnel-path 1004
show security-info 1005
show nms server-proxy ratelimit 1006
show software 1006
show support omp peer 1007
show system buffer-pool-status 1011
show system netfilter 1012
show system on-demand 1013
show system statistics 1015
show system status 1019
show tech-support 1023
show tenant-mapping 1025
show tenant omp peers 1026
show tenant omp routes 1027
show tenant-summary 1028
show transport connection 1029
show tunnel gre-keepalives 1030
show tunnel inbound-connections 1031
show tunnel local-sa 1032

show tunnel statistics 1033
show umbrella deviceid 1034
show uptime 1035
show users 1036
show version 1036
show vrrp 1037
show wlan clients 1038
show wlan interfaces 1039
show wlan radios 1040
show wlan radius 1042
show ztp entries 1043
tcpdump 1044
test policy match control-policy 1045
timestamp 1048
tools ip-route 1048
tools iperf 1049
tools minicom 1051
tools netstat 1052
tools nping 1054
tools ss 1062
tools stun-client 1064
traceroute 1066
vshell 1068

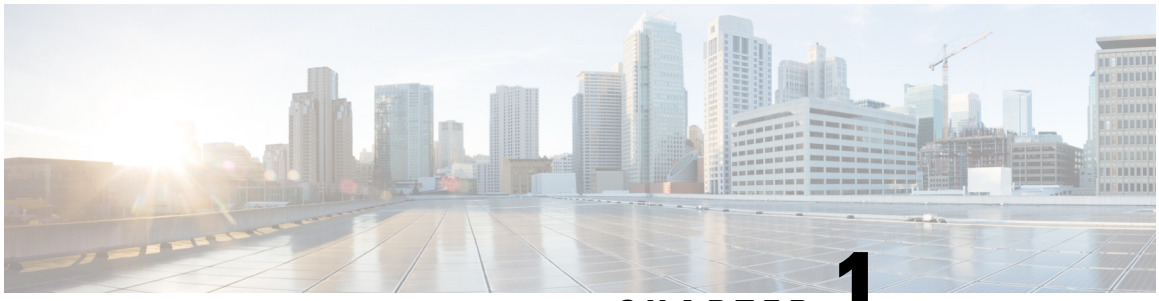
CHAPTER 5 **Configuration Management Commands** 1071
Overview of Configuration Management Commands 1072
abort 1072
clear 1073
commit 1074
describe 1075
do 1076
end 1077
exit 1077
help 1078

load 1079
no 1080
pwd 1081
revert 1082
rollback 1082
save 1084
show configuration 1086
show configuration commit 1087
show configuration diff 1088
show configuration merge 1089
show configuration rollback 1090
show configuration running 1091
show full-configuration 1092
show history 1092
show parser dump 1093
top 1094
validate 1095

CHAPTER 6 **Command Filters for CLI Operational Commands** 1097

Overview of Command Filters for CLI Operational Commands 1098
append 1099
begin 1100
best-effort 1101
context-match 1101
count 1102
de-select 1103
details 1104
display xml 1106
exclude 1107
include 1108
linnum 1109
match-all 1109
match-any 1110
more 1111

nomore 1112
notab 1113
repeat 1114
save 1114
select 1115
sort-by 1116
tab 1117
until 1118



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
- User Documentation for Cisco SD-WAN Release 20

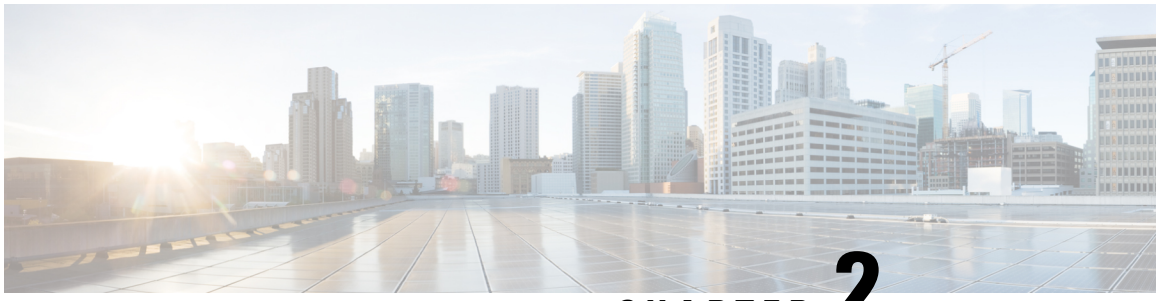
Communications, Services, and Additional Information

- 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

CLI Configuration Commands

Use the CLI configuration commands to modify and then activate a device's configuration parameters.

To enter configuration mode, type the **config** command in operational mode. All changes to the device's configuration are made to a copy of the active configuration, called a candidate configuration. These changes do not take effect until you issue a successful **commit** or **commit confirm** command.

- CLI Operational Commands, on page 3
- CLI Overview, on page 3

CLI Operational Commands

Use the CLI operational commands to view system status, monitor and troubleshoot a Cisco vEdge device and network connectivity, initiate configuration mode, and control the CLI environment. When you first enter the CLI, you are in operational mode.

CLI Overview

The CLI on the Cisco vEdge devices is one of the ways you can configure and monitor these devices. The CLI provides various commands for configuring and monitoring the software, hardware, and network connectivity of the vSmart controllers and the vEdge routers. The CLI provides the following features:

- Displaying help about CLI commands
- Completing partial commands
- Editing the command line with keyboard sequences
- Configuring CLI session settings
- Filtering command output
- Adding comments to device configurations
- Activating and deactivating parts of a configuration
- Displaying CLI messages

The Cisco SD-WAN CLI design is based on the YANG data modeling language, defined in RFC 6020.

CLI Modes

The CLI has two modes:

- Operational mode, for monitoring the state of the Cisco vEdge device. When you log in to the CLI, you are in operational mode. In this mode, you view device status, monitor and troubleshoot the device and network connectivity, enter into configuration mode, and control the CLI session parameters.
- Configuration mode, for changing the operational parameters of the Cisco vEdge device. You enter configuration mode by issuing the configure command in operational mode. This mode has a number of submodes for manipulating different parts of the configuration. For example, the mode interface-eth1 allows you to configure parameters for Ethernet interface 1. All changes to the device's configuration are done to a copy of the active configuration, called a candidate configuration. Configuration changes take effect only when you enter a commit or commit confirmed command and that command is successful.

Start the CLI

Before you begin, make sure the vSmart controller and the vEdge router hardware is set up and the Cisco SD-WAN software is installed. You must have a direct console connection to the device or network using SSH. If your device is not set up, follow the installation instructions provided to you with the vSmart controller or the vEdge router before proceeding.

The login prompt for a Cisco vEdge device shows the software version and then prompts for a username and password.

When you log into a vSmart controller or a vEdge router, you are prompted to enter your user name and password. Once you enter your password, you are automatically placed at the CLI prompt.

For security reasons, each time you log out of the device, the CLI session ends and you are required to log in again to access the CLI.

CLI Prompts

The prompt indicates the mode the CLI is in:

- *host-name#*: The host name followed by a hash mark indicates that the CLI is in operational mode. An operational mode prompt is similar to vsmart#.
- *host-name*(config)#: When the CLI is in configuration mode, the string config is added to the prompt. For example, a configuration mode prompt is similar to vsmart(config)#. If you are configuring a lower hierarchy in the commands, the prompt also indicates that level. For example, if you are configuring Ethernet interface 1 for a VPN, in the hierarchy vpn > interface, the configuration mode prompt is vsmart(config-interface-eth1)#. The CLI prompt shows only the parent hierarchy, not the full path to the command, so that the CLI prompt never gets too long.

To change the operational mode prompt, use the **prompt1** operational command:

```
vsmart# prompt1 eve@vsmart#
eve@vsmart#
```

To change the configuration mode prompt, use the **prompt2** operational command:

```
vsmart# prompt2 eve@vsmart(config)#
eve@vsmart(config)#
```

Configure CLI Session Settings

The following are the default CLI session settings for a Linux terminal:

```
vsmart# show cli
autowizard            false
complete-on-space     false
history               100
idle-timeout          1800
ignore-leading-space  true
output-file           terminal
paginate              true
prompt1               \h\M#
prompt2               \h(\m)#
screen-length         30
screen-width          80
service prompt config true
show-defaults         false
terminal              xterm-256color
timestamp             disable
```

To change the session values, use the command names listed in the output above. For more information on the commands, see Operational Commands .

Command Hierarchies

CLI commands are organized in a hierarchy that groups commands that perform related or similar functions. For example, in operational mode, commands that display information about OMP are collected under the **show omp** command hierarchy. In configuration mode, commands that configure OMP properties are collected under the **omp** command hierarchy.

Display Help about CLI Commands

To list the available CLI commands, along with a short description of the command, type a **?** (question mark).

If you type **?** at the prompt, the CLI displays a list of available commands. In operational mode, you see:

```
vsmart# ?
Possible completions:
  autowizard          Automatically query for mandatory elements

  clear               Clear parameter

  clock               System clock

  commit              Confirm a pending commit

  complete-on-space   Enable/disable completion on space

  config              Manipulate software configuration information

  debug               Debugging commands

  exit                Exit the management session

  file                Perform file operations

  help                Provide help information

  history             Configure history size

  idle-timeout        Configure idle timeout

  job                 Job operations

  leaf-prompting      Automatically query for leaf values
```

```
  logout              Logout a user
  monitor             Monitor a file
  no                  Negate a command or set its defaults
  nslookup            Look up a DNS name
  paginate            Paginate output from CLI commands
  ping                Ping a host
  poweroff            Shut down the system
  prompt1             Set operational mode prompt
  prompt2             Set configure mode prompt
  quit                Exit the management session
  reboot              Reboot the system
  request             Perform an action
  screen-length       Configure screen length
  screen-width        Set CLI screen width
  show                Show information about the system
  tcpdump             Perform tcpdump on a network interface
  timestamp           Enable/disable the display of timestamp
  tools               Tools commands
  traceroute          Trace connectivity to a host
  vdig                Asynchronous FQDN resolution
  vping               Send L2, L3, L7 probes to remote host
  vshell              System shell
```

If you type tools and **?** at the prompt, the CLI displays a list of available commands for tools. In operational mode, you see:

```
vm9# tools ?

Possible completions:

  consent-token   Access restricted functionality using Consent Token
  core-state      Show Core state
  cpu-util        Show CPU Utilization
  flood-ping      Flood-ping a host
  ike-debug       IKE debug tools
  internal        (TESTBED) Internal commands
  ip-route        Display route table
```

```
  iperf           Network bandwidth measurement tool
  netstat         Display network status
  nping           Network packet generation tool
  ss              Display network statistics
  stun-client     STUN client protocol tool
  support         Support commands
  vtysh           Integrated shell for Quagga routing software suite
```



Note To access **vtysh** commands, see *Quagga docs* on the Quagga Routing website.

If you type **?** at the prompt after entering configuration mode, you see:

```
vsmart(config)# ?
Possible completions:
  apply-policy   Apply network policy
  banner         Set banners
  omp            OMP information
  policy         Configure policy
  security       Configure security
  snmp           Configure SNMP
  system         Configure System
  vpn            VPN Instance
  ---
  abort          Abort configuration session
  clear          Remove all configuration changes
  commit         Commit current set of changes
  describe       Display transparent command information
  do             Run an operational-mode command
  end            Terminate configuration session
  exit           Exit from current mode
  help           Provide help information
  load           Load configuration from an ASCII file
  no             Negate a command or set its defaults
  pwd            Display current mode path
  revert         Copy configuration from running
  rollback       Roll back database to last committed version
  save           Save configuration to an ASCII file
  show           Show a parameter
  top            Exit to top level and optionally run command
  validate       Validate current configuration
```

If you type **?** after a command name, the CLI shows all possible completions for that command. For example:

```
vsmart# show interface vpn 0 ?
Possible completions:
  eth0  eth1  |  <>
```

If you type **help** before a command name, it will you give you more information about the command. For example:

```
vsmart# help show cli
Help for command: show cli
    Display cli settings
```

The **show parser dump** command also displays information about available commands and their syntax.

Enter User-Defined Strings

For many configuration commands, you define a string that identifies an instance of a configurable object. For example, when you create user accounts, you configure a user-defined string for the username:

```
vEdge(config-system)# aaa user eve
```

In this command, the strings "aaa" and "user" are Cisco SD-WAN software keywords, and the string "eve" is a user-defined string.

User-defined strings can include all uppercase and lowercase letters, all digits, spaces, and all special characters except for angle brackets (< and >).

To include a space or an exclamation point (!) in a user-defined string, either type a backslash (\) before the space or enclose the entire string in quotation marks (" "). For example:

```
vEdge(config)# banner login "Remember to log out when you are done!"
vEdge(config-banner)# show full-configuration
banner
 login "Remember to log out when you are done!"
!
vEdge(config-banner)#

vEdge(config-system)# organization-name My\ Company
vEdge(config-system)# show configuration
system
 organization-name "My Company"
!
vEdge(config-system)#
```

Complete Partial Commands and Strings

The CLI provides command completion. It recognizes commands and options based on the first few letters you type so that you do not always have to remember or type the full command or option name.

To display a list of all possible command or option completions, type the partial command followed immediately by a question mark. For example:

```
vsmart@# s?
Possible completions:
  screen-length        Configure screen length
  screen-width         Set CLI screen width
  show                 Show information about the system
```

To complete a command or option that you have partially typed, press the tab key after you have typed a partially completed command name. If the partially typed letters begin a string that uniquely identifies a command, the complete command name is displayed. Otherwise, a list of possible completions is displayed.

Command completion also works with other strings, such as filenames, directory names, interface names, and usernames.

To enable command completion when you press the space bar, enable it for the duration of the terminal session:

```
vEdge# complete-on-space true
```

When this is enabled, you can press the tab key or the space bar to complete a partially typed command name or variable string.

Command completion is disabled within quoted strings. So if an argument contains spaces and you quote them with a backslash (for example, **prefix-list my\ list**) or with quotation marks (for example, **prefix-list "my list"**), you cannot use command completion. Space completion does not work with filenames.

Edit the Command Line with Keyboard Sequences

You can use keyboard sequences in the CLI to move around and edit text on the command line itself. You can also use keyboard sequences to scroll through a list of recently executed commands. The following table lists some of the CLI keyboard sequences.

Table 1:

Category	Action	Keyboard Sequence
Move the cursor	Move the cursor back one character.	Ctrl-B or Left Arrow
	Move the cursor back one word.	Esc-B or Alt-B
	Move the cursor forward one character.	Ctrl-F or Right Arrow
	Move the cursor forward one word.	Esc-F or Alt-F
	Move the cursor to the beginning of the command line.	Ctrl-A or Home
	Move the cursor to the end of the command line.	Ctrl-E or End
Delete characters	Delete the character before the cursor.	Ctrl-H, Delete, or Backspace
	Delete the character following the cursor.	Ctrl-D
	Delete all characters from the cursor to the end of the line.	Ctrl-K
	Delete the whole line.	Ctrl-U or Ctrl-X
	Delete the word before the cursor.	Ctrl-W, Esc-Backspace, or Alt-Backspace
	Delete the word after the cursor.	Esc-D or Alt-D
Insert recently deleted text	Insert the most recently deleted text at the cursor.	Ctrl-Y
Display previous command lines	Scroll backward through the list of recently executed commands.	Ctrl-P or Up Arrow
	Scroll forward through the list of recently executed commands.	Ctrl-N or Down Arrow
	Search the command history in reverse order.	Ctrl-R
	Show list.	
Capitalization	Capitalize the word at the cursor; that is, make the first character uppercase and the rest of the word lowercase.	Esc-C

Category	Action	Keyboard Sequence
	Change the word at the cursor to all lowercase.	Esc-l
Special cases	Cancel a command; that is, clear a line.	Ctrl-C
	Quote insert character; that is, do not treat the next keystroke as an edit command.	Ctrl-V/Esc-Q
	Redraw the screen.	Ctrl-l
	Transpose characters.	Ctrl-T
	Enter multiline values when prompted for a value in the CLI (not available when editing a CLI command).	Esc-M
	Exit configuration mode.	Ctrl-Z

Filter Command Output

You can filter the output from a command by adding the pipe (|) symbol at the end of the command, followed by one of the filtering commands listed in the following table. You can chain together a series of filters on a single command line.

Table 2:

Filter	Description
append *filename*	Append output text to a file.
begin *regular-expression*	Begin with the line that matches a regular expression.
best-effort	Display data even if the data provider is unavailable, or continue loading from a file even if failures are occurring.
count	Count the number of lines in the output.
csv	Display the outfield fields in a comma-separated format.
display	Display the output as XML.
exclude *regular-expression*	Exclude lines that match a regular expression.
include *regular-expression*	Include lines that match a regular expression.
linnum	Enumerate lines in the output.
match-all	All selected filters must match.
match-any	At least one selected filter must match.
more	Paginate the output.
nomore	Suppress pagination of the output.

Filter	Description
notab	Display each output field on a separate line instead of in a table.
repeat *seconds*	Execute the command repeatedly, every specified number of seconds.
save *filename*	Save the output to a file.
select	For tabular output, select the columns to display.
tab	Enforce the table output of fields.
until *regular-expression*	End the display with the line that matches a regular expression.

Use Regular Expressions

The regular expressions available for use in filtering commands are a subset of those used in the UNIX **egrep** command and in the AWK programming language. The following table lists some common operators.

Table 3:

Operator	Action
.	Match any character.
^	Match the beginning of a string.
$	Match the end of a string.
[abc...]	Character class, which matches any of the characters abc... Character ranges are specified by a pair of characters separated by a -.
[^abc...]	Negated character class, which matches any character except abc.
r1 | r2	Alternation. It matches either r1 or r2.
r1r2	Concatenation. It matches r1 and then r2.
r+	Match one or more *r*s.
r*	Match zero or more *r*s.
r?	Match zero or one *r*s.
(r)	Grouping. It matches *r*.

Understand CLI Messages

The CLI displays messages at various times, such as when you enter and exit configuration mode, commit a configuration, and type a command or value that is not valid.

When you type an invalid command or value, a CLI message indicates the nature of the error:

```
vsmart# show c
Possible completions:
  certificate     Display installed certificate properties
```

```
  cli             Display cli settings
  clock           System clock
  configuration   Display configuration history
  control         Display Control Information
```

When you commit a configuration, the CLI first validates the configuration. If there is a problem, the CLI indicates the nature of the problem:

```
Entering configuration mode terminal
vsmart(config)# no vpn 0
vsmart(config)# commit
Aborted: 'vpn' : Cannot delete vpn 0
vsmart(config>)#
```

Count the Number of Lines in Command Output

To count the number of lines in the output from a command, use the **count** filtering command. For example:

```
vsmart# show interface | count
Count: 17 lines
```

Display Line Numbers in Command Output

To display line numbers in the output, use the **linnum** command filter. For example:

```
vsmart# show interface | linnum
1: interface vpn 0 interface eth0
2:  ip-address      10.0.1.12/24
3:  if-admin-status Up
4:  if-oper-status  Up
5:  encap-type      null
6:  mtu             1500
7:  hwaddr          00:50:56:00:01:02
8:  speed-mbps      1000
9:  duplex          full
10:  rx-packets      3035
11:  tx-packets      1949
12: interface vpn 0 interface eth1
13:  if-admin-status Down
14:  if-oper-status  Down
15:  hwaddr          00:0c:29:81:00:17
16:  rx-packets      0
17:  tx-packets      0
```

Search for a String in Command Output

To have the command output include only lines matching a regular expression, use the **include** command filter. For example:

```
vsmart# show cli | include screen
screen-length         30
screen-width          80
```

To have the command output include only the lines not containing a regular expression, use the **exclude** filtering command. For example:

```
vsmart# show cli | exclude e
history               100
prompt1               \h\M#
prompt2               \h\(m)#
```

To display the output starting at the first match of a regular expression, use the **begin** command filter. For example:

```
vsmart# show cli | begin show
show-defaults         false
terminal              linux
timestamp             disable
```

To end the command output when a line matches a regular expression, use the **until** command filter. For example:

```
vsmart# show cli | until history
autowizard            false
complete-on-space     true
history               100
```

Save Command Output to a File

To save command output to a file, use the **save** *filename* or **append** *filename* command filter. For example:

```
vsmart# show running-config omp | save filename
```

To save the configuration except for any passwords, add the **exclude password** command filter:

```
vsmart# show running-config system | exclude password | save filename
```

Configure a Device from the CLI

To configure a vSmart controller or vEdge router directly from the device, enter configuration mode:

```
vsmart# config
```

Then type either the full configuration command or type one command at a time to move down through the command hierarchy. Here is an example of typing a full configuration command:

```
vsmart(config)# vpn 1 interface ge0/1 ip address 1.1.1.1/16
```

Here is an example of moving down the command hierarchy by typing one command at a time:

```
vsmart(config)# vpn1
vsmart(config-vpn-1)# interface eth1
vsmart(config-interface-eth1)# ip address 1.1.1.1/16
vsmart(config-interface-eth1)#
```

To move to another portion of the hierarchy, simply type the name of the top-level command. For example:

```
vsmart(config-interface-eth1)# policy
vsmart(config-policy)#
```

To look at the configuration changes:

```
vsmart(config-policy)# top show configuration
vpn 1
 interface eth1
  ip address 1.1.1.1/16
  shutdown
 !
!
```

To commit the changes:

```
vsmart(config-policy)# commit
Commit complete.
```

Add Comments in a Configuration

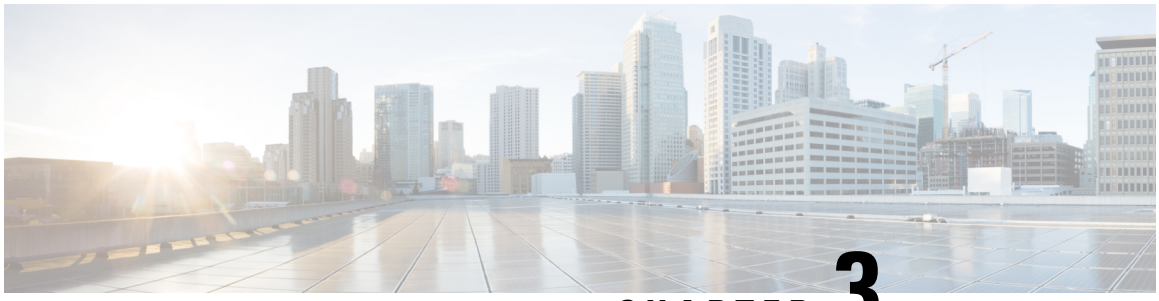
All characters following an exclamation point (!) character up to the next newline in a configuration are ignored. This allows you to include comments in a file containing CLI commands and then paste the file into

the CLI. To enter the ! character as an argument or to include it in a password, prefix it with a backslash (\) or place it inside quotation marks (" ").

Delete Commands from a Configuration

Use the **no** command to delete commands from a configuration. For example:

```
vsmart(config)# do show running-config
vpn 1
 interface eth1
  ip address 1.1.1.1/16
  auto-negotiation
  shudown
  no proxy-arp
 !
!
vsmart(config)# no vpn 1 interface eth1 ip address
vsmart(config)# commit
commit complete.
vsmart(config)# do show running-config
vpn 1
 interface eth1
  auto-negotiation
  shudown
  no proxy-arp
 !
!
```



CHAPTER 3

Configuration Commands

Note For a list of Cisco IOS XE SD-WAN commands qualified for use in Cisco vManage CLI templates, see List of Commands Qualified in Cisco IOS XE Release 17.x. For information about specific commands, see the appropriate chapter in Cisco IOS XE SD-WAN Qualified Command Reference Guide.

- Overview of Configuration Commands, on page 23
- aaa, on page 24
- aaa netconf-accounting, on page 27
- access-list, on page 28
- access-list, on page 30
- accounting-interval, on page 31
- acct-req-attr, on page 32
- action, on page 34
- action, on page 48
- address-family, on page 50
- address-pool, on page 53
- admin-auth-order, on page 54
- admin-state, on page 55
- admin-tech-on-failure, on page 56
- advertise, on page 57
- age-time, on page 58
- alarms, on page 59
- allow-local-exit, on page 60
- allow-same-site-tunnels, on page 61
- allow-service, on page 63
- api-key, on page 65
- app-probe-class, on page 66
- app-route-policy, on page 67
- app-visibility, on page 69
- applications, on page 71
- apply-policy, on page 72
- archive, on page 75

- area, on page 77
- arp, on page 79
- arp-timeout, on page 80
- auth-fail-vlan, on page 81
- auth-fallback, on page 82
- auth-order, on page 84
- auth-order, on page 85
- auth-reject-vlan, on page 87
- auth-req-attr, on page 88
- authentication, on page 90
- authentication-type, on page 91
- authentication-type, on page 92
- auto-cost reference-bandwidth, on page 94
- auto-sig-tunnel-probing, on page 95
- auto-rp, on page 95
- autonegotiate, on page 96
- bandwidth-downstream, on page 97
- bandwidth-upstream, on page 99
- banner login, on page 101
- banner motd, on page 102
- best-path, on page 103
- bfd app-route, on page 105
- bfd color, on page 106
- bfd app-route color, on page 109
- bgp, on page 110
- bind, on page 112
- block-icmp-error, on page 113
- block-non-source-ip, on page 114
- bridge, on page 115
- capability-negotiate, on page 117
- carrier, on page 118
- cellular, on page 119
- cflowd-template, on page 121
- channel, on page 122
- channel-bandwidth, on page 124
- cipher-suite, on page 125
- class-map, on page 127
- clear-dont-fragment, on page 128
- clock, on page 129
- cloud-qos, on page 130
- cloud-qos-service-side, on page 132
- cloudexpress, on page 135
- collector, on page 136
- color, on page 137
- community, on page 139
- compatible rfc1583, on page 140

- connections-limit, on page 142
- console-baud-rate, on page 143
- contact, on page 144
- container, on page 145
- control, on page 145
- control-connections, on page 146
- control-direction, on page 147
- control-policy, on page 148
- control-session-pps, on page 149
- controller-group-id, on page 150
- controller-group-list, on page 151
- controller-send-path-limit, on page 152
- cost, on page 153
- country, on page 154
- cpu-usage, on page 156
- crypto pki trustpoint, on page 157
- crypto pki authenticate, on page 158
- crypto pki enroll, on page 160
- crypto pki import, on page 161
- custom-eflow, on page 162
- das, on page 163
- data-policy, on page 165
- data-security, on page 168
- dead-interval, on page 170
- dead-peer-detection, on page 171
- default-action, on page 172
- default-information originate, on page 175
- default-vlan, on page 176
- description, on page 178
- device-groups, on page 179
- dhcp-helper, on page 179
- dhcp-server, on page 181
- dialer down-with-vInterface, on page 182
- direction, on page 183
- discard-rejected, on page 184
- disk-speed, on page 185
- disk-usage, on page 186
- distance, on page 188
- dns, on page 189
- domain-id, on page 190
- dot1x, on page 191
- duplex, on page 195
- ebgp-multihop, on page 196
- ecmp-hash-key, on page 197
- ecmp-limit, on page 198
- eco-friendly-mode, on page 199

- eigrp, on page 200
- elephant-flow, on page 201
- encapsulation, on page 202
- exclude, on page 205
- exclude-controller-group-list, on page 207
- flow-active-timeout, on page 208
- flow-control, on page 209
- flow-inactive-timeout, on page 210
- flow-sampling-interval, on page 211
- flow-visibility, on page 212
- gps-location, on page 213
- graceful-restart, on page 214
- group, on page 215
- group, on page 217
- group, on page 218
- guard-interval, on page 219
- guest-vlan, on page 220
- hello-interval, on page 221
- hello-interval, on page 223
- hello-interval, on page 224
- hello-tolerance, on page 225
- hold-time, on page 227
- host, on page 228
- host-mode, on page 229
- host-name, on page 230
- host-policer-pps, on page 231
- icmp-error-pps, on page 232
- icmp-redirect-disable, on page 233
- idle-timeout, on page 234
- igmp, on page 235
- ike, on page 236
- implicit-acl-logging, on page 238
- interface, on page 239
- interface, on page 243
- interface, on page 246
- interface, on page 247
- interface, on page 248
- interface, on page 250
- interface gre, on page 251
- interface ipsec, on page 252
- interface irb, on page 255
- interface ppp, on page 256
- integrity-type, on page 258
- ip address, on page 259
- ip address-list, on page 260
- ip dhcp-client, on page 262

- ip gre-route, on page 264
- ip ipsec-route, on page 265
- ip route, on page 267
- ip secondary-address, on page 269
- ipsec, on page 270
- ipsec, on page 271
- iptables-enable, on page 272
- ipv6 address, on page 272
- ipv6 dhcp-client, on page 274
- ipv6 route, on page 275
- join-group, on page 277
- join-prune-interval, on page 278
- keepalive, on page 279
- last-resort-circuit, on page 281
- lease-time, on page 282
- lists, on page 283
- local-interface-list, on page 292
- location, on page 293
- location, on page 295
- log-frequency, on page 295
- log-translations, on page 297
- logging disk, on page 298
- logging host, on page 303
- logging tls-profile, on page 305
- logging server, on page 305
- logs, on page 308
- low-bandwidth-link, on page 309
- mac-accounting, on page 310
- mac-address, on page 311
- mac-authentication-bypass, on page 312
- match, on page 313
- match, on page 314
- match, on page 316
- max-clients, on page 328
- max-control-connections, on page 329
- max-controllers, on page 331
- max-leases, on page 331
- max-macs, on page 332
- max-metric, on page 333
- max-omp-sessions, on page 334
- memory-usage, on page 336
- mgmt-security, on page 337
- mode, on page 338
- mtu, on page 339
- multicast-buffer-percent, on page 340
- multicast-replicator, on page 341

- name, on page 342
- name, on page 343
- nas-identifier, on page 344
- nas-ip-address, on page 345
- nat, on page 346
- nat-refresh-interval, on page 348
- natpool, on page 349
- neighbor, on page 350
- network, on page 351
- next-hop-self, on page 352
- node-type, on page 353
- nssa, on page 354
- ntp, on page 356
- offer-time, on page 359
- omp, on page 360
- on-demand enable, on page 361
- on-demand idle-timeout, on page 361
- options, on page 362
- organization-name, on page 364
- orgid, on page 364
- ospf, on page 365
- ospfv3 authentication, on page 367
- overlay-as, on page 368
- overload, on page 369
- parameter-map type umbrella global, on page 371
- parent, on page 371
- passive-interface, on page 372
- password, on page 373
- peer, on page 374
- perfect-forward-secrecy, on page 376
- pim, on page 377
- pmtu, on page 378
- policer, on page 379
- policy, on page 382
- policy ipv6, on page 388
- port-forward, on page 390
- port-hop, on page 391
- port-offset, on page 393
- port-scan, on page 394
- ppp, on page 395
- pppoe-client, on page 397
- priority, on page 398
- probe, on page 399
- probe-path branch, on page 401
- probe-path gateway, on page 402
- profile, on page 403

- profile, on page 405
- propagate-aspath, on page 406
- propagate-community, on page 407
- radius, on page 407
- radius-servers, on page 411
- range, on page 414
- reauthentication, on page 415
- redistribute, on page 416
- redistribute leaked routes, on page 418
- refresh, on page 418
- rekey, on page 419
- rekey, on page 421
- remote-as, on page 422
- replay-window, on page 422
- replay-window, on page 423
- replicator-selection, on page 424
- respond-to-ping, on page 425
- retransmit-interval, on page 426
- rewrite-rule, on page 427
- route-consistency-check, on page 429
- route-export, on page 430
- route-import, on page 431
- route-import-service (for route leak), on page 431
- route-map, on page 432
- route-policy, on page 433
- router, on page 435
- router-id, on page 437
- router-id, on page 438
- secret, on page 439
- security, on page 440
- send-community, on page 440
- send-ext-community, on page 441
- send-path-limit, on page 442
- sense level, on page 443
- service, on page 445
- service-insertion appnav-controller-group appqoe, on page 448
- **service-insertion service-node-group** appqoe, on page 449
- set ip next-hop verify-availability, on page 450
- shaping-rate, on page 451
- shutdown, on page 452
- site-id, on page 454
- sla-class, on page 455
- snmp, on page 456
- sp-organization-name, on page 457
- speed, on page 458
- spt-threshold, on page 459

- ssid, on page 460
- static, on page 462
- static-ingress-qos, on page 464
- static-lease, on page 465
- stub, on page 466
- system, on page 467
- system-ip, on page 470
- system-tunnel-mtu, on page 472
- **system patch-confirm**, on page 473
- table-map, on page 474
- tacacs, on page 474
- tcp-mss-adjust, on page 477
- tcp-optimization, on page 479
- tcp-optimization-enabled, on page 479
- tcp-syn-flood-limit, on page 480
- tcp-timeout, on page 481
- technology, on page 483
- template-refresh, on page 484
- timeout inactivity, on page 485
- timer, on page 486
- tracker-dns-cache-timeout, on page 488
- timers, on page 489
- timers, on page 490
- timers, on page 492
- tloc-extension, on page 494
- tloc-extension-gre-from, on page 496
- tloc-extension-gre-to, on page 497
- track, on page 499
- track-default-gateway, on page 500
- track-interface-tag, on page 501
- track-list, on page 503
- track-transport, on page 504
- tracker, on page 505
- trap group, on page 507
- trap target, on page 509
- tunnel-destination, on page 511
- tunnel-destination, on page 512
- tunnel-interface, on page 513
- tunnel-source, on page 514
- tunnel-source, on page 515
- tunnel-source-interface, on page 517
- tunnel-source-interface, on page 518
- tunnel vrf multiplexing, on page 519
- udp-timeout, on page 519
- update-source, on page 520
- upgrade-confirm, on page 521

- usb-controller, on page 523
- user, on page 524
- user, on page 525
- usergroup, on page 527
- vbond, on page 529
- vbond-as-stun-server, on page 532
- view, on page 533
- vlan, on page 535
- vmanage-connection-preference, on page 536
- vpn, on page 537
- vpn-membership, on page 541
- vrrp, on page 542
- wake-on-lan, on page 546
- wlan, on page 547
- wpa-personal-key, on page 549
- zone, on page 550
- zone-based-policy, on page 551
- zone-pair, on page 553
- zone-to-nozone-internet, on page 555

Overview of Configuration Commands

The configuration command reference pages describe the CLI commands that you use to configure the functional network properties of vSmart controllers, vEdge devices, and vBond orchestrators. To configure a Cisco vEdge device, enter configuration mode by issuing the **config** command from operational mode in the CLI. You know that you are in configuration mode because the CLI prompt changes to include the string **(config)**.

In the CLI, configuration commands are organized into functional hierarchies. The top-level configuration hierarchies are:

- apply-policy—Apply control policy and data policy.
- banner—Set login messages for the device.
- bridge—Configure Layer 2 bridging for a rvEdge route.
- omp—Configure properties for the Viptela Overlay Management Protocol.
- policy—Configure control policy and data policy.
- security—Configure IPsec parameters.
- snmp—Configure SNMP parameters.
- system—Configure basic system parameters.
- vpn—Configure the properties of a VPN, including the interfaces that participate in the VPN and the routing protocols that are enabled in the VPN.

To manage a configuration session, use the Configuration Session Management Commands.

aaa

To configure role-based access to a device using authentication, authorization, and accounting use the system aaa command in privileged EXEC mode.

vManage Feature Template

Configuration > **Templates** > **AAA**



Note You can only configure the password-policy commands using the device CLI template on Cisco SD-WAN Manager.

Command Hierarchy

```
system
  aaa
    [no] accounting
    admin-auth-order
    auth-fallback
    auth-order (local | radius | tacacs)
    logs
      [no] audit-disable
      [no] netconf-disable
    password-policy min-password-length length
    password-policy num-lower-case-characters number-of-lower-case-characters
    password-policy num-numeric-characters number-of-numeric-characters
    password-policy num-special-characters number-of-special-characters
    password-policy num-upper-case-characters number-of-upper-case-characters

    radius-servers tag
    user username
      group group-name
      password password

    task name
      config
        default action {accept | deny}
        accept "xpath"
        deny "xpath
      oper-exec
        default action {accept | deny}
        accept "command"
        deny "command

    usergroup group-name
      task {interface | policy | routing | security | system | authorization_task} {read |
 write}
```

]

Syntax Description

password-policy min-password-length *length*	The minimum allowed length of a password. You can specify between 8 to 32 characters.

password-policy num-lower-case-characters *number-of-lower-case-characters*	The minimum number of lower case characters. You can specify between 1 to 128 characters.
password-policy num-numeric-characters *number-of-numeric-characters*	The minimum number of numeric characters. You can specify between 1 to 128 characters.
password-policy num-special-characters *number-of-special-characters*	The minimum number of special characters. You can specify between 1 to 128 characters.
password-policy num-upper-case-characters *number-of-upper-case-characters*	The minimum number of upper case characters. You can specify between 1 to 128 characters.
task "*name*"	The name of an authorization task.
accept "*xpath*"	The XPath string for a configuration command that the authorization feature allows a user to execute.
deny "*xpath*"	The XPath string for a configuration command that the authorization feature does not allow a user to execute.
accept "*command*"	An operational command that the authorization feature allows a user to execute.
deny "*command*"	An operational command that the authorization feature does not allow a user to execute.
task *authorization_task*	The name of a configured authorization task.

Command History

Release	Modification
Cisco SD-WAN Release 14.1	Command introduced.
Cisco SD-WAN Release 20.4.1	`password-policy` commands introduced.
Cisco SD-WAN Release 20.5.1	`accounting` command introduced. `task` commands introduced. `authorization_task` argument introduced.

The following example shows to set up a user, their password, and group using the `system aaa` command:

```
Device# config
Entering configuration mode terminal
Device(config)# system aaa
Device(config-aaa)# user eve
Device(config-user-eve)# password 123456
Device(config-user-eve)# group operator
```

```
Device(config-user-eve)# exit
vEdge(config-aaa)# commit and-quit
Commit complete.
```

The following example shows how to enable accounting using the `system aaa` command:

```
Device# config
Entering configuration mode terminal
Device(config)# system aaa
Device(config-aaa)# accounting
Device(config-aaa)# exit
vEdge(config-aaa)# commit and-quit
Commit complete.
```

The following example shows how to configure and authorization task using the `system aaa` command and how to associate the task with a user group:

```
Device# config
Entering configuration mode terminal
Device(config)# system aaa
Device(config-aaa)# task task1
Device(config-task-task1)# config default-action deny
Device(config-config)# accept "/vpn/"
Device(config-accept-/vpn/)# exit
Device(config-config)# exit
Device(config-task-task1)# oper-exec default-action accept
Device(config-oper-exec)# deny "show system"
Device(config-deny-show system)# deny "request admin-tech"
Device(config-deny-request admin-tech)# exit
Device(config-oper-exec)# exit
Device(config-task-task1)# exit
Device(config-aaa)# usergroup group1
Device(config-usergroup-group1)# task task1 read write
Device(config-usergroup-group1)# commit
Commit complete.
```

The following example shows how to verify your AAA configuration:

```
vEdge# show running-config system aaa
system
 aaa
  auth-order local radius
  task task1
   oper-exec
    default-action accept
    deny "show system"
  !
    deny "request admin-tech"
  !
   config
    default-action accept
    accept /vpn/
  !
  usergroup basic
   task system read write
   task interface read
  !
  usergroup group1
   task task1 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
  !
 !
!
```

Operational Commands

```
show aaa usergroup

show users

request aaa unlock-user
```

Related Topics

dot1x, on page 191
radius, on page 407
tacacs, on page 474

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)#
```

access-list

Configure or apply an IPv6 access list (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

Create an Access List

```
policy ipv6
  access-list acl-name
    default-action action
    sequence number
```

```
      match
        class class-name
        destination-port number
        next-header protocol
        packet-length number
        plp (high | low)
        source-port number
        tcp flag
        traffic-class value
      action
        drop
        count counter-name
        log
        accept
          class class-name
          policer policer-name
          set traffic-class value
```

Apply an Access List

```
vpn vpn-id
  interface interface-name
    ipv6 access-list acl-name (in | out)
```

Syntax Description

acl-name	Access List Name: Name of the access list to configure or to apply to the interface. acl-name can be up to 32 characters long. The number of acl-name entries is limited to 4096.
(**in** |**out**	Direction in which to Apply Access List: 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 History

Release	Modification
16.3	Command introduced.
26.2.1	The number of acl-name entries limited to 4096.

Example

Apply an IPv6 access list to data traffic being recieved on an interface in VPN 1:

```
vpn 1
  interface ge0/4
    ip address fd00:1234:/16
    no shutdown
    access-list acl-filter in
```

Operational Commands

show policy access-list-associations

show policy access-list-counters

show policy access-list-names

Related Topics

access-list, on page 30

access-list

Configure or apply an IPv4 access list (on vEdge routers only).

Command Hierarchy

Create an Access List

```
policy
  access-list acl-name
    default-action action
    sequence number
      match
        class class-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dscp number
        packet-length number
        plp (high | low)
        protocol number
        source-data-prefix-list list-name
        source-ip prefix-length
        source-port number
        tcp flag
      action
        drop
          count counter-name
          log
        accept
          class class-name
          count counter-name
          log
          policer policer-name
          set dscp value
          set next-hop ipv4-address
```

Apply an Access List

```
vpn vpn-id
  interface interface-name
    access-list acl-name (in | out)
```

Syntax Description

acl-name	Access List Name: Name of the access list to configure or to apply to the interface. The number of acl-name entries is limited to 4096.

(**in** |**out**)	Direction in which to Apply Access List: 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 History

Release	Modification
14.1	Command introduced.
26.2.1	The number of acl-name entries limited to 4096..

Example

Apply an access list to an interface in VPN 1:

```
vpn 1
  interface ge0/4
    ip address 10.20.24.15/24
    no shutdown
    access-list acl1 in
```

Operational Commands

show policy access-list-associations

show policy access-list-counters

show policy access-list-names

Related Topics

access-list, on page 28

accounting-interval

How often an 802.1X interfaces sends interim accounting updates to the RADIUS accounting server during an 802.1X session (on vEdge routers only). By default, no interim accounting updates are sent; they are sent only when the 802.1X session ends.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      accounting-interval seconds
```

Syntax Description

seconds	Accounting Update Interval: How often to send 802.1X interim accounting updates to the RADIUS server. Range: 0 through 7200 seconds Default: 0 (no interim accounting updates are sent)

Command History

Release	Modification
16.3	Command introduced.

Example

Send 802.1X interim accounting updates once per hour:

```
vpn 0
  interface ge0/7
    dot1x
      accounting-interval 3600
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

acct-req-attr, on page 32
nas-identifier, on page 344
nas-ip-address, on page 345
radius, on page 407
radius-servers, on page 411

acct-req-attr

Configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS accounting server during an 802.1X session (on vEdge routers only). These AV pairs are defined in RFC 2865, RADIUS, and RFC 2866, RADIUS Accounting, and they are placed in the Attributes field of the RADIUS Accounting Request packet.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      acct-req-attr attribute-number (integer integer | octet octet | string string)
```

Syntax Description

attribute-number	Accounting Attribute Number: RADIUS accounting attribute number. Range: 1 through 64
(**integer***integer* | **octet***octet* | **string**)	Attribute Value: Value of the attribute. Specify the value as an integer, octet, or string, depending on the accounting attribute itself.

Command History

Release	Modification
16.3	Command introduced.

Example

Set the Acct-Authentic attribute to RADIUS:

```
vpn 0
  interface ge0/0
    dot1x
      acct-req-attr 45 integer 1
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

auth-req-attr, on page 88
nas-identifier, on page 344

nas-ip-address, on page 345
radius, on page 407
radius-servers, on page 411

action

Configure the actions to take when the match portion of an IPv4 policy is met (on vEdge routers, Cisco IOS XE Catalyst SD-WAN devices, and vSmart controllers).

vManage Feature Template

For vEdge routers, Cisco IOS XE Catalyst SD-WAN devices, and vSmart controllers:

Configuration ► Policies

Configuration ► Security (for zone-based firewall policy)

Command Hierarchy

For Application-Aware Routing

```
policy
  app-route-policy policy-name
    vpn-list list-name
      default-action sla-class sla-class-name
      sequence number
        action
          backup-sla-preferred-color colors
          count counter-name
          log
          sla-class sla-class-name [strict] [preferred-color colors]
```

For Centralized Control Policy

Configure on vSmart controllers only.

```
policy
  control-policy policy-name
   default-action action
   sequence number
     action
       reject
       accept
         export-to (vpn vpn-id | vpn-list vpn-list)
         set
           omp-tag number
           preference value
           service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
           tloc ip-address color color [encap encapsulation]
           tloc-action action
           tloc-list list-name
```

For Centralized Data Policy

Configure on Cisco IOS XE Catalyst SD-WAN devices and vSmart controllers only.

```
policy
  data-policy policy-name
    vpn-list list-name
      default-action action
      sequence number
```

```
        action
          cflowd (not available for deep packet inspection)
          count counter-name
          drop
          log
          tcp-optimization
          accept
            nat [pool number] [use-vpn 0] (in Releases 16.2 and earlier, not available for
 deep packet inspection)
            redirect-dns (host | ip-address)
            set
              dscp number
              forwarding-class class
              local-tloc color color [encap encapsulation]
              local-tloc-list color color [encap encapsulation] [restrict]
              next-hop ip-address

              policer policer-name
              service service-name local [restrict] [vpn vpn-id]
              service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
              tloc ip-address color color [encap encapsulation]
              tloc-list list-name
              vpn vpn-id
  vpn-membership policy-name
    default-action (accept | reject)
      sequence number
        action (accept | reject)
```

For Cflowd Traffic Flow Monitoring

```
policy
  data-policy policy-name
    vpn-list list-name
      default-action
        (accept | drop)
      sequence number
        action
          accept
            cflowd
```

For Localized Control Policy

Configure on vEdge routers and Cisco IOS XE Catalyst SD-WAN devices only.

```
policy
  route-policy policy-name
    default-action action
    sequence number
      action
        reject
        accept
          set
            aggregator as-number ip-address
            as-path (exclude | prepend) as-numbers
            atomic-aggregate
            community value
            local-preference number
            metric number
            metric-type (type1 | type2)
            next-hop ip-address
                        omp-tag number
            origin (egp | igp | incomplete)
            originator ip-address
            ospf-tag number
            weight number
```

For Localized Data Policy

Configure on vEdge routers and Cisco IOS XE Catalyst SD-WAN devices only.

```
policy
  access-list acl-name
    default-action action
    sequence number
      action
        drop
          count counter-name
          log
        accept
          class class-name
          count counter-name
          log
          policer policer-name
          set dscp value
          set next-hop ipv4-address
```

For Zone-Based Firewall Policy

Configure on vEdge routers and Cisco IOS XE Catalyst SD-WAN devices only.

```
policy
  zone-based-policy policy-name
    default-action action
    sequence number
      action
        drop
        inspect
        log
        pass
```

Syntax Description

default-action sla-class *sla-class-name*	Default Action for Application-Aware Routing: Default SLA to apply if a data packet being evaluated by the policy matches none of the match conditions. If you configure no default action, all data packets are accepted and no SLA is applied to them.
policy control-policy *policy-name* **default-action** (**accept** | **reject**) **policy route-policy** *policy-name* **default-action** (**accept** | **reject**) **policy data-policy** *policy-name* **default-action** (**accept** | **drop**) **policy vpn-membership** *policy-name* **default-action** (**accept** | **drop**) **policy access-list** *acl-name* **default-action** (**accept** | **drop**)	Default Action for Control Policy and Data Policy: Default action to take if an item being evaluated by a policy matches none of the match conditions. If you configure no policy (specifically, if you configure no match–action sequences within a policy), the default action, by default, is to accept all items. If you configure a policy with one or more match–action sequences, the default action, by default, is to either reject or drop the item, depending on the policy type.

default-action (**drop** | **inspect** | **pass**)	Default Action for Zone-Base Firewall Policy: Default action to take if a data traffic flow matches none of the match conditions. drop discards the data traffic. inspect inspects the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. pass allows the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

Syntax Description

For Application-Aware Routing

count *counter-name*	Count of Matching Items Count the packets or bytes that match the application-aware routing policy, saving the information to the specified filename.
log	Log Packets: Place a sampled set of packets that match the SLA class rule into the vsyslog and messages system logging (syslog) files.

sla-class *sla-class-name* [**strict**] **sla-class** *sla-class-name* [**strict**] **preferred-color** *colors***backup-sla-preferred-color** *colors*	Tunnel To Send Data Traffic: Direct data packets that match the parameters in the **match** portion of the **policy app-route-policy** configuration to a tunnel interface that meets the SLA characteristics in the SLA class *sla-class-name*. Configure the SLA class with the **policy sla-class** command. • **sla-class** *sla-class-name*—When you specify an SLA class with no additional parameters, data traffic that matches the SLA is forwarded as long as one tunnel interface is available. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels. • **sla-class** *sla-class-name* **preferred-color** *color*—To set a specific tunnel to use when data traffic matches an SLA class, include the **preferred-color** option, specifying the color of the preferred tunnel. If more than one tunnel matches the SLA, traffic is sent to the preferred tunnel. If a tunnel of the preferred color is not available, traffic is sent through any tunnel that matches the SLA class. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not. The number of preferred-color entries is limited to 32. • **sla-class** *sla-class-name* **preferred-color** *colors*—To set multiple tunnels to use when data traffic matches an SLA class, include the **preferred-color** option, specifying two or more tunnel colors. Traffic is load-balanced across all tunnels. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not. When no tunnel matches the SLA, you can choose how to handle the data traffic: • **strict**—Drop the data traffic. • **backup-sla-preferred-color**—Direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available; if that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more tunnel colors. As with the **preferred-color** option, the backup SLA preferred color is loose matching. The number of backup-sla-preferred-color entries is limited to 32. In a single **action** configuration, you cannot include both the **strict** and **backup-sla-preferred-color** options. In these options, *color* can be one of **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**.

Syntax Description

For Centralized Control Policy

(**accept** | **reject**)	Accept or Reject: By default, all items that match the parameters in the **match** portion of the **policy control-policy** configuration are rejected. Include **reject** to explicitly reject matching items. Include **accept** to accept matching items and to perform any specified actions.
set omp-tag *number*	OMP Tag: Set the tag string that is included in accepted OMP routes.
set preference *number*	Preference Value: Set the preference value that is included in accepted OMP routes. Range: 1 through 256
export-to(**vpn***vpn-id* | **vpn-list***vpn-list*)	Send to VPN: Direct matching routes to the specified VPN or VPN list. You can configure this option only with **match route** match conditions.
service *service-name* (**tloc** *ip-address* | **tloc-list** *list-name*) [**vpn** *vpn-id*]	Service: Direct matching routes to the named service. *service-name* can be **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, and **netsvc4**. The IP address of one TLOC or list of TLOCs identifies the TLOCs to which the traffic should be directed to reach the service. If the list contains multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the vEdge routers that are collocated with the service devices, using the **vpn service** configuration command.

set tloc-action *action*	

TLOC Action:

Direct matching routes or TLOCs using the mechanism specified by *action*, and enable end-to-end tracking of whether the ultimate destination is reachable. Setting a TLOC action is useful when traffic is first directed, via policy, to an intermediate destination, which then forwards the traffic to its ultimate destination. For example, for traffic from vEdge-A destined for vEdge-D, a policy might direct traffic from vEdge-A first to vEdge-B (the intermediate destination), and vEdge-B then sends it to the final destination, vEdge-D.*action* can be one of the following:

• **ecmp**—Equally direct matching control traffic between the intermediate destination and the ultimate destination. In our example, traffic would be sent to vEdge-B (which would then send it to vEdge-D) and directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.

• **primary**—First direct matching traffic to the intermediate destination. If that router is not reachable, then direct it to the final destination. In our example, traffic would first be sent to vEdge-B. If this router is down, it is sent directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the final destination.

• **backup**—First direct matching traffic to the final destination. If that router is not reachable, then direct it to the intermediate destination. In our example, traffic would first be sent directly to vEdge-D. If the vEdge-A is not able to reach vEdge-D, traffic is sent to vEdge-B, which might have an operational path to reach vEdge-D. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination.

• **strict**—Direct matching traffic only to the intermediate destination. In our example, traffic is sent only to vEdge-B, regardless of whether it is reachable. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a **set tloc-action** action in a centralized control policy, **strict** is the default behavior.

Note

- TLOC action is only supported end-to-end if there is a data plane tunnel set up from the same TLOC on the intermediate hop to the source as the TLOC from which the intermediate hop builds the tunnel to the final (ultimate) destination.

  If the TLOC used to reach the intermediate hop from a site is different from the TLOC used from the intermediate hop to reach the final (ultimate) destination, this will result in a policy failure with TLOC action. This is also known as disjoint underlay.

- If the action is **accept set tloc-action**, configure the **service**

	TE on the intermediate destination. Setting the TLOC action option enables the vSmart controller to perform end-to-end tracking of the path to the ultimate destination router. In our example, matching traffic goes from vEdge-A to vEdge-B and then, in a single hop, goes to vEdge-D. If the tunnel between vEdge-B and vEdge-D goes down, the vSmart controller relays this information to vEdge-A, and vEdge-A removes its route to vEdge-D from its local route table. End-to-end tracking works here only because traffic goes from vEdge-B to vEdge-D in a single hop, via a single tunnel. If the traffic from vEdge-A went first to vEdge-B, then to vEdge-C, and finally to vEdge-D, the vSmart controller is unable to perform end-to-end tracking and is thus unable to keep vEdge-A informed about whether full path between it and vEdge-D is up.
set tloc-list *list-name*	TLOC List: Direct matching routes or TLOCs to the TLOC or TLOCs in the named TLOC list . If the list contains multiple TLOCs, the traffic is load-balanced amont them. Changing an OMP route's TLOC is one way to use policy to effect traffic engineering, which directs packets to specific vEdge routers. The color configured in the TLOC list provides a means to separate streams of traffic.

Syntax Description

For Centralized Data Policy

(**accept** | **drop**)	Accept or Drop: By default, all packets that match the parameters in the **match** portion of the **policy data-policy** configuration are dropped. Include **drop** to explicitly reject matching packets. Include **accept** to accept matching packets and to perform any specified actions.
count *counter-name*	Count Packets: Count the packets that match the match criteria, saving the information to the specified filename.
log	Log Packets: Place a sampled set of packets that match the match conditions into the vsyslog and messages system logging (syslog) files.
nat use-vpn 0	NAT Functionality: Direct matching traffic to the NAT functionality so that it can be directed directly to the Internet or other external destination. In Releases 16.2 and earlier, you cannot use NAT with deep packet inspection.

nat fallback	This command attempts to route traffic through an alternate route, typically through a data center route, in the following conditions:
	• The **nat use-vpn 0** command is routing traffic through a NAT direct internet access (DIA) interface.
	• The NAT DIA interface is not available or is inactive.
	Without this command, when the **nat use-vpn 0** command is used and the NAT DIA interface is not available or is inactive, the traffic is dropped.
	Use **nat use-vpn 0** and **nat fallback** with the **match** command to operate when specific criteria are met.
	Example:
	`from-vsmart data-policy service-side-nat-policy`
	`direction from-service`
	`vpn-list vpn-1`
	`sequence 91`
	`match`
	`source-data-prefix-list RFC1918`
	`action accept`
	`nat use-vpn 0`
	`nat fallback`
	`exit`

next-hop *ip-address*	Next-Hop Address: Set the next-hop address in accepted packets.
tcp-optimization	Optimize TCP Traffic: Fine-tune TCP to decrease round-trip latency and improve throughout for TCP traffic.
policer *policer-name*	Policer: Policy the packets using the specified policer.
service *service-name* (**tloc** *ip-address* | **tloc-list** *list-name*) [**vpn** *vpn-id*]	Service: Direct matching packets to the named service. *service-name* can be **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, and **netsvc4**. The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be directed to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the vEdge routers that are collocated with the service devices, using the **vpn service** configuration command.
service *service-name***local** [**restrict**] [**vpn** *vpn-id*]	Service via GRE Tunnel: Direct matching packets to the named service that is reachable via a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the **restrict** option. In the service VPN, you must also advertise the service using the **service** command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).

redirect-dns (*ip-address* | **host**)	Split DNS Server: For a policy that enables split DNS (that is, when the **match** condition specifies **dns-app-list** and **dns**), specify how to direct matching packets. For DNS queries (**dns request**), specify the IP address of the DNS server to use to resolve the DNS query. For DNS responses (**dns response**), specify **host** so that the response from the DNS server is properly forwarded to the requesting service VPN.
set tloc-list *list-name*	TLOC from a List of TLOCs: Direct matching packets to one of the TLOCs is the list defined with a **policy lists tloc-list** list. When the list contains multiple TLOCs that are available and that satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.
set local-tloc color *color* [**encap** *encapsulation*] [**set local-tloc-list color** *color* [**encap***encapsulation*] [**restrict**]	TLOC Identified by Color: Direct matching packets to a TLOC identified by its color and, optionally, 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**. The number of local-tloc-list color entries is limited to 32. By default, *encapsulation* is **ipsec**. It can also be **gre**. By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if the TLOC is unavailable, include the **restrict** option.
set tloc *ip-address* **color** *color* [**encap** *ecapsulation*]	TLOC Identified IP Address and Color: Direct 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**.
set vpn *vpn-id*	VPN: Set the VPN Identifier that is included in accepted packets.

Syntax Description

For Cflowd Traffic Flow Monitoring

(**accept** | **reject**)	Accept or Reject: By default, all items that match the parameters in the **match** portion of the **policy data-policy** configuration are rejected. Include **reject** to explicitly reject matching items. Include **accept** to accept matching items and to perform any specified actions.
cflowd	Enable Packet Collection: Collect packets for traffic monitoring.

Syntax Description

For Localized Control Policy

(**accept** | **reject**)	Accept or Reject: By default, all items that match the parameters in the **match** portion of the **policy control-policy** configuration are rejected. Include **reject** to explicitly reject matching items. Include **accept** to accept matching items and to perform any specified actions.
set aggregator *as-number ip-address*	Aggregator: Set the AS number in which a route aggregator is located and the IP address of the route aggregator. *as-number* can be a value from 1 through 65535.
set as-path (**exclude** | **prepend**) *as-numbers*	AS Path: Exclude or append one or more AS numbers at the beginning of the AS path. Each *as-number* can be a value from 1 through 65535. If you specify more than one AS number, include the numbers in quotation marks.
set atomic-attribute	Atomic Aggregate: Set the BGP atomic aggregate attribute.
set community *value*	Community: Set the BGP community value. It can be *aa*:*nn*, **internal**, **local-as**, **no-advertise**, and **no-export**. In *aa*:*nn*, *aa* is the AS community number and *nn* is a two-byte number.
set local-preference *number*	Local Preference: Set the BGP local preference value. *number* can be a value from 0 through 4294967295.
set metric *number*	Metric: Set the metric. *number* can be a value from 0 through 4294967295.
set metric-type *type*	Metric Type: Set the metric type. *type* can be **type1** or **type2**.
set next-hop *ip-address*	Next-Hop Address: Set the next-hop address.
set omp-tag *number*	OMP Tag Value: Set the OMP tag value. *number* can be a value from 0 through 4294967295.
set origin *origin*	Origin Code: Set the BGP origin code. *origin* can be **egp**, **igp** (default), and **incomplete**.
set originator *ip-address*	Originator: Set the IP address from which the route was learned.

set ospf-tag *number*	OSPF Tag Value: Set the OSPF tag value. *number* can be a value from 0 through 4294967295.
set weight *number*	Weight: Set the BGP weight. *number* can be a value from 0 through 4294967295.

Syntax Description

For Localized Data Policy

(**accept** | **drop**)	Accept or Drop: By default, all packets that match the parameters in the **match** portion of the **policy access-list** configuration are dropped. Include **drop** to explicitly reject matching packets. Include **accept** to accept matching packets and to perform any specified actions.
count *counter-name*	Count Packets Count the packets that match the match criteria, saving the information to the specified filename. If you configure a counter and additional actions, such as policing, the data packets are counted before the other actions are performed, regardless of the order in which you enter the commands in the configuration.
class *class-name*	Class Assign the packets to the specified QoS class name.
set dscp *value*	DSCP; For QoS, set or overwrite the DSCP value in the packet. *value* can be a number from 0 through 63.
log	Log Packet Headers: Log the packet headers into the vsyslog and messages system logging (syslog) files.
set next-hop *ipv4-address*	Next-Hop Address: Set the next-hop address. The address must be an IPv4 address.
policer *policer-name*	Policing: Police the packets using the specified policer.

Syntax Description

For Zone-Based Firewall Policy

drop	Drop: Discard the data traffic.

inspect	Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender.
log	Log Packet Headers: Log the packet headers into the vsyslog and messages system logging (syslog) files.
pass	Pass Through: Allow the packet to pass through to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

Command History

Release	Modification
14.1	Command introduced.
14.2	Added application-aware routing policy.
14.3	Added Cflowd traffic monitoring.
15.2	Added setting GRE encapsulation and preferred color for an SLA class.
15.4	Added match condition for localized control policy.
16.1	Added log option to application-aware policy action.
16.3	Added backup-sla-preferred-color option for application-aware routing.
17.1	Added load-balancing among multiple colors for application-aware routing.
17.2	Added redirect-dns option for centralized data policy.
18.2	Added zone-based firewall policy.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Added support to Cisco IOS XE Catalyst SD-WAN devices for selecting one or more local TLOCs for an action.
Cisco IOS XE Release 17.4.1 Cisco SD-WAN Release 20.4.1	Added support for Cisco IOS XE Catalyst SD-WAN devices for redirecting application traffic to a Secure Internet Gateway (SIG).
26.2.1	Added entry limits for local-tloc-list colors, preferred-color, and backup-sla-preferred-color. Removed obsolete mirror option.

Example

Create a centralized control policy that changes the TLOC for accepted packets:

```
policy
  control-policy change-tloc
    sequence 10
      action accept
        set tloc 1.1.1.2
```

Related Topics

apply-policy, on page 72
lists, on page 283
match, on page 316
policy, on page 382
policy ipv6, on page 388

action

Configure the actions to take when the match portion of an IPv6 policy is met (on vEdge routers only).

Command Hierarchy

Localized Data Policy for IPv6

Configure on vEdge routers only.

```
policy ipv6
  access-list acl-name
    default-action action
    sequence number
      action
        drop
          count counter-name
          log
        accept
          class class-name
          count counter-name
          log
          policer policer-name
          set
            traffic-class value
```

Syntax Description

(**accept** | **drop**)	Accept or Drop: By default, all packets that match the parameters in the **match** portion of the **policy access-list** configuration are dropped. Include **drop** to explicitly reject matching packets. Include **accept** to accept matching packets and to perform any specified actions.
count*counter-name*	Count Packets: Count the packets that match the match criteria, saving the information to the specified filename. If you configure a counter and additional actions, such as policing, the data packets are counted before the other actions are performed, regardless of the order in which you enter the commands in the configuration.

class*class-name*	Class: Assign the packets to the specified QoS class name.
log	Log Packet Headers: Log the packet headers into system logging (syslog) files.
policer*policer-name*	Policing: Police the packets using the specified policer.
set traffic-class*value*	Traffic Class: For QoS, set or overwrite the traffic class value in the packet. *value* can be a number from 0 through 63.

Command History

Release	Modification
14.1	Command introduced.
16.3	Command modified for IPv6.
26.2.1	Removed obsolete mirror option.

Example

Configure an IPv6 ACL that changes the traffic class on TCP port 80 data traffic, and apply the ACL to an interface in VPN 0:

```
vEdge# show running-config policy ipv6 access-list
policy
 ipv6 access-list traffic-class-48-to-46
 sequence 10
  match
   destination-port 80
   traffic-class    48
  !
  action accept
   count port_80
   log
   set
    traffic-class 46
   !
  !
 !
 default-action accept
 !
!
vEdge# show running-config vpn 0 interface ge0/7 ipv6
vpn 0
 interface ge0/7
  ipv6 access-list traffic-class-48-to-46 in
 !
!
```

Operational Commands

show running-config

Related Topics

policy, on page 382

address-family

Configure global and per-neighbor BGP address family information (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      address-family ipv4_unicast
        aggregate-address prefix/length [as-set] [summary-only]
        maximum-paths paths number
        network prefix/length
       redistribute (connected | nat | natpool-outside | omp | ospf | static) [route-policy
 policy-name]

vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        address-family ipv4_unicast
          maximum-prefixes number [threshold] [restart minutes | warning-only]
          route-policy policy-name (in | out)
```

Syntax Description

ipv4_unicast	Address Family: Currently, Cisco SD-WAN software supports only the BGP IPv4 unicast address family.
aggregate-address *prefix / length* [**as-set**][**summary-only**]	Aggregate Prefixes: For all BGP sessions, aggregate the specified prefixes. To generate set path information, include the **as-set** option. To filter out more specific routes from BGP updates, include the **summary-only** option.
maximum-paths paths *number*	IBGP and EBGP Multipath Load Sharing: For all BGP sessions, enable multipath load sharing, and configure the maximum number of parallel paths that can be installed into a route table. Range: 0 to 32

network *prefix / length*	Networks To Advertise: Networks to be advertised by BGP. Identify the networks by their prefix and length.
maximum-prefixes *number* [*threshold*] [**restart** *minutes* | **warning-only**]	Prefixes Received from a Neighbor: Configure how to handle prefixes received from the BGP neighbor: *number* is the maximum number of prefixes that can be received from the neighbor. Range: 1 through 4294967295 Default: 0 (there is no limit to the number of prefixes received) Treshold is the percentage of the maximum number of prefixes at which to either generate a warning message or restart the BGP peering session. Range: 1 through 100 percent Default: 0 (no warning message is generated) **restart** *minutes* is how long to wait after the maximum number of prefixes has been exceeded before restarting the BGP peering session with the neighbor. Range: 0 through 65535 minutes (approximately 1092 hours, or 45 days) Default: None **warning-only** displays a warning message only when the maximum prefix limit is exceeded.
route-policy *policy-name* (**in** |**out**)	Policy to Apply to Received Prefixes: Apply the specified policy, *policy-name*, to prefixes received from the neighbor. You can apply the policy inbound (**in**) as the prefixes are received from the neighbor or outbound (**out**) as they are send to the neighbor.
redistribute (**connected** | **nat** | **natpool-outside** | **omp** | **ospf** | **static**) [**route-policy** *policy-name*]	Redistribute Routes into BGP: For all BGP sessions, redistribute routes learned from other protocols into BGP. Optionally, apply a route policy to the redistributed routes.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added redistribute natpool-outside option.

Example

Redistribute OMP routes into BGP:

```
vpn 1
  router
    bgp 123
      address-family ipv4-unicast
      redistribute omp
      !
    !
  !
!
```

Have BGP advertise the network 1.2.0.0/16:

```
vEdge(config-address-family-ipv4-unicast)# network 61.0.1.0/24
vEdge(config-address-family-ipv4-unicast)# network 10.20.25.0/24
vEdge(config-address-family-ipv4-unicast)# show full-configuration
vpn 1
 router
  bgp 1
   address-family ipv4-unicast
    network 61.0.1.0/24
    network 10.20.24.0/24
   !
  !
 !
!
vEdge(config-address-family-ipv4-unicast)# commit and-quit
Commit complete.
vEdge# show bgp routes

                                      LOCAL                  AS     PATH
VPN  PREFIX         NEXTHOP  METRIC  PREF   WEIGHT  ORIGIN  PATH   STATUS
-------------------------------------------------------------------------------
1    10.20.25.0/24  0.0.0.0  0       -      32768   igp     Local  valid,best
1    61.0.1.0/24    0.0.0.0  0       -      32768   igp     Local  valid,best
```

Operational Commands

clear bgp neighbor

show bgp neighbor

show bgp routes

address-pool

Configure the pool of addresses in the service-site network for which the vEdge router interface acts as DHCP server (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      address-pool prefix/length
```

Syntax Description

prefix/length	Address Pool: IPv4 prefix range of the DHCP address pool.

Command History

Release	Modification
14.3	Command introduced.

Example

Configure the interface to be the DHCP server for the addresses covered by the IP prefix 10.0.100.0/24:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server address-pool 10.0.100.0/24
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   address-pool 10.0.100.0/24
  !
 !
!
```

Operational Commands

show dhcp interface

show dhcp server

admin-auth-order

Have the "admin" user use the authentication order configured in the **auth-order** command, when verifying access to an overlay network device through an SSH session or a console connection.

If you do not configure the **admin-auth-order** command, the "admin" user is always authenticated locally.

In Releases 17.1 and earlier, when you log in as "admin" from a console port, you are authenticated locally. No other authentication methods can be used.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
    admin-auth-order
```

Command History

Release	Modification
16.2	Command introduced.
17.2	Modified for supporting authentication order process for console connections.

Operational Commands

show aaa usergroup

show users

Example

Set the authentication order for the "admin":

```
Viptela# config
Entering configuration mode terminal
Viptela(config)# system aaa admin-auth-order
Viptela(config)# commit and-quit
Commit complete.
Viptela# show running-config system aaa
system
 aaa
  admin-auth-order
 !
!
```

Command History

Command introduced in Viptela Software Release 16.2.In Release 17.2, support authentication order process for console connections.

Related Topics

auth-fallback, on page 82
auth-order, on page 85
radius, on page 407
tacacs, on page 474
usergroup, on page 527

admin-state

Enable or disable the DHCP server functionality on the interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      admin-state (down | up)
```

Syntax Description

down	Disable DHCP Server Functionality: By default, DHCP server functionality is disabled on a vEdge router interface.
enable	Enable DHCP Server Functionality: Allow the vEdge router to act as a DHCP server for the local site networks accessible through this interface.

Command History

Release	Modification
14.3	Command introduced.

Example

Enable DHCP server functionality on an interface:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server address-pool 10.0.100.0/24
vEdge(config-interface-ge0/4)# dhcp-server admin-state up
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
```

```
  dhcp-server
   admin-state up
   address-pool 10.0.100.0/24
  !
 !
!
```

Operational Commands

show dhcp interface

show dhcp server

admin-tech-on-failure

When a Cisco vEdge device reboots, collect 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.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  admin-tech-on-failure
```

This comand has no keywords or arguments.

Command History

Release	Modification
17.1	Command introduced.

Example

Configure the device to collect system status information in an admin-tech file when the device reboots:

```
vEdge# show running-config system
system
 admin-tech-on-failure
!
```

Operational Commands

request admin-tech

Related Topics

request admin-tech, on page 655
show crash, on page 803

advertise

To advertise additional paths for a BGP peer policy template based on selection, use the **advertise** command in address family configuration 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 all VPNs on a device.

advertise isis command is added to support IS-IS route redistribution in OMP. OMP is updated to advertise both Level 1 and Level 2 IS-IS routes for Software Defined Access (SDA). This command is supported for both the IPv4 and IPv6 address families.

advertise [**aggregate** *prefix* [**aggregate-only**]] [**bgp**] [**connected**] [**ospf** *type*] [**static**] [**route-map** *map-tag*]

no advertise [**bgp**] [**connected**] [**ospf** *type*] [**static**] [**route-map** *map-tag*]

Syntax Description

aggregate *prefix* [**aggregate-only**]	Aggregate Routes: Aggregate routes from the specified prefix before advertising them into OMP. By default, the aggregated prefixes and all individual prefixes are advertised. To advertise only the aggregated prefix, include the **aggregate-only** option.
bgp	BGP Routes: Advertise all BGP routes learned by the Cisco vEdge device or Cisco IOS XE SD-WAN device to OMP.
connected	Connected Routes: Advertise all connected routes on the Cisco vEdge device or Cisco IOS XE SD-WAN device to OMP. Connected routes are advertised by default. To disable advertisement, use the **no advertise connected** command.
network *prefix*	Network Routes: Advertise a specific route learned by the Cisco vEdge device or Cisco IOS XE SD-WAN device to OMP. This route must be in the device route table for the VPN. Use this option to advertise a specific route instead of advertising all routes for a protocol.
ospf *type*	OSPF Routes: Advertise all OSPF routes learned by the local Cisco vEdge device or Cisco IOS XE SD-WAN device 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 vEdge device or Cisco IOS XE SD-WAN device to OMP. Static routes are advertised by default. To disable advertisement, use the **no advertise static** command.
isis	IS-IS Routes Advertise both Level 1 and Level 2 IS-IS routes for Software Defined Access (SDA) for both the IPv4 and IPv6 address families.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.

Command Default

This command has no default behavior.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

Command History

Release	Modification
14.1	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Added route-map.

Example

The following example shows the ISIS route distribution in OMP:

age-time

Configure when MAC table entries age out (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Bridge

Command Hierarchy

```
bridge bridge-id
  age-time seconds
```

Syntax Description

seconds	MAC Table Entry Aging Time: How long an entry is in the MAC table before it ages out. Default: 300 seconds (5 minutes) Range: 10 through 4096 seconds

Command History

Release	Modification
15.3	Command introduced.

Example

Change the age out time for bridge 1 to 6 minutes.

```
vEdge# show running-config bridge
bridge 1
  age-time 360
  vlan 1
  interface ge0/2
    no native-vlan
    no shutdown
  !
  interface ge0/5
    no native-vlan
    no shutdown
  !
  interface ge0/6
    no native-vlan
    no shutdown
  !
!
```

Operational Commands

show bridge interface

show bridge mac

show bridge table

alarms

To enter the alarms configuration mode and set alarm parameters, use the **alarms** command in system configuration mode.

alarms

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes System configuration (config-system)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples The following example shows how you can enter the alarm configuration mode:

```
config

 system

  alarms
```

Related Commands

Command	Description
cpu-usage	Configures CPU-usage watermarks and polling interval.
memory-usage	Configures memory-usage watermarks and polling interval.
disk-usage	Configures disk-usage watermarks and polling interval.
disk-speed	Configures watermarks for the disk read and write speeds for disk partitions on a Cisco vManage server.
show alarms	Displays alarms history and watermarks for CPU, memory, and disk usage, and the disk read and write speeds.

allow-local-exit

Configure Cloud OnRamp for SaaS (formerly called CloudExpress service) to use an interface with Direct Internet Access (DIA) as an exit to the Internet (on vEdge routers only). To ensure that Cloud OnRamp for SaaS is set up properly, configure it in vManage NMS, not using the CLI.

Command Hierarchy

```
vpn vpn-id
  cloudexpress
    allow-local-exit
```

Command History

Release	Modification
16.3	Command introduced.

Example

Allow local exit for Cloud OnRamp for SaaS in VPN 100:

```
vEdge# show running-config vpn 100 cloudexpress
vpn 100
 cloudexpress
  allow-local-exit
 !
!
```

Operational Commands

clear cloudexpress computations

show cloudexpress applications

show cloudexpress gateway-exits

show cloudexpress local-exits

show omp cloudexpress

show running-config vpn cloudexpress

allow-same-site-tunnels

Allow tunnels to be formed between vEdge routers in the same site (on Cisco vEdge routers only).

Note No BFD sessions are established between two collocated Cisco vEdge routers. However, with the command "allow-same-site-tunnels", we can form tunnels between Cisco vEdge Routers at the same site.

vManage Feature Template

For Cisco vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  allow-same-site-tunnels
```

Command History

Release	Modification
15.4	Command introduced.

Example

In this example, vEdge2 has two circuits, one to the Internet and the second to an MPLS network. vEdge1 is also located at the same site, but has no circuits. This configuration binds two subinterfaces from vEdge1 to the two circuit interfaces on vEdge2 so that vEdge1 can establish TLOCs on the overlay network.

```
vEdge1# show running-config system
allow-same-site-tunnels
...
vEdge1# show running-config vpn 0
interface ge0/2.101
  ip address 101.1.19.15/24
  mtu 1496
  tunnel-interface
    color lte
  !
  no shutdown
!
interface ge0/2.102
  ip address 102.1.19.15/24
  mtu 1496
  tunnel-interface
    color mpls
  !
  no shutdown
!
vEdge2# show running-config system
allow-same-site-tunnels
...
vEdge2# show running-config vpn 0
interface ge0/0
  ip address 172.16.255.2
  tunnel-interface
    color lte
  !
  no shutdown
!
interface ge0/3
  ip address 172.16.255.16
  tunnel-interface
    color mpls
  !
  no shutdown
!
interface ge0/2.101
  ip address 101.1.19.16/24
  mtu 1496
  tloc-extension ge0/0
  no shutdown
!
interface ge0/2.102
  ip address 102.1.19.16/24
  mtu 1496
  tloc-extension ge0/3
  no shutdown
!
```

Related Topics

tloc-extension, on page 494

allow-service

Configure the services that are allowed to run over the WAN connection in VPN 0, which is the VPN that is reserved for control plane traffic. For other VPNs, use of these services is not restricted.

On a vEdge router, services that you configure on a tunnel interface act as implicit access lists (ACLs). If you explicitly configure ACLs on a tunnel interface, with the **policy access-list** command, the handling of packets matching both implicit and explict ACLs depends on the exact configuration. For more information, see the *Configuring Localized Data Policy* article for your software release.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      [no] allow-service service-name
```

interface-name	Interface Type: Name of a physical interface. The services that you configure in **allow-service** commands apply only to physical interfaces, such as **ge** and **eth** interfaces. They do not apply to non-physical interfaces, such as loopback interfaces.

service-name	Type of Service: Type of service to allow or disallow on the WAN tunnel connection. On vEdge routers, *service-name* can be **all** or one of more of **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 vEdge router tunnel interface. On vSmart controllers, *service-name* can be **all** or one or more of **dhcp**, **dns**, **icmp**, **netconf**, **ntp**, **sshd**, and **stun**. By default, DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP are enabled on a vSmart controller tunnel interface. On vManage NMSs, *service-name* can be **all** or one or more of **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **sshd**, and **stun**. By default, DHCP (for DHCPv4 and DHCPv6), DNS, ICMP, and HTTPS are enabled on a vManage NMS tunnel interface. You cannot disallow the following services: DHCP, DNS, NTP, and STUN. If you allow the NTP service on the WAN connection in VPN 0, 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 vEdge 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 vEdge router that is behind a NAT, you can also have tunnel interface to discover its public IP address and port number from the vBond controller, 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. **Caution** When **allow-service all** overrides the commands allowing or restricting individual services, the implicit ACLs created by the configuration of the services are disabled. Disabling the implicit ACLs could open the control-plane to attacks. Before you configure **allow-service all**, consider whether you should configure explicit ACLs or a ZBFW.

Command History

Release	Modification
14.1	Command introduced.
15.4	BGP, OSPF services and support for netconf added on vEdge routers.
16.3	Added support for DHCPv6.
18.1.1	Added support for *https* service on vEdge routers.

Example

Display the services that are enabled by default on the WAN connection:

```
vEdge# show running-config vpn 0 interface ge0/2 tunnel-interface | details
vpn 0
 interface ge0/2
  tunnel-interface
   encapsulation ipsec weight 1
   color lte
```

```
   max-controllers     2
   control-connections
   carrier             default
   hello-interval      1000
   hello-tolerance     12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service https
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  !
 !
!
```

Operational Commands

show ntp associations

show ntp peer

show running-config vpn 0

Related Topics

connections-limit, on page 142
icmp-redirect-disable, on page 233
implicit-acl-logging, on page 238
ntp, on page 356
service, on page 445
vbond-as-stun-server, on page 532

api-key

To configure the API key for Umbrella registration, on Cisco IOS XE Catalyst SD-WAN devices, use the **api-key** command in config-profile mode.

api-key *api-key*

Syntax Description

api-key	API key (hexadecimal).

Command Mode

config-profile

Command History

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

Examples

Use **parameter-map type umbrella global** to enter config-profile mode, then use **orgid**, **api-key**, and **secret** to configure Umbrella registration.

In config-profile mode, you can use **show full-configuration** to display Umbrella registration details.

Example

This example configures Umbrella registration details.

```
Device(config)# parameter-map type umbrella global
Device(config-profile)# orgid 1234567
Device(config-profile)# api-key aaa12345aaa12345aaa12345aaa12345
Device(config-profile)# secret 0 bbb12345bbb12345bbb12345bbb12345
```

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	This command was introduced.

In the following example, you can create real-time-video app-probe-class with DSCP measurements:

```
Device(config)# app-probe-class real-time-video
Device(config)# forwarding-class videofc
Device(config)# color mpls dscp 34
```

```
Device(config)# color biz-internet dscp 40
Device(config)# color lte dscp 0
```

app-route-policy

Configure or apply a policy for application-aware routing (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

Create 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]
```

Apply a Policy for Application-Aware Routing

```
apply-policy
  site-list list-name app-route-policy policy-name
```

Syntax Description

policy-name	Application-Aware Routing 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. The number of app-route-policy entries is limited to 2048.

Command History

Release	Modification
14.2	Command introduced.
26.2.1	Added limit for app-route-policy entries.

Example

Configure and apply a simple 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
 !
!
```

Operational Commands

show app-route stats

Related Topics

sla-class, on page 455

app-visibility

Enable application visibility so that a vEdge router can monitor and track the applications running on the LAN (on vEdge routers only).

vManage Feature Template

For vEdge routers:

Configuration ► Policies ► Localized Policy

Command Hierarchy

```
policy
   app-visibility
```

Command History

Release	Modification
15.2	Command introduced.

Example

Enable application-visibility on a vEdge router:

```
vEdge# show running-config policy
policy
 app-visibility
!

vEdge# show app dpi flows

                                    Source  Dest

VPN  SRC IP         DST IP          Port    Port   PROTOCOL  APPLICATION  FAMILY
  ACTIVE SINCE
-------------------------------------------------------------------------------------------------------
1    10.192.42.2    23.4.153.244    1557    443    tcp       https        Web
  2015-05-04T13:47:29+00:00
1    10.192.42.2    74.125.20.95    20581   443    udp       unknown      Standard
  2015-05-04T13:47:07+00:00
1    10.192.42.2    74.125.25.188   55742   5228   tcp       gtalk        Instant Messaging
  2015-05-03T21:06:57+00:00
1    10.192.42.2    192.168.15.3    19286   53     udp       dns          Network Service
  2015-05-04T13:47:25+00:00
1    10.192.42.2    192.168.15.3    20605   53     udp       dns          Network Service
  2015-05-04T13:47:08+00:00
1    10.192.42.2    192.168.15.3    34716   53     udp       dns          Network Service
  2015-05-04T13:47:29+00:00
1    10.192.42.2    192.168.15.3    43894   53     udp       dns          Network Service
  2015-05-04T13:47:28+00:00
1    10.192.42.2    192.168.15.3    50865   53     udp       dns          Network Service
  2015-05-04T13:47:25+00:00
```

```
1    10.192.42.2    216.58.217.10  60079   443    tcp       google       Web
  2015-05-04T13:47:08+00:00
1    10.192.42.2    216.115.20.77  10000   10000  udp       sip          Audio/Video
  2015-05-03T08:22:51+00:00
1    192.168.20.83  1.1.42.1       51586   22     tcp       ssh          Encrypted
  2015-05-04T13:28:03+00:00

vEdge# show app dpi applications

VPN  SRC IP          APPLICATION         FAMILY
-------------------------------------------------------------
1    2.51.88.142     bittorrent          Peer to Peer
1    10.192.42.1     syslog              Application Service
1    10.192.42.1     tcp                 Network Service
1    10.192.42.1     unknown             Standard
1    10.192.42.2     addthis             Web
1    10.192.42.2     adobe               Web
1    10.192.42.2     adobe_update        Web
1    10.192.42.2     akamai              Web
1    10.192.42.2     alexa               Web
1    10.192.42.2     alibaba             Web
1    10.192.42.2     aliexpress          Web
1    10.192.42.2     amazon              Web
1    10.192.42.2     amazon_adsystem     Web
1    10.192.42.2     amazon_aws          Web
1    10.192.42.2     amazon_cloud_drive  Web
1    10.192.42.2     aol                 Web
1    10.192.42.2     apple               Web
1    10.192.42.2     appstore            Application Service
1    10.192.42.2     ask                 Web
1    10.192.42.2     att                 Web
1    10.192.42.2     bing                Web
1    10.192.42.2     bittorrent          Peer to Peer
1    10.192.42.2     blackberry          Web
1    10.192.42.2     blackberry_locate   Web
1    10.192.42.2     blackberry_update   Web
1    10.192.42.2     brightcove          Web
1    10.192.42.2     chrome_update       Web
1    10.192.42.2     cloudflare          Web
...
1    216.58.192.14   https               Web
1    216.58.217.10   https               Web
1    216.58.217.10   tcp                 Network Service
1    216.58.217.46   https               Web
1    216.59.38.123   tcp                 Network Service
1    216.115.100.103 tcp                 Network Service
1    221.13.84.240   bittorrent          Peer to Peer
1    222.54.68.154   bittorrent          Peer to Peer
1    222.117.30.93   bittorrent          Peer to Peer
1    222.228.8.6     bittorrent          Peer to Peer
```

Operational Commands

clear app dpi all

clear app dpi apps

clear app dpi flows

show app dpi applications

show app dpi flows

show app dpi supported-applications

applications

Configure applications for which to enable Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only). To ensure that Cloud OnRamp for SaaS is set up properly, configure it in vManage NMS, not using the CLI.

Command Hierarchy

```
vpn vpn-id
  cloudexpress
    applications applications
```

Syntax Decription

applications	Interface Node Type: List of applications. Values: amazon_aws, box_net, concur, dropbox, google_apps, gotomeeting, intuit, office365, oracle, salesforce, sugar_crm, zendesk, zoho_crm Default: none

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a list of applications for which to enable Cloud OnRamp for SaaS:

```
vEdge# show running-config vpn 100 cloudexpress
vpn 100
 cloudexpress
  applications salesforce office365 amazon_aws oracle box_net dropbox intuit concur zendesk
 gotomeeting google_apps
 !
!
```

Operational Commands

clear cloudexpress computations

show cloudexpress applications

show cloudexpress gateway-exits

show cloudexpress local-exits

show omp cloudexpress

show running-config vpn cloudexpress

apply-policy

Have a policy take effect by applying it to sites within the overlay network (on vSmart controllers only).

Command Hierarchy

For Application-Aware Routing Policy

```
apply-policy
  site-list list-name
    app-route-policy policy-name
```

For Centralized Control Policy

```
apply-policy
  site-list list-name
    control-policy policy-name (in | out)
```

For Centralized Data Policy

```
apply-policy
  site-list list-name
    data-policy policy-name (all | from-service | from-tunnel)
    cflowd-template template-name
apply-policy
  site-list list-name vpn-membership policy-name
```

Syntax Description

cflowd-template *template-name*	Cflowd Template: For a centralized data policy that applies to cflowd flow collection, associate a flow collection template with the data policy. The number of cflowd-template entries is limited to 2048.

app-route-policy *policy-name* **control-policy** *policy-name* (**in**| **out**)**data-policy** *policy-name* (**all** | **from-service** | **from-tunnel**)**vpn-membership**	Policy Name: *policy-name* Name of the policy to apply to the specified sites. *policy-name* must match that which you specified in the , **data-policy**, or **vpn-membership** configuration **control-policy**command. For centralized control policy, specify the direction in which to apply the policy. The **in** option applies the policy to packets before they are placed in the vSmart controller's RIB, so the specified actions affect the OMP routes stored in the RIB. The **out** option applies the policy to packets after they are exported from the RIB. For centralized data policy, specify the direction in which to apply the policy. The **all** option (which is the default) applies to all data traffic passing through the vEdge router: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. To apply the data policy only to policy exiting from the local site, use the **from-service** option. To apply the policy only to incoming traffic, use the **from-tunnel** option. You can apply different data policies in each of the two traffic directions. app-route-policy entries are limited to 1. data-policy entries are limited to 2.
site-list *list-name*	Site List: List of sites to which to apply the policy. *list-name* must match a list name that you configured in the **policy lists site-list** portion of the configuration. For the same type of policy, when you apply policies with **apply-policy** commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists **site-list 1 site-id 1-100** and **site-list 2 site-id 70-130**. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different **control-policy** policies, for example, the attempt to commit the configuration on the vSmart controller would fail. You can, however, apply one of these sites lists to a **control-policy** policy and the other to a **data-policy** policy. The restriction regarding overlapping site IDs applies to the following types of policies: • Application-aware routing policy (**app-route-policy**) • Centralized control policy (**control-policy**) • Centralized data policy (**data-policy**) • Centralized data policy used for cflowd flow monitoring (a **data-policy** that includes a **cflowd** action and an **apply-policy** that includes a **cflowd-template** command)

Command History

Release	Modification
14.1	Command introduced.
14.2	Added app-route-policy.
14.3	Added cflowd-template.
15.2	Added **all**, **from-service**, and from-tunnel options
15.4	Added restrictions so that you cannot apply the same type of policy.
16.3	Added support for overlapping sites in different site lists.
26.2.1	Added limits for cflowd-template, app-route-policy, and data-policy entries.

Operational Commands

show running-config apply-policy

Example 1

Apply a centralized control policy to the sites defined in the list **west**:

```
apply-policy
  site-list west control-policy change-tloc out
```

On a vSmart controller, configure site lists to use for control and data policies that contain overlapping site identifiers, and apply the policies to these site lists:

```
policy
  lists
    # site lists for control-policy
    site-list us-control-list
      site-id 1-200
    site-list emea-control-site-list
      site-id 201-300
    site-list apac-control-site-list
      site-id 301-400
    # site lists for data-policy
    site-list platinum-site-list
      site-id 50-70
    site-list titanium-site-list
      site-id 70-130
    site-list rhodium-site-list
      site-id 131-301
  control-policy us-control-policy
    ...
  control-policy emea-control-policy
    ...
  control-policy apac-control-policy
    ...
  data-policy platinum-data-policy
    ...
  data-policy titanium-data-policy
    ...
  data-policy rhodium-data-policy
    ...
```

```
apply-policy
  # Apply control policies. Among the control policies, there is no overlap of site IDs.
  site-list us-control-site-list
    control-policy us-control-policy in        # policy is applied to sites 1-200
                                               # sites overlap with data-policy
platinum-data-policy
  site-list emea-control-site-list
    control-policy emea-control-policy in      # policy is applied to sites 201-300
                                               # sites overlap with data-policy
rhodium-data-policy
  site-list apac-control-site-list
    control-policy apac-control-site-list in   # policy is applied to sites 301-400
                                               # sites overlap with data-policy
rhodium-data-policy

  # Apply data policies. Among the data policies, there is no overlay of site IDs.
  site-list platinum-site-list
    data-policy platinum-data-policy all       # policy is applied to sites 50-70
                                               # sites overlap with control-policy
us-control-policy
  site-list titanium-site-list
    data-policy titanium-data-policy all       # policy is applied to sites 70-130
                                               # sites overlap with control-policy
us-control-policy
  site-list rhodium-site-list
    data-policy rhodium-data-policy all        # policy is applied to sites 131-301
                                               # sites overlap with control-policy
us-control-policy,
                                          # emea-control-policy, and apac-control-policy
```

Command History

Command introduced in Cisco SD-WAN Software Release 14.1.**app-route-policy** option added in Release 14.2.**cflowd-template** option added in Release 14.3.**all**, **from-service**, and **from-tunnel** options for centralized data policy added in Release 15.2.In Release 15.4, added restrictions so that you cannot apply the same type of policy (for example, data-policy or control-policy) to site lists that contain overlapping site IDs.In Release 16.3, add support for overlapping sites in different site lists.

Related Topics

show policy from-vsmart, on page 971
action, on page 48
cflowd-template, on page 121
control-policy, on page 148
data-policy, on page 165
lists, on page 283
match, on page 314
policy, on page 382

archive

Periodically archive a copy of the full running configuration to an archival file. What is archived is the configuration that is viewable by the user "admin".

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► Archive

Command Hierarchy

```
system
  archive
    interval minutes
    path file-path
    ssh-id-file filename
    vpn vpn-id
```

Syntax Description

interval *minutes*	Archival Time Interval: How often to archive the full running configuration. In addition, the running configuration is archived each time you issue the **commit** command on a Cisco vEdge device. *Range*: 5 minutes through 525600 minutes (about one year) *Default*: 10080 minutes (7 days)
path *file-path / filename*	Location of Archival File: Path to the directory in which to store the archival file and the base name of the file. *file-path* can be one of the following: • **ftp:** *file-path*—Path to a file on an FTP server. • **scp:** *user* **@** *host* **:** *file-path* • **/** *file-path* **/** *filename*—Path to a file on the local Cisco vEdge device. A separate file is created for each archiving operation. To distinguish the files, a timestamp is appended to the filename. The timestamp has the format *yyyy-mm-dd_hh-mm-ss*.
ssh-id-file *filename*	SSH Key File Name of the SSH private key file on the local Cisco vEdge device. This file is used to SCP into a remote file server. The Cisco SD-WAN software automatically generates a public and a private key and places the public key in the SSH key file archive_id_rsa.pub, which is located in /home/admin directory on the Cisco vEdge device. If you do not include the **ssh-id-file** option in the configuration, the software uses the automatically generated private key. You can also manually generate and upload an SSH private key file.
vpn *vpn-id*	VPN: VPN in which the archival file server is located or through which the server can be reached. On vEdge routers, *vpn-id* can be a value from 0 through 65530. On vSmart controllers, *vpn-id* can be either 0 or 512.

Command History

Release	Modification
14.2	Command introduced.

Example

Archive the running configuration on a vEdge router every two weeks:

```
system
  archive
    interval 20160
    path scp://eve@eves-computer:/usr/archives
    ssh-id-file /ssh-key-file
    vpn 1
```

Operational Commands

show running-config system

Related Topics

load, on page 1079
save, on page 1084

area

Configure an OSPF area within a VPN on a vEdge router.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
 router
    ospf
      area number
        interface interface-name
          authentication
            authentication-key key
            message-digest key
            type (message-digest | simple)
          cost number
          dead-interval seconds
          hello-interval seconds
        network (broadcast | point-to-point)
          passive-interface
          priority number
          retransmit-interval seconds
        ! end area interface
        nssa
          no-summary
```

```
    translate (always | candidate | never)
  range prefix/length
     cost number
     no-advertise
  stub
    no-summary
```

Syntax Description

number	Area Number: Number of the OSPF area. *Range:* The area is a 32-bit number.

Command History

Release	Modification
14.1	Command introduced.

The remaining commands are explained separately.

Example

In VPN 1 on a vEdge router, configure OSPF area 0. The interface **ge0/0** participates in the local OSPF network.

```
vEdge# show running-config vpn 1 router ospf
vpn 1
 router
  ospf
   redistribute static
   redistribute omp
   area 0
    interface ge0/0
    exit
   exit
  !
 !
!

vEdge# show interface vpn 1
                             IF      IF

                             ADMIN   OPER    ENCAP  PORT                              SPEED
                         RX      TX
VPN  INTERFACE  IP ADDRESS    STATUS  STATUS  TYPE   TYPE     MTU   HWADDR            MBPS
   DUPLEX  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------
1    ge0/0      10.2.2.11/24  Up      Up      null   service  1500  00:0c:29:ab:b7:58  10
    full    0:01:36:54  725      669
```

Operational Commands

show ospf interface

show ospf neighbor detail

arp

Configure an ARP table entry for an interface in a VPN (on vEdge routers only).

Address Resolution Protocol (ARP) resolves network layer IP address to a link layer physical address, such as an Ethernet MAC address. By default, ARP is enabled on vEdge routers, and they maintain an ARP cache that maps IP addresses to MAC addresses for devices in their local network. To learn a device's MAC address, vEdge routers broadcast ARP messages to that device's IP address, requesting the MAC address.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
   interface interface-name
    arp
      ip ip-address mac mac-address
```

ip *ip-address* **mac** *mac-address*	Add a Permanent ARP Table Entry: Configure a permanent (static) ARP table entry. Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name. Enter the MAC address in colon-separated hexadecimal notation.
no arp ip *ip-address*	Disable ARP: Remove a static ARP mapping address.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure a permanent MAC address for the ARP table:

```
vpn 0
 interface ge0/0
    arp ip 10.10.0.0 mac 00:10:FA:B5:AE:15
```

Operational Commands

clear arp

show arp

arp-timeout

Configure how long it takes for a dynamically learned ARP entry to time out (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    arp-timeout seconds
```

seconds	Timeout Time Time before a dynamically learned ARP entry times out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 seconds (20 minutes)

Command History

Release	Modification
14.1	Command introduced.

Example

Set the ARP timeout value to 40 minutes:

```
vEdge(config-interface-ge0/4)# arp-timeout 2400
```

Operational Commands

clear arp

show arp

auth-fail-vlan

Configure an authentication-fail VLAN on an interface running IEEE 802.1X, to provide network access when RADIUS authentication or the RADIUS server fails (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      auth-fail-vlan vlan-id
```

Syntax Description

vlan-id	VLAN Identifier: Identifier of the VLAN to be the restricted VLAN. Range: 1 through 4094

Command History

Release	Modification
16.3	Command introduced.

Example

Configure VLAN 30 as the critical VLAN:

```
bridge 30
 name Critical_VLAN
 vlan 30
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
interface ge0/5
 dot1x
  auth-fail-vlan   30
 !
```

```
 no shutdown
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

auth-reject-vlan, on page 87
bridge, on page 115
default-vlan, on page 176
guest-vlan, on page 220
radius, on page 407

auth-fallback

Configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user. By default, authentication fallback is disabled.

The fallback process applies to both SSH sessions and console connections to an overlay network device.

Enable authentication fallback if you want the next authentication method to attempt to authenticate the user even when the user is rejected by the first or second method.

Cisco vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
    auth-fallback
```

Command History

Release	Modification
15.2.8	Command introduced.
17.2	Added support for authentication order process for console connections.

Example

Display the AAA configuration. If authentication fallback is enabled, the **auth-fallback** command is shown in the configuration:

The following examples illustrate the default authentication behavior and the behavior when authentication fallback is enabled:

- If the authentication order is configured as radius local:
  - With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
  - With authentication fallback enabled, local authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access to a user.
- If the authentication order is configured as local radius:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
  - With authentication fallback enabled, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device. In this case, the behavior of two authentication methods is identical.
- If the authentication order is configured as radius tacacs local:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.
  - With authentication fallback enabled, TACACS+ authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access a user. Local authentication is used next, when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.
- When admin-auth-order is enabled and auth-fallback is disabled—Local authentication is used only when all TACACS+ servers are unreachable. If TACACS+ server denies access, a user cannot log in using local authentication.
- When admin-auth-order and auth-fallback are enabled—Local authentication is used when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.

```
vEdge# show running-config system aaa
system
 aaa
  auth-order local radius
  auth-fallback
 !
!
```

Operational Commands

show running config

Related Topics

admin-auth-order, on page 54
auth-order, on page 85
radius, on page 407
tacacs, on page 474
usergroup, on page 527

auth-order

Configure the order in which the Cisco SD-WAN software tries different authentication methods when authenticating devices that are attempting to connect to an 802.1X WAN (on vEdge routers only).

The default authentication order is **radius**, then **mab**.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      auth-order (mab | radius)
```

Syntax Description

mab	MAC Authentication Bypass: Use MAC authentication bypass for authentication, which provides authentication for non-802.1X–compliant devices.
radius	RADIUS Authentication: Use RADIUS servers for authentication.

Example

Configure the router to use MAB authentication before RADIUS authentication:

```
vpn 0
  interface ge0/0
    dot1x
      auth-order mab radius
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

mac-authentication-bypass, on page 312
radius, on page 407
radius-servers, on page 411

auth-order

Configure the order is which the software tries different authentication methods when verifying user access to an overlay network device through an SSH session or a console port. When verifying a user's login credentials, the software starts with the method listed first. Then, if the login credentials do not match, it tries the next authentication method.

To configure the authentication for the "admin" user, use the **admin-auth-order** command.

The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the system radius servercommand. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco vEdge device is denied.

You can configure one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

In Releases 17.1 and earlier, when you log in as "admin" from a console port, you are authenticated locally. No other authentication methods can be used.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
    auth-order (local | radius | tacacs)
```

Syntax Description

	Default Authentication Order: The default authentication order is **local**, then **radius**, and then **tacacs**.
local	Locally Configured Username and Password: Verify users based on the username and password configured on the local overlay network device. If you specify only one authentication method, it must be **local**.
radius	RADIUS Authentication: Verify users based on usernames and passwords configured on a RADIUS server. RADIUS authentication is performed only if a RADIUS server is configured with the **system radius server** command.
tacacs	TACACS+ Authentication: Verify users based on usernames and passwords configured on a RADIUS server. RADIUS authentication is performed only if a RADIUS server is configured with the **system tacacs server** command.

Command History

Release	Modification
14.1	Command introduced.
17.2	Added authentication order process for console connections.

Example

Set the authentication order to be RADIUS first, followed by local authentication:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# system aaa radius local
vEdge(config-aaa)# commit and-quit
Commit complete.
vEdge# show running-config system aaa
system
 aaa
  auth-order local radius
 !
!
```

Operational Commands

show aaa usergroup

show users

Related Topics

admin-auth-order, on page 54
auth-fallback, on page 82
radius, on page 407
tacacs, on page 474
usergroup, on page 527

auth-reject-vlan

Configure an authentication-reject VLAN to place IEEE 802.1X-enabled clients into if authentication is rejected by the RADIUS server (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      auth-reject-vlan vlan-id
```

Syntax Description

vlan-id	VLAN Identifier: Identifier of VLAN into which to place 802.1x-enabled clients if authentication for the clients is rejected by the RADIUS servers. Range: 1 through 4094

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a restricted VLAN:

```
bridge 40
 name Restricted_VLAN
 vlan 40
 interface ge0/5
  no native-vlan
```

```
  no shutdown
 !
!
vpn 0
 interface ge0/5
  dot1x
   auth-reject-vlan 40
  !
  no shutdown
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

auth-fail-vlan, on page 81
bridge, on page 115
default-vlan, on page 176
guest-vlan, on page 220

auth-req-attr

Configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session (on vEdge routers only). These AV pairs are defined in RFC 2865 , RADIUS, and they are placed in the Attributes field of the RADIUS Accounting Request packet.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      auth-req-attr attribute-number (integer integer | octet octet | string string)
```

Syntax Description

attribute-number	Authentication Attribute Number: RADIUS authentication attribute number. Range: 1 through 64
(**integer** *integer* | **octet** *octet* | **string** *string*)	Attribute Value: (**integer** *integer* | **octet** *octet* | **string** *string*) Value of the attribute. Specify the value as an integer, octet, or string, depending on the authentication attribute itself.

Command History

Release	Modification
16.3	Command introduced.

Example

Set the Service-Type authentication attribute to service type 2, which is a Framed service:

```
vEdge# show running-config vpn 0 dot1x
vpn 0
  name "Transport VPN"
  interface ge0/5
  dot1x
    auth-req-attr 6 integer 2
    ...
  !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

acct-req-attr, on page 32
nas-identifier, on page 344
nas-ip-address, on page 345
radius, on page 407
radius-servers, on page 411

authentication

vpn router ospf area interface authentication—Configure authentication for OSPF protocol exchanges (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          authentication
            authentication-key key
            message-digest message-digest-key key-id md5 encrypted-key
            type (message-digest | simple)
```

Syntax Description

key	Authentication Key: Specify the authentication key (password). Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. It can be 1 to 32 characters.
authentication type message-digest message-digest-key *key-id* **md5** *encrypted-key*	MD5 Authentication: Use MD5 authentication for OSPF protocol exchanges on an interface, and specify the key ID and the encrypted key (password) to use to verify received packets. MD5 authentication includes an MD5 checksum in each transmitted packet. *key-id* can be from 1 to 255 characters. If you specify the *encrypted-key* in clear text and the text contains special characters, enclose the key in quotation marks (" ").
authentication type simple	Simple Authentication: Use simple, or plain text, authentication for all OSPF protocol exchanges on an interface.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure MD5 authentication for OSPF:

```
vEdge(config)# vpn 1 router ospf area 3
vEdge(config-area-3)# interface ge0/1
vEdge(ospf-if-ge0/1)# authentication message-digest message-digest-key 6 md5 "$4$P3T3Z2sCirxa5+cCLEFXKw==<"
```

Operational Commands

show ospf interface

authentication-type

vpn interface ike authentication-type—Configure the type of authentication to use during IKE key exchange (on vEdge routers only). IKE supports preshared key (PSK) authentication only.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Security

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ike
      authentication-type pre-shared-key
        local-id id
        pre-shared-secret password
        remote-id id
```

Syntax Description

local-id *id* **remote-id***id*	IKE Session Identifier: String to associate the IKE session with the preshared password. Configure this identifier if the remote IKE connection peer requires a local ID or remote ID from its peer. *id* can be an IP address or any text string from 1 through 63 characters long. Default: Tunnel's source IP address (for **local-id**); tunnel's destination IP address (for **remote-id**)
pre-shared-secret *password*	Preshared Password: Password to use with the preshared key. *password* can be an ASCII or a hexadecimal string from 1 through 127 characters long. **Note** From Cisco SD-WAN 19.2.x release onwards, the pre-shared key needs to be at least 16 bytes in length. The IPsec tunnel establishment fails if the key size is less than 16 characters when the router is upgraded to version 19.2.

Command History

Release	Modification
17.2	Command introduced.

Example

Configure the preshared-key password:

```
vEdge(config)# vpn 1 interface ipsec1 ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret $C$123456
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

show running-config

Related Topics

mode, on page 338

authentication-type

security ipsec authentication-type—Configure the type of authentication to use on IPsec tunnel connections between vEdge routers (on vEdge routers only).

Note This command is deprecated in Cisco SD-WAN Release 20.6.1 and later. Use the command **integrity-type** instead.

Command Hierarchy

```
security
  ipsec
    authentication-type type
```

Syntax Description

type	Authentication Type: Type of authentication to use on IPsec tunnel connections. You can configure multiple authentication types. Configure each type with a separate **security ipsec authentication-type** command. The order in which these commands appear in the configuration does not matter. Each pair of vEdge routers advertise their configured authentications in their TLOC properties, and then the two routers negotiate the authentication to use on the IPsec tunnel connection between them. They use the strongest authentication type configured on each router. For example, if vEdge-1 advertises AH-HMAC-SHA1, ESP HMAC-SHA1, and none and vEdge-2 advertises ESP HMAC-SHA1 and none, the two routers negotiate to use ESP HMAC-SHA1 as the integrity method between them. *type* can be one of the following options, which are listed in order from most strong to least strong: • **ah-sha1-hmac** enables 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), and AH authenticates these fields, as well as the non-mutable fields in the outer header. AH creates an HMAC-SHA1 hash and places it in the last field of the data packet. • **ah-no-id** enables a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the packet's outer IP header. This option accommodates some non-Cisco-vEdge devices, including the Apple AirPort Express NAT, that have a bug that causes the ID field in the IP header, a non-mutable field, to be modified. Configure the **ah-no-id** option in the list of authentication types to have the Cisco SD-WAN AH software ignore the ID field in the IP header so that the Cisco SD-WAN software can work in conjunction with these devices. • **sha1-hmac** enables ESP HMAC-SHA1. With this authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable). ESP then creates an HMAC-SHA1 hash and places it in the last field of the data packet. • **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. You can choose this option in situations where data plane authentication and integrity are not a concern. For information about which data packet fields are affected by these authentication types, see the "Data Plane Integrity" section in the Data Plane Security Overview article for your software release. For Releases 16.2 and later, the encryption algorithm on IPsec tunnel connections is either AES-256-GCM or AES-256-CBC. For unicast traffic, if the remote side supports AES-256-GCM, that encryption algorithm is used. Otherwise, AES-256-CBC is used. For multicast traffic, the encryption algorithm is AES-256-CBC. For Releases 16.1 and earlier, the encryption algorithm on IPsec tunnel connections is AES-256-CBC. You cannot modify the encryption algorithm choice made by the software. When you change the IPsec authentication, the AES key for the data path is changed. Default: **ah-sha1-hmac** and **sha1-hmac**

Command History

Release	Modification
14.2	Command introduced.
Cisco SD-WAN Release 20.6.1	This command was deprecated. Starting from Cisco SD-WAN Release 20.6.1, use the command **integrity-type** instead.

Example

Have the vEdge router negotiate the IPsec tunnel authentication type among AH-SHA1, ESP SHA1-HMAC, and none:

```
vEdge# config
Entering configuration mode terminal
vm6(config)# security ipsec authentication-type sha1-hmac
vm6(config-ipsec)# authentication-type ah-sha1-hmac
vm6(config-ipsec)# authentication-type none
```

auto-cost reference-bandwidth

vpn router ospf auto-cost reference-bandwidth—Control how OSPF calculates the default metric for an interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      auto-cost reference-bandwidth mbps
```

Syntax Description

mbps	Reference Bandwidth: Interface speed. Range: 1 through 4294967 Mbps Default: 100 Mbps

Command History

Release	Modification
14.1	Command introduced.

Example

Set the reference bandwidth to 10 Mbps:

```
vEdge(config)# vpn 1 router ospf
vEdge(config-ospf)# auto-cost reference-bandwidth 10
vEdge(config-ospf)# show config
vpn 1
 router
  ospf
   auto-cost reference-bandwidth 10
  !
 !
!
```

Operational Commands

show ospf process

auto-sig-tunnel-probing

To allow cloudexpress probes in all the active auto SIG tunnels, use the **auto-sig-tunnel-probing** command in config-cloudexpress mode. To disable auto-sig-tunnel-probing, use the **no** form of this command.

auto-sig-tunnel-probing

no auto-sig-tunnel-probing

Command Default Enabled

Command Modes config-cloudexpress

Command History

Release	Modification
Cisco SD-WAN Release 20.6.1	This command was introduced.

Usage Guidelines Use **auto-sig-tunnel-probing** 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.

Example

In this example, you allow cloudexpress probes in all the auto SIG tunnels.

```
Device(config)# vpn 2
Device(config-vpn-2)cloudexpress
Device(config-cloudexpress)# applications amazon_aws concur
Device(config-cloudexpress)# auto-sig-tunnel-probing
Device(config-cloudexpress)# node-type gateway
```

auto-rp

vpn router pim auto-rp— Enable and disable auto-RP for PIM (on vEdge routers only). By default, auto-RP is disabled.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
     auto-rp
```

Command History

Release	Modification
14.2	Command introduced.

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show pim interface

show pim neighbor

autonegotiate

vpn interface autonegotiate—Configure whether an interface runs in autonegotiation mode (on vEdge routers only).

On all vEdge router models, all interfaces support 1-Gigabit Ethernet SFPs. These SFPs can either be copper or fiber. For fiber SFPs, the supported speeds are 1 Gbps full duplex and 100 Mbps full duplex. For copper SFPs, the supported speeds are 10/100/1000 Mbps and half/full duplex. To use a fixed speed and duplex configuration for interfaces that do not support autonegotiation, you must disable autonegotiation and then use the **speed** and **duplex** commands to set the appropriate interface link characteristics.

Integrated routing and bridging (IRB) interfaces do not support autonegotiation. In Releases 17.1 and later, the **autonegotiate** command is not available for these interfaces.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

vManage Feature Template

For all Cisco SD-WAN devices:

Configuration ► Templates ► VPN Interface Bridge

Command Hierarchy

```
vpn vpn-id
  interface geport/slot
    [no] autonegotiate
```

Command History

Release	Modification
15.3	Command introduced.
17.1	Disable this command for IRB interfaces.

Example

Set the interface speed to 10 Mbps:

```
vpn 0
 interface ge0/0
   no autonegotiate
   speed 10
```

Operational Commands

show interface

Related Topics

duplex, on page 195
speed, on page 458

bandwidth-downstream

vpn interface bandwidth-downstream—Generate notifications when the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit (on vEdge routers and vManage NMSs only). Specifically, notifications are generated when traffic exceeds 85 percent of the bandwidth you configure with this command. Notifications generated include Netconf notifications, which are sent to the vManage NMS, SNMP traps, and syslog messages. Notifications are sent when either the transmitted or received bandwidth exceeds 85 percent of the bandwidth configured for that type of traffic.

By default, no bandwidth notifications of any kind are generated, so if you are interested in monitoring bandwidth usage, you must do so manually.

Note Starting from Cisco SD-WAN Release 20.6, the device sends the port speed information for bandwidth, when bandwidth is not configured.

You can configure this command on all interface types except for GRE and loopback interfaces.

vManage Feature Template

For vEdge routers and vManage NMSs only:

Configuration ► Templates ► VPN Interface Bridge

Command Hierarchy

```
vpn 0
  interface interface-name
    bandwidth-downstream kbps
```

Syntax Description

kbps	Interface Received Bandwidth: Maximum received on a physical interface to allow before generating a notification. When the transmission rate exceeds 85 percent of this rate, an SNMP trap is generated. Range: 1 through 2147483647 (2^{32} / 2) – 1 kbps

Example

Have the vEdge router generate a notification when the received or transmitted traffic on an interface exceeds 85 percent of a 50-Mbps circuit:

```
vEdge# show running-config vpn 0 interface ge0/2
vpn 0
 interface ge0/2
  ip address 10.0.5.11/24
  tunnel-interface
   encapsulation ipsec
   color lte
   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
  !
  no shutdown
  bandwidth-upstream   50000
  bandwidth-downstream 50000
 !
!
vEdge# show interface detail ge0/2
interface vpn 0 interface ge0/2
 if-admin-status         Up
 if-oper-status          Up
 if-addr
  ip-address     10.0.5.11/24
  broadcast-addr 10.0.5.255
  secondary      false
 ...
 rx-packets              122120
```

```
rx-octets               25293100
rx-errors               0
rx-drops                1403
tx-packets              117618
tx-octets               24737443
tx-errors               0
tx-drops                0
rx-pps                  13
rx-kbps                 36
tx-pps                  13
tx-kbps                 37
rx-arp-requests         325
tx-arp-replies          333
tx-arp-requests         704
rx-arp-replies          683
...
bandwidth-upstream      50000
bandwidth-downstream    50000
```

Operational Commands

show interface detail (see the rx-kbps and bandwidth-downstream fields)

Related Topics

bandwidth-upstream, on page 99

bandwidth-upstream

vpn interface bandwidth-upstream—Generate notifications when the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit (on vEdge routers and vManage NMSs only). Specifically, notifications are generated when traffic exceeds 85 percent of the bandwidth that you configure with this command. Notifications generated include Netconf notifications, which are sent to the vManage NMS, SNMP traps, and syslog messages. Notifications are sent when either the transmitted or received bandwidth exceeds 85 percent of the bandwidth configured for that type of traffic.

By default, no bandwidth notifications of any kind are generated, so if you are interested in monitoring bandwidth usage, you must do so manually.

Note Starting from Cisco SD-WAN Release 20.6, the device sends the port speed information for bandwidth, when bandwidth is not configured.

You can configure this command on all interface types except for GRE and loopback interfaces.

vManage Feature Template

For vEdge routers and vManage NMSs only:

Configuration ► Templates ► VPN Interface Bridge

Command Hierarchy

```
vpn 0
  interface interface-name
    bandwidth-upstream kbps
```

Syntax Description

kbps	Interface Transmission Bandwidth: Maximum transmitted traffic 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 (2^{32} / 2) – 1 kbps

Command History

Release	Modification
16.2	Command introduced.

Example

Have the vEdge router generate a notification when the received or transmitted traffic on an interface exceeds 85 percent of a 50-Mbps circuit:

```
vEdge# show running-config vpn 0 interface ge0/2
vpn 0
 interface ge0/2
  ip address 10.0.5.11/24
  tunnel-interface
   encapsulation ipsec
   color lte
   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
  !
  no shutdown
  bandwidth-upstream   50000
  bandwidth-downstream 50000
 !
!
vEdge# show interface detail ge0/2
interface vpn 0 interface ge0/2
 if-admin-status         Up
 if-oper-status          Up
 if-addr
  ip-address     10.0.5.11/24
  broadcast-addr 10.0.5.255
  secondary      false
 ...
 rx-packets              122120
```

```
rx-octets               25293100
rx-errors               0
rx-drops                1403
tx-packets              117618
tx-octets               24737443
tx-errors               0
tx-drops                0
rx-pps                  13
rx-kbps                 36
tx-pps                  13
tx-kbps                 37
rx-arp-requests         325
tx-arp-replies          333
tx-arp-requests         704
rx-arp-replies          683
...
bandwidth-upstream      50000
bandwidth-downstream    50000
```

Operational Commands

show interface detail (see the tx-kbps and bandwidth-upstream fields)

Related Topics

bandwidth-downstream, on page 97

banner login

banner login—Configure banner text to be displayed before the login prompt on a Cisco vEdge device.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► Banner

Command Hierarchy

```
banner
  login "text"
```

Syntax Description

text	Login Banner Text: Text string for the login banner. The string can be from 1 to 2048 characters long. If the string contains spaces, enclose it in quotation marks. To insert a line break, type **\n**. For Cisco IOS XE SD-WAN Release 16.12.1r, to insert a line break, type **\x0a**. From Cisco IOS XE Catalyst SD-WAN Release 17.3.1a onwards, to insert a line break, type **\n** and delimiters like double-quotes ("") are not required in the banner string.

Command History

Release	Modification
14.1	Command introduced.
15.1.1	Changed maximum banner length to 2048 characters.
Cisco IOS XE SD-WAN 16.12.1r	Changed the value for inserting a line break for the banner string.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Changed the value for inserting a line break to **\n** for the banner string.

Example

Set a login banner:

```
vSmart(config)# banner login "vSmart Controller in Data Center 1\n  AUTHORIZED USERS ONLY"
vSmart(config-banner)# commit and-quit
Commit complete.
vSmart# exit
MacBook-Pro:~ me$ ssh 10.0.5.19
vSmart Controller in Data Center 1
     AUTHORIZED USERS ONLY
login:
```

Operational Commands

show running-config

Related Topics

banner motd, on page 102

banner motd

banner motd—Configure banner text to be displayed after a user logs in to a Cisco vEdge device.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► Banner

Command Hierarchy

```
banner
  motd "text"
```

Syntax Description

"text"	Login Banner Text: Text string for the login banner. The string can be from 1 to 2048 characters long. If the string contains spaces, enclose it in quotation marks. To insert a line break, type **\n**. For Cisco IOS XE SD-WAN Release 16.12.1r, to insert a line break, type **\x0a**. From Cisco IOS XE Catalyst SD-WAN Release 17.3.1a onwards, to insert a line break, type **\n** and delimiters like double-quotes ("") are not required in the banner string.

Command History

Release	Modification
14.1 15.1.1	Command introduced. Chnaged maximum banner length to 2048 characters.
Cisco IOS XE SD-WAN 16.12.1r	Changed the value for inserting a line break for the banner string.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Changed the value for inserting a line break to **\n** for the banner string.

Example

Set a post-login banner:

```
vSmart(config)# banner motd "Welcome to vSmart Controller 1"
vSmart(config-banner)# commit and-quit
Commit complete.
vSmart# exit
MacBook-Pro:~ me$ ssh 10.0.5.19
login: admin
password:
Welcome to vSmart Controller 1
admin connected from 10.0.1.1 using  on vSmart
```

Operational Commands

show running-config

Related Topics

banner login, on page 101

best-path

vpn router bgp best-path—Configure how the active BGP path is selected (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn id
  router
    bgp local-as-number
      best-path
        as-path multipath-relax
        compare-router-id
        med (always-compare | deterministic | missing-as-worst)
```

Syntax Description

as-path multipath-relax	Select Routes with BGP Multipath: By default, when you are using BGP multipath, the BGP best path process selects from routes in the same AS to load-balance across multiple paths. If you configure the **as-path multipath-relax** option, the BGP best path process selects from routes in different ASs.
med (**always-compare** | **deterministic** | **missing-as-worst**)	Use the MED to Select the Active BGP Path: Compare the specified multi-exit discriminator (MED) parameter to determine the active path. The MED parameter can be one of: **always-compare**: Always compare MEDs regardless of whether the peer ASs of the compared routes are the same. **deterministic**: Compare MEDs from all routes received from the same AS regardless of when the route was received. **missing-as-worst**: If a path is missing a MED attribute, consider it to be the worst path.

compare-router-id	Use the Router ID to Select the Active BGP Path: Compare the router IDs among BGP paths to determine the active path. The system prefers the router with the lowest router ID. If the received route contains an ORIGINATOR_ID attribute (through iBGP reflection), the system uses that router ID; if the attribute is not present, the system uses the router ID of the peer that route was received from.

Command History

Release	Modification
14.1	Command introduced.

Example

Compare the router IDs among different BGP paths to determine which path will be the active one:

```
vEdge(config-best-path)# show config
vpn 1
 router
bgp 666
   best-path
    compare-router-id
   !
  !
 !
!
```

Operational Commands

show bgp routes

bfd app-route

bfd app-route—Configure Bidirectional Forwarding Protocol timers used by application-aware routing (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BFD

Command Hierarchy

```
bfd app-route
  multiplier number
  poll-interval milliseconds
```

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 History

Release	Modification
14.2	Command introduced.

Example

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

```
vEdge(config)# bfd app-route poll-interval 900000
vEdge(config)# bfd app-route multiplier 4
```

Operational Commands

show app-route stats

show bfd summary

Related Topics

bfd color, on page 106

bfd color

bfd color—Configure the Bidirectional Forwarding Protocol timers used on transport tunnels (on vEdge routers only).

Note BFD is always enabled on vEdge routers. There is no **shutdown** configuration command to disable it.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BFD

Command Hierarchy

```
bfd color color
  hello-interval milliseconds
  multiplier number
  pmtu-discovery
```

Syntax Description

hello-interval *milliseconds*	Hello Packet Interval: For the transport tunnel, how often BFD sends Hello packets. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel. Range: 100 through 300000 milliseconds (5 minutes) Default: 1000 milliseconds (1 second)
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**
multiplier *number*	Multiplier for the Hello Packet Interval: How many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time. For example, with the default Hello packet interval of 1000 milliseconds (1 second) and the default multiplier of 7, if BFD has not received a Hello packet after 7 seconds, it considers that the tunnel has failed and implements its redundancy plan. Range: 1 through 60 Default: 7 (for hardware vEdge routers), 20 (for vEdge Cloud software routers)

pmtu-discovery	Path MTU Discovery: Control BFD path MTU discovery on the transport tunnel. By default, BFD PMTU discovery is enabled, and it is recommended that you do not modify this behavior. With PMTU discovery enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. With PMTU discovery enabled, 16 bytes might be required by PMTU discovery, so the effective tunnel MTU might be as low as 1452 bytes. From an encapsulation point of view, the default IP MTU for GRE is 1468 bytes, and for IPsec it is 1442 bytes because of the larger overhead. Enabling PMTU discovery adds to the overhead of the BFD packets that are sent between the vEdge routers, but does not add any overhead to normal data traffic. If PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes (tunnel MTU of 1500 bytes less 4 bytes for the GRE header, 20 bytes for the outer IP header, and 4 bytes for the MPLS header). However, the effective tunnel MTU might be 1468 bytes, because the software might sometimes erroneously add 4 bytes to the header. **Note** If interface IP MTU is 1500 byte, then Tunnel MTU is 1442 (1500 default interface MTU - 58 bytes for tunnel overhead). When the BFD session is established, Tunnel MTU is set to 1441. Once the BFD is up, Tunnel MTU is lowered by 1 byte. Whereas, when BFD is in down state, Tunnel MTU is 1442. Default: Enabled

Command History

Release	Modification
14.1	Command introduced.
15.1 15.1.1	Added pmtu-discovery option, renamed interval option to hello-interval, and changed Hello interval units from seconds to milliseconds.
15.2	Changed default multiplier from 3 to 7.
15.3.2	Added colors private3, private4, private5, and private6.
16.1	Enabled path MTU discovery by default.
16.2	Added default multiplier for vEdge Cloud routers.
20.5	Changed maximum hello interval from 60 seconds to 5 minutes. Added the sla-damp-multiplier keyword for Cisco vEdge devices.

Example

Change the BFD Hello packet interval for the **lte** tunnel connection to 2 minutes:

```
vEdge# show running-config bfd
bfd color lte
 hello-interval 2000
!
```

Operational Commands

show bfd sessions

show control connections

show app-route stats

Note Note that the default BFD configuration is not displayed when you issue the **show running-config** command. This is because BFD is always enabled on vEdge routers, and there is no **shutdown** configuration command to disable it. However, if you configure additional BFD properties, they are displayed by the **show running-config** command.

Related Topics

bfd app-route, on page 105
encapsulation, on page 202
last-resort-circuit, on page 281
mtu, on page 339
pmtu, on page 378
hello-interval, on page 221
hello-tolerance, on page 225

bfd app-route color

bfd app-route color—Configure the Bidirectional Forwarding Protocol timers used on transport tunnels (on vEdge routers only).

Note BFD is always enabled on vEdge routers. There is no **shutdown** configuration command to disable it.

Cisco vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BFD

Command Hierarchy

```
bfd app-route color <color>
```

Syntax Description

color *color*	Specifies an identifier for the transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider. The following are the color 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 History

Release	Modification
20.5.1	This command is introduced.

Example

```
vvEdge (config)# bfd app-route color public-internet
```

Operational Commands

request sla-dampening-reset color

bgp

vpn router bgp— Configure BGP within a VPN on a vEdge router.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      address-family ipv4-unicast
        aggregate-address prefix/length [as-set] [summary-only]
        maximum-paths paths number
        network prefix/length
       redistribute (connected | nat | natpool-outside | omp | ospf | static) [route-policy
 policy-name]
      best-path
        as-path multipath-relax
        compare-router-id
        med (always-compare | deterministic | missing-as-worst)
      distance
        external number
```

```
    internal number
    local number
  neighbor ip-address
    address-family ipv4-unicast
      maximum-prefixes number [threshold] [restart minutes | warning-only]
      route-policy policy-name (in | out)
    capability-negotiate
    description text
    ebgp-multihop ttl
    next-hop-self
    password md5-digest-string
    remote-as remote-as-number
    send-community
    send-ext-community
    [no] shutdown
    timers
      advertisement-interval number
      connect-retry seconds
      holdtime seconds
      keepalive seconds
    update-source ip-address
  ! end neighbor configuration
  propagate-aspath
  router-id ip-address
  [no] shutdown
  timers
    holdtime seconds
```

Syntax Description

local-as-number	Local AS Number: AS number of the local BGP site. 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 History

Release	Modification
14.1	Command introduced.

Example

Configure BGP in VPN 1:

```
vpn 1
  router
    bgp 123
      address-family ipv4_unicast
      redistribute omp
       neighbor 10.0.19.17
         no shutdown
         remote-as 456
```

Operational Commands

clear bgp neighbor

show bgp neighbor

show bgp routes

show bgp summary

show omp routes detail

bind

vpn 0 interface tunnel-interface bind—Bind a physical WAN interface to a loopback interface.

vManage Feature Template

Configuration ► Templates ► VPN Interface Cellular

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      bind interface-name
```

Syntax Description

interface-name	Interface Name Physical WAN interface to bind to a loopback interface. *interface-name* has the format **ge** *slot*/*port*. Both the loopback and physical WAN interfaces must be in VPN 0.

Command History

Release	Modification
14.2	Command introduced.
Cisco SD-WAN Release 19.2 Cisco IOS XE SD-WAN Release 16.12.1	Added support for Cisco XE SD-WAN routers.

Examples

Example 1

(for Cisco vEdge routers)

Bind the physical interface **ge0/0** to the interface **loopback2**:

```
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  no shutdown
 !
 interface loopback2
  ip address 172.16.15.15/24
  tunnel-interface
   color   metro-ethernet
   carrier carrier1
   bind    ge0/0
  !
  no shutdown
 !
```

Example 2

(for Cisco IOS XE Catalyst SD-WAN devices)

```
Device#show sdwan running-config
sdwan
interface Loopback1
  tunnel-interface
   encapsulation ipsec
   color red
   bind GigabitEthernet1
   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
  exit
exit
```

Operational Commands

show control connections

block-icmp-error

vpn interface nat block-icmp-error—Prevent a vEdge router that is acting as a NAT device from receiving inbound ICMP error messages (on vEdge routers only). By default, such a vEdge router blocks these error messages. Blocking error messages is useful in the face of a DDoS attack.

NAT uses ICMP to relay error messages across a NAT, so if you want to receive these messages, disable the blocking of ICMP error messages.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    nat
      block-icmp-error
```

Syntax Description

None

Command History

Release	Modification
14.2	Command introduced.

Example

Configure a vEdge router acting as a NAT so that it does not block inbound ICMP error messages, to allow the router to receive NAT ICMP relay error messages:

```
vEdge# config
vEdge(config)# vpn 1 interface ge0/4 nat
vEdge(config-nat)# no block-icmp-error
vEdge(config-nat)# show full-configuration
vpn 1
 interface ge0/4
  nat
    no block-icmp-error
  !
 !
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

block-non-source-ip

vpn interface block-non-source-ip—Do not allow an interface to forward traffic if the source IP address of the traffic does not match the inteface's IP prefix range (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    block-non-source-ip
```

Command History

Release	Modification
17.1.1	Command introduced.

Syntax Description

None

Example

Have the router block traffic being sent out the transport interface (in VPN 0) and out one service-side interface (in VPN 1) when the traffic's source IP address does not match the IP address configured on the interface:

```
vpn 0
  interface ge0/0
    block-non-source-ip
    ...
vpn 1
  interface ge1/0
    block-non-source-ip
    ...
```

Operational Commands

show interface

show ip routes

bridge

bridge—Create a bridging domain (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Bridge

Command Hierarchy

```
bridge bridge-id
  age-time seconds
  interface interface-name
    description "text description"
    native-vlan
    [no] shutdown
    static-mac-address mac-address
  max-macs number
  name text
  vlan vlan-id
```

Syntax Description

name *text*	Bridging Domain Description: Text description of the bridging domain. If *text* contains spaces, enclose it in quotation marks.
bridge-id	Bridging Domain Identifier: Number that identifies the bridging domain. Range: 1 through 63

Example

Configure three bridge domains on a vEdge router:

```
vEdge# show running-config bridge
bridge 1
 vlan 1
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/5
  no native-vlan
  no shutdown
 !
 interface ge0/6
  no native-vlan
  no shutdown
 !
!
bridge 2
 vlan 2
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/5
  no native-vlan
  no shutdown
 !
 interface ge0/6
  no native-vlan
  no shutdown
 !
!
```

```
bridge 50
 interface ge0/2
  native-vlan
  no shutdown
 !
 interface ge0/5
  native-vlan
  no shutdown
 !
 interface ge0/6
  native-vlan
  no shutdown
 !
!
vEdge# show bridge interface

                        ADMIN   OPER    ENCAP                RX    RX      TX    TX
BRIDGE  INTERFACE  VLAN STATUS  STATUS  TYPE   IFINDEX  MTU  PKTS  OCTETS  PKTS  OCTETS
-------------------------------------------------------------------------------------
1       ge0/2      1    Up      Up      vlan   34       1500 0     0       2     168
1       ge0/5      1    Up      Up      vlan   36       1500 0     0       2     168
1       ge0/6      1    Up      Up      vlan   38       1500 0     0       2     168
2       ge0/2      2    Up      Up      vlan   40       1500 0     0       3     242
2       ge0/5      2    Up      Up      vlan   42       1500 0     0       3     242
2       ge0/6      2    Up      Up      vlan   44       1500 0     0       3     242
50      ge0/2      -    Up      Up      null   16       1500 0     0       2     140
50      ge0/5      -    Up      Up      null   19       1500 0     0       2     140
50      ge0/6      -    Up      Up      null   20       1500 0     0       2     140
```

Operational Commands

show bridge interface

show bridge mac

show bridge table

Related Topics

interface irb, on page 255

capability-negotiate

vpn router bgp capability-negotiate—Allow the BGP session to learn about the BGP extensions that are supported by the neighbor (on vEdge routers only).

This feature is disabled by default. If you have enabled it, use the **no capability-negotiate** configuration command to disable it.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        capability-negotiate
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Enable BGP capability negotiation:

```
vEdge# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
  bgp 666
   neighbor 1.10.10.10
    no shutdown
    remote-as 777
    capability-negotiate
    !
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

carrier

vpn 0 interface tunnel-interface carrier—Associate a carrier name or private network identifier with a tunnel interface (on vEdge routers, vManage NMSs, and vSmart controllers only).

vManage Feature Template

For vEdge routers, vManage NMSs, and vSmart controllers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      carrier carrier-name
```

Table 4: Syntax Description

v*carrier-name*	Private Network Identifier: Carrier name to associate with a tunnel interface. Values: **carrier1**, **carrier2**, **carrier3**, **carrier4**, **carrier5**, **carrier6**, **carrier7**, **carrier8**, **default** Default: default

Command History

Release	Modification
14.2	Command introduced.

Example

Associate a carrier name with a tunnel connection:

```
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  no shutdown
 !
 interface loopback2
  ip address 172.16.15.15/24
  tunnel-interface
   color   metro-ethernet
   carrier carrier1
   bind    ge0/0
  !
  no shutdown
 !
```

Operational Commands

show control connections

cellular

cellular—Configure a cellular module on a vEdge router (on vEdge routers only).

The firmware installed in the router's cellular modules is specific to each service provider and determines which profile properties you can configure. You can modify the attributes for a profile only if allowed by the service provider.

To associate a cellular profile with a cellular interface, use the interface cellular profile configuration command.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Cellular Profile

Command Hierarchy

```
cellular cellularnumber
  profile number
   apn name
   auth auth-method
   ip-addr ip-address
   name profile-name
   pdn-type type
   primary-dns ip-address
   secondary-dns ip-address
   user-name user-name
   user-pass password
```

Syntax Description

cellular *number*	Cellular Interface Name: Name of the cellular interface. It must be **cellular0**.

Command History

Release	Modification
16.1	Command introduced.

Example

Configure a cellular interface with a profile, and the profile with an APN.

```
vEdge# show running-config cellular
cellular cellular0
 profile 1
  apn reg_ims
 !
```

Operational Commands

clear cellular errors

clear cellular session statistics

show cellular modem

show cellular network

show cellular profiles

show cellular radio

show cellular sessions

show cellular status

show interface

Related Topics

profile, on page 405

cflowd-template

policy cflowd-template—Create a template that defines the location of cflowd collectors, how often sets of sampled flows should be sent to the collectors, and how often the cflowd template should be sent to the collectors (on vSmart controllers only). You can configure a maximum of four cflowd collectors per vEdge router. To have a template take effect, apply it with the appropriate data policy.

You must configure at least one cflowd-template, but it need not contain any parameters. With no parameters, the data flow cache on vEdge nodes is managed using default settings, and no flow export occurs.

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
      source-interface interface-name
    flow-active-timeout seconds
    flow-inactive-timeout seconds
    flow-sampling-interval number
    template-refresh seconds
apply-policy
  site-list list-name
    data-policy policy-name
    cflowd-template template-name
```

Syntax Description

template-name	Template Name: Name of the template. The number of template-name entries is limited to 2048.

Command History

Release	Modification
14.3	Command introduced.

Release	Modification
26.2.1	The number of template-name entries limited to 2048.

Example

Configure a cflowd flow collection template, and apply it to a group of sites in the overlay network:

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233
 flow-active-timeout 60
 flow-inactive-timeout 90
 flow-sampling-interval 64
 template-refresh 120
!
vSmart# show running-config apply-policy
apply-policy
 site-list site-list-for-cflowd
  data-policy     policy-for-cflowd
  cflowd-template test-cflowd-template
 !
!
```

Operational Commands

clear app cflowd flow-all (on vEdge routers only)

clear app cflowd flows (on vEdge routers only)

clear app cflowd statistics (on vEdge routers only)

show running-config policy (on vSmart controllers only)

show app cflowd collector (on vEdge routers only)

show app cflowd flow-count (on vEdge routers only)

show app cflowd flows (on vEdge outers only)

show app cflowd statistics (on vEdge routers only)

show app cflowd template (on vEdge routers only)

show policy from-vsmart (on vEdge routers only)

channel

wlan channel—Specify the radio channel (on vEdge cellular wireless routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi Radio

Command Hierarchy

```
wlan radio-band
  channel (auto | auto-no-dfs) (channel)
```

Syntax Description

(**auto** | **auto-no-dfs**)	Automatic Channel Selection: Have the router automatically select the best channel to use from among all channels or from among all channels except for those with dynamic frequency selection (DFS) capabilities. Airport radar uses frequencies that overlap DFS channels. If you are using a 5-GHz radio band, and if your installation is near an airport, it is recommended that you configure **auto-no-dfs**, to remove DFS channels from the list of available channels. Default: **auto**
channel	Channel for 2.4-GHz WLANs: Use a 2.4-GHz radio band. This band supports IEEE 802.11b, 802.11g, and 802.11n clients. Range: 1 through 13, depending on the country configuration.
channel	Channel for 5-GHz WLANs: Use a 5-GHz radio band. This band supports IEEE 802.11a, 802.11n, and 802.11ac clients. You can configure channels for standard or for DFS capabilities.*Channels available for 5-GHz, including DFS:* 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, and 165, depending on the country configuration

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a 5-GHz channel:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
```

```
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

channel-bandwidth, on page 124

channel-bandwidth

wlan channel-bandwidth—Specify the IEEE 802.11n and 802.11ac channel bandwidth (on vEdge cellular wireless routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi Radio

Command Hierarchy

```
wlan radio-band
  channel-bandwidth megahertz
```

Syntax Description

megahertz	Channel Bandwidth Bandwidth available on the WLAN channel. Values: 20, 40, 80 MHz Default: 20 MHz (for 2.4 GHz); 80 MHz (for 5 GHz)

Example

Explicitly configure the default channel bandwidth for a 5-GHz radio band:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 channel-bandwidth 80
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

channel, on page 122

cipher-suite

vpn interface ipsec ike cipher-suite—Configure the type of authentication and encryption to use during IKE key exchange (on vEdge routers only).

vpn interface ipsec ipsec cipher-suite—Configure the authentication and encryption to use on an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ike
      cipher-suite suite
    ipsec
      cipher-suite suite
```

Syntax Description

suite	Authentication and Encryption Type for IKE Key Exchange: Type of authentication and integrity checking to use during IKE key exchange. It can be one of the following: • **aes128-cbc-sha1**—Use the AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. • **aes128-cbc-sha2**—Use the AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity. • **aes256-cbc-sha1**—Use the AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. This is the default. • **aes256-cbc-sha2**—Use the AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity.
suite	Encryption Type for IPsec Tunnel: Type of encryption to use on an IPsec tunnel that is being used for IKE key exchange. It can be one of the following: • **aes256-cbc-sha1**—Calculate message encryption using the AES-256 cipher in CBC (cipher block chaining) mode and using HMAC-SHA1-96 keyed-hash message authentication. • **aes256-gcm**—Calculate message encryption using the AES-256 algorithm in GCM (Galois/counter mode). This is the default. • **null-sha1**—Do not encrypt the IPsec tunnel that is being used for IKE key exchange traffic.

Command History

Release	Modification
17.2	Command introduced.
18.2	Added support for SHA2-based ciphers for IKE.

Example

Change the IKE key exchange to use AES-128 encryption and HMAC-SHA1:

```
vEdge(config)# vpn 1 interface ipsec1 ike
vEdge(config-ike)# cipher-suite aes128-sha1
```

Change the IPsec tunnel encryption to AES-256 in CBC mode:

```
vEdge(config)# vpn 1 interface ipsec1 ipsec
vEdge(config-ipsec)# cipher-suite aes256-cbc-sha1
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

class-map

policy class-map—Map forwarding classes to output queues (on vEdge routers only). When you are configuring QoS policy, you refer to the forwarding class mappings when you configure a QoS scheduler.

Class mappings can apply to unicast and multicast traffic.

vManage Feature Template

For vEdge routers:

Configuration ► Policies ► Localized Policy

Command Hierarchy

```
policy
  class-map
    class class-name queue number
```

Syntax Description

class *class-name* **queue** *number*	Class Mapping to Output Queue: Map a class name to an interface queue number. The class name can be a text string from 1 to 32 characters long. On hardware vEdge routers and Cloud vEdge virtualized routers, each interface has eight queues, numbered from 0 through 7. Queues 1 through 7 are available for data traffic, and the default scheduling method for these seven queues is weighted round-robin (WRR). Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ). For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ; 100 percent of control traffic is transmitted. In Releases 17.2 and earlier, on Cloud vEdge virtualized routers, each interface has four queues, numbered from 0 through 3. Queue 0 is reserved for control traffic, and queues 1, 2, and 3 are available for data traffic. The scheduling method for all four queues is WRR. LLQ is not supported. The number of class entries is limited to 64.

Command History

Release	Modification
14.1 14.2 16.3 17.2.2	Command introduced. Changed the LLQ queue from queue 1 to queue 0. The software supports only one queue for LLQ, and it must be queue 0. Added support for multicast traffic and for vEdge Cloud routers. vEdge Cloud routers support eight queues, with queue 0 reserved for LLQ
26.2.1	The number of class entries limited to 64.

Example

Map forwarding classes:

```
vEdge# show running-config policy class-map
policy
 class-map
  class be queue 2
  class af1 queue 3
  class af2 queue 4
  class af3 queue 5
 !
!
```

Related Topics

access-list, on page 30
cloud-qos, on page 130
rewrite-rule, on page 427

clear-dont-fragment

vpn interface clear-dont-fragment—Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface (on vEdge routers only). When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Note **vpn interface 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.

By default, the clearing of the DF bit is disabled.

vManage Feature Template

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    clear-dont-fragment
```

Syntax Description None

Example

Clear the DF bit in IPv4 packets being sent out an interface:

```
vpn 0
  interface ge0/0
    clear-dont-fragment
```

Operational Commands

show interface detail

Related Topics

mtu, on page 339
pmtu, on page 378

clock

Set the timezone to use on the local device.

vManage Feature Template

For all Cisco SD-WAN devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  clock
    timezone timezone
```

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). *timezone* has the format *area*/*location*. *area* is the name of a continent (Africa, America, Antarctica, Asia, Australia, or Europe), an ocean (Arctic, Atlantic, Indian, or Pacific), or Etc (such as Etc/UTC and Etc/GMT). *location* is the name of a specific location within the area, usually a city or small island. For more information, see the IANA Time Zone Database. Default: UTC

Examples

California time zone

California time:

```
vm6# show running-config system
system
  clock timezone America/Los_Angeles
```

Command History

Release	Modification
14.1	Command introduced.
15.2	Support for the IANA timezone database added .

Related Commands

clock set date

clock set time

show system status

cloud-qos

policy cloud-qos—Enable QoS scheduling and shaping for traffic on WAN interfaces (applicable to Cisco vEdge Cloud, Cisco vEdge 5000, and Cisco ISR1100 routers).

vManage Feature Template

For vEdge routers:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Cloud QoS**

Command Hierarchy

```
policy
  cloud-qos
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Enable QoS scheduling and shaping to the transport-side tunnel interface in VPN 0 and to a service-side interface in VPN 1, configure ACLs for QoS, and apply the policy to the two router interfaces:

```
vEdgeCloud# show running-config policy
policy
  cloud-qos
  cloud-qos-service-side
  class-map
    class class0 queue 0
    class class16 queue 0
    class class1 queue 1
    class class17 queue 1
    class class2 queue 2
    class class22 queue 2
    class class3 queue 3
    class class31 queue 3
  rewrite-rule rewrite rewrite-all-dscps
    class class0 low dscp 63
    class class1 low dscp 62
    class class16 low dscp 47
    class class2 low dscp 61
    class class22 low dscp 41
    class class3 low dscp 60
    class class31 low dscp 32
  rewrite-rule rewrite-to-0
    class class16 low dscp 0
    class class22 low dscp 0
    class class31 low dscp 0
  access-list acl-match-class
    sequence 16
      match
        class16
      action accept
        class class31
    sequence 22
      match
        class22
      action accept
        class class31
    sequence 31
      match
        class31
      action accept
        class class31
    default-action accept
  access-list acl-match-class-action-drop
    sequence 16
      match
        class16
      action drop
    sequence 22
      match
```

```
        class22
      action drop
    sequence 31
      match
        class31
      action drop
    default-action accept
  access-list acl-match-dscp
    sequence 0
      match
        dscp 0
      action accept
        count counter-dscp-0
        class class0
    sequence 1
      match
        dscp 1
      action accept
        count counter-dscp-1
        class class1
    default-action accept

vEdgeCloud# show running-config vpn 0
vpn 0
  interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
    color lte
    encap ipsec
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no-allow-service sshd
    no-allow-service ntp
    no allow-service stun
  no shutdown
  access-list acl-match-dscp in
  rewrite-rule rewrite-all-dscps

vEdgeCloud# show running-config vpn 1
vpn 1
  interface ge1/0
  ip address 10.2.2.11/24
  no shutdown
  access-list acl-match-dscp-action-drop in
  rewrite-rule rewrite-to-0
```

Related Topics

access-list, on page 30
class-map, on page 127
cloud-qos-service-side, on page 132
rewrite-rule, on page 427

cloud-qos-service-side

policy cloud-qos-service-side—Use this command along with the `policy cloud-qos` command to enable QoS scheduling and shaping for traffic on LAN interfaces (applicable to Cisco vEdge Cloud, Cisco vEdge 5000, and Cisco ISR1100 routers).

vManage Feature Template

For Cisco vEdge devices:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Cloud QoS Service Side**

Command Hierarchy

```
policy
   cloud-qos-service-side
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Enable QoS scheduling and shaping to the transport-side tunnel interface in VPN 0 and to a service-side interface in VPN 1, configure ACLs for QoS, and apply the policy to the two router interfaces:

```
vEdgeCloud# show running-config policy
policy
  cloud-qos
  cloud-qos-service-side
  class-map
    class class0 queue 0
    class class16 queue 0
    class class1 queue 1
    class class17 queue 1
    class class2 queue 2
    class class22 queue 2
    class class3 queue 3
    class class31 queue 3
  rewrite-rule rewrite rewrite-all-dscps
    class class0 low dscp 63
    class class1 low dscp 62
    class class16 low dscp 47
    class class2 low dscp 61
    class class22 low dscp 41
    class class3 low dscp 60
    class class31 low dscp 32
  rewrite-rule rewrite-to-0
    class class16 low dscp 0
    class class22 low dscp 0
    class class31 low dscp 0
  access-list acl-match-class
    sequence 16
      match
        class16
      action accept
        class class31
    sequence 22
      match
        class22
      action accept
```

```
        class class31
    sequence 31
      match
        class31
      action accept
        class class31
    default-action accept
  access-list acl-match-class-action-drop
    sequence 16
      match
        class16
      action drop
    sequence 22
      match
        class22
      action drop
    sequence 31
      match
        class31
      action drop
    default-action accept
  access-list acl-match-dscp
    sequence 0
      match
        dscp 0
      action accept
        count counter-dscp-0
        class class0
    sequence 1
      match
        dscp 1
      action accept
        count counter-dscp-1
        class class1
    default-action accept

vEdgeCloud# show running-config vpn 0
vpn 0
  interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
    color lte
    encap ipsec
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no-allow-service sshd
    no-allow-service ntp
    no allow-service stun
  no shutdown
  access-list acl-match-dscp in
  rewrite-rule rewrite-all-dscps

vEdgeCloud# show running-config vpn 1
vpn 1
  interface ge1/0
  ip address 10.2.2.11/24
  no shutdown
  access-list acl-match-dscp-action-drop in
  rewrite-rule rewrite-to-0
```

Related Topics

access-list, on page 30

class-map, on page 127
cloud-qos, on page 130
rewrite-rule, on page 427

cloudexpress

vpn cloudexpress—Configure Cloud OnRamp for SaaS (formerly called CloudExpress service) in a VPN (on vEdge routers only).

Note To ensure that CloudExpress service is set up properly, configure it in vManage NMS, not using the CLI.

Command Hierarchy

```
vpn vpn-id
  cloudexpress
    allow-local-exit
    applications application-names
    local-interface-list interface-names
    node-type type
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Configure Cloud OnRamp for SaaS in VPN 100:

```
vEdge# show running-config vpn 100 cloudexpress
vpn 100
 cloudexpress
  node-type            client
  allow-local-exit
  local-interface-list ge0/0 ge0/2
  applications         salesforce office365 amazon_aws oracle sap box_net dropbox jira intuit concur zendesk gotomeeting webex
 google_apps
 !
!
```

Operational Commands

clear cloudexpress computations

show cloudexpress applications

show cloudexpress gateway-exits

show cloudexpress local-exits

show omp cloudexpress

show running-config vpn cloudexpress

collector

policy cflowd-template collector—Configure the address of a cflowd collector (on vSmart controllers only). The Cisco SD-WAN software can export flows to a maximum of four collectors. Note that if one or more vManage NMSs are present in the overlay network, the collected flows are also sent to the NMSs. (The NMSs are not counted in the maximum number of collectors.) Configuring a cflowd collector is optional.

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
      source-interface interface-name
```

Syntax Description

address *ip-address* **port** *port number*	Address and Port of the Collector: IP address of the collector and port number to use. The default collector port is 4739.
source-interface *interface-name*	Interface to Reach Collector: Interface to use to send flows to the collector. *interface-name* can be a Gigabit Ethernet or 10-Gigabit Ethernet interface (**ge**) or a loopback interface (**loopback** *number*).
transport *transport-type*	Transport Protocol Transport protocol used to reach the collector. *transport-type* can be **transport_tcp** or **transport_udp**.
vpn *vpn-id*	VPN: Number of the VPN in which the collector is located.

Command History

Release	Modification
14.3	Command introduced.
16.2.2	Added source-interface option.

Example

Configure a cflowd template:

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233 transport transport_udp
 flow-active-timeout 60
 flow-inactive-timeout 90
 template-refresh 120
!
```

Operational Commands

show running-config policy (on vSmart controllers only)

show app cflowd collector (on vEdge routers only)

show app cflowd template (on vEdge routers only)

color

vpn 0 interface tunnel-interface color—Identify an individual WAN transport tunnel (on vEdge routers only). In the Cisco SD-WAN software, the tunnel is identified by a color. The color is one of the TLOC parameters associated with the tunnel.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      color color [restrict]
```

Syntax Description

color *color*	Color: Identify an individual WAN transport tunnel by assigning it a color. The color is one of the TLOC parameters associated with the tunnel. (While the CLI on a vSmart controller allows you to configure a color, the color has no meaning because vSmart controllers have no TLOCs.) On a vEdge router, 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 vEdge router 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** Default: **default**
color *color* **restrict**	Restrict WAN Transport Tunnel: Allow the local WAN transport tunnel to be created and a BFD session for the tunnel to established to the remote vEdge router only if a tunnel of the same color exists on the remote router. If, for a tunnel, you change the color only, the **restrict** option remains configured. To remove the restriction on a color, first issue the **no color** command and then configure the new color.

Command History

Release	Modification
14.1	Command introduced.
15.1	Added restrict option.
15.2	Added colors private3, private4, private5, and private6.
15.2	Supporeted application of restrict option to any color.

Example

On a vEdge router, configure two tunnel interfaces (two TLOCs). The tunnel on **ge0/1** connects to a public WAN, and the tunnel on **ge0/2** connects to a private MPLS network. BFD sessions on the tunnel on interface **ge0/2** are established only to other TLOCs on other vEdge routers whose color is also **mpls**. The **no control-connections** command disables attempts to establish control connections over the MPLS network.

```
vpn 0
  interface ge0/1
    ip address 172.16.31.3/24
    tunnel-interface
      encapsulation ipsec
      color biz-internet
```

```
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service ntp
      no allow-service stun
      !
    no shutdown
    !
  interface ge0/2
    ip address 10.10.23.3/24
    tunnel-interface
      encapsulation ipsec
      color mpls restrict
      no control-connections
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service ntp
      no allow-service stun
      !
    no shutdown
    !
  !
!
```

Operational Commands

show control connections

show omp tlocs

Related Topics

encapsulation, on page 202

community

snmp community—Define an SNMP community (on vEdge routers and vSmart controllers only).

vManage Feature Template

For vEdge routers and vSmart controllers only:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  community name
    authorization read-only
    view string
```

Syntax Description

authorization read-only	Authorization Level: Set the access authorization level for SNMP Get, GetNext, and GetBulk requests. The MIBs supported by the Cisco SD-WAN software do not allow write operations, so you can configure only read-only authorization (which is the default authorization).
community *name*	Community String: Define the name an SNMP community, which authorizes SNMP clients based on the source IP address of incoming packets. The community name can be a maximum of 32 characters. If it includes spaces, enclose it in quotation marks (" "). The name can include angle brackets (< and >).
view *string*	Specify the MIB Objects an SNMP Manager Can Access: Configure the view, or MIB objects, that the SNMP manager can access for this community. You define the view name with the **snmp view** configuration command. The view name can be a maximum of 255 characters. If it includes spaces, enclose the name in quotation marks (" ").

Command History

Release	Modification
14.1	Command introduced.
16.3	Allowed angle brackets in the community string.

Example

Configure the **public** community to be read-only:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# snmp community public
vEdge(config-community-public)# authorization read-only
vEdge(config-community-public)# show config
snmp
 community public
  authorization read-only
 !
!
vEdge(config-community-public)#
```

Operational Commands

show running-config snmp

compatible rfc1583

vpn router ospf compatible rfc1583—Calculate the cost of summary routes based on RFC 1583 rather than RFC 2328 (on vEdge routers only). By default, calculation is done per RFC 1583.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      compatible rfc1583
```

Syntax Description

no compatible rfc1583	RFC 2328 Compliance: Per RFC 1583, RFC 1583 compliance is enabled by default, and no configuration is necessary. To calculate the cost of OSPF summary routes based on RFC 2328, include the **no compatible rfc1583** configuration command.

Command History

Release	Modification
14.1	Command introduced.

Example

Check that RFC 1583 compliance is the default:

```
vm1# show running-config vpn 1 router ospf area 0
vpn 1
 router
  ospf
   area 0
    interface ge0/0
    exit
   exit
  !
 !
!
vm1# show ospf process | include rfc1583
 rfc1583-compatible    true
```

Enable RFC 2328 compliance:

```
vm1# config
Entering configuration mode terminal
vm1(config)# vpn 1 router ospf
vm1(config-ospf)# no compatible rfc1583
vm1(config-ospf)# show config
vpn 1
router
  ospf
   no compatible rfc1583
  !
!
```

```
!
vm1# show ospf process | include rfc1583
rfc1583-compatible    false
vm1#
```

Operational Commands

show ospf process

connections-limit

vpn 0 interface tunnel-interface connections-limit—Configure the maximum number of HTTPS connections that can be established to a vManage application server (on vManage NMSs only).

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      connections-limit number
```

Syntax Descriptions

number	Number of HTTPS Connections: Set the maximum number of HTTPS connections to a vManage application server. Range: 1 through 512 Default: 50

Command History

Release	Modification
16.1.1	Command introduced.

Example

Configure the maximum number of HTTPS connections that a vManage NMS server accepts to 25:

```
vManage# show running-config vpn 0
vpn 0
 host my ip 10.0.1.1
 interface eth0
  ip dhcp-client
  no shutdown
 !
 interface eth1
  tunnel-interface
   connections-limit 25
```

```
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  shutdown
 !
!
```

Operational Commands

show control connections

show omp tlocs and show omp tlocs detail (see display the configured preference and weight values)

Related Topics

allow-service, on page 63

console-baud-rate

system console-baud-rate—Change the baud rate of the console connection on a vEdge router (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  console-baud-rate rate
```

Syntax Description

rate *rate*	Baud Rate: Set 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 Default: 115200

Command History

Release	Modification
14.2	Command introduced.

Example

Change the console baud rate to 57600:

```
system
  console-baud-rate 57600
```

Operational Commands

show running-config system

contact

snmp contact—Configure the name of a network management contact person for this vEdge device.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  contact string
```

Syntax Description

string	Name of Contact: Name of the contact person in charge of managing the Cisco vEdge device. The string can be a maximum of 255 characters. If it contains spaces, enclose the string in quotation marks (" ").

Command History

Release	Modification
14.1	Command introduced.

Example

Configure the name and phone number of the contact person:

```
vEdge(config)# snmp contact "Eve Lynn, 408-702-1234"
```

Operational Commands

show running-config snmp

container

The support for vContainer Host is deferred. For more information, refer to deferral notice.

Related Topics

ip address-list, on page 260

control

security control—Configure the protocol to use on control plane connections to a vSmart controller (Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controllers only).

vManage Feature Template

For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controllers only:

Configuration ► Templates ► Security

Synax Description

protocol (**dtls** | **tls**)	Protocol for Control-Plane Connections: Protocol to use for control plane connections. Default: DTLS
tls-port*port-number*	TLS Port Number: For TLS tunnels only, port number to use for TLS control plane connections. Range: 1025 through 65535 Default: 23456

Command History

Release	Modification
14.3	Command introduced.

Operational Commands

show control connections

control-connections

vpn 0 interface tunnel-interface control-connections—Attempt to establish a DTLS or TLS control connection for a TLOC (on vEdge routers only). This is the default behavior.

When a vEdge router has multiple tunnel interfaces and hence multiple TLOCs, the router establishes only a single control connection to the Cisco SD-WAN Manager. The router chooses a TLOC at random for this control connection, selecting one that is operational (that is, one whose administrative status is up). If the chosen TLOC becomes non-operational, the router chooses another one.

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).

Note The interface marked as "last-resort" or admin down is skipped when calculating the number of control connections and partial status is determined based on the other tlocs which are UP. Since the last resort is expected to be down, it is skipped while calculating the partial connection status. Same is the case with admin down interfaces when a particular interface is configured as shutdown.

For example, when LTE transport is configured as a last resort circuit, and if the Edge device has 3 tlocs in total including the one with LTE interface, then the device reports partial on 2(4) control connection status.

Starting in Release 15.4, this command is deprecated. Use the max-control-connections command instead.

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      [no] control-connections
```

Table 5: Syntax Description

no control-connections	Do Not Establish a Control Connection for a TLOC: Do not attempt to establish a control connection for a TLOC. You can configure this option only on a vEdge router that has multiple TLOCs. One of the TLOCs must attempt to establish a DTLS or TLS control connection so that the router learns overlay network routing information from the Cisco Catalyst SD-WAN Controllers. This routing information is shared across all the TLOCs on the router.

Command History

Release	Modification
15.1	Command introduced.
15.3.3	Supported a vEdge router establishes only one control connection to Cisco SD-WAN Manager.
15.4	This command is deprecated. Use the max-control-connections command instead.

Example

On a vEdge router, configure two tunnel interfaces (two TLOCs). The tunnel on ge0/1 connects to a public WAN, and the tunnel on ge0/2 connects to a private MPLS network. The router establishes a control connection over ge0/1. The **no control-connections** command on ge0/2 disables attempts to establish control connections over the MPLS network.

```
vpn 0
  interface ge0/1
    ip address 172.16.31.3/24
    tunnel-interface
      encapsulation ipsec
      color biz-internet
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service ntp
      no allow-service stun
      !
    no shutdown
    !
  interface ge0/2
    ip address 10.10.23.3/24
    tunnel-interface
      encapsulation ipsec
      color mpls restrict
      no control-connections
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service ntp
      no allow-service stun
      !
    no shutdown
    !
  !
!
```

Operational Commands

show control connections

control-direction

vpn interface dot1x control-direction—Configure how the 802.1x interface sends packets to and receive packets from unauthorized clients (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      control-direction (in-and-out | in-only)
```

Syntax Description

in-and-out	Send and Receive Packets: Set the 802.1x interface to send packets to and receive packets from unauthorized clients. Bidirectionality is the default behavior.
in-only	Send Packets Only: Set the 802.1x interface to send packets to unauthorized clients, but not to receive them.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure an 802.1x interface to send packets to but not receive packets from unauthorized clients:

```
vEdge# show running-config vpn 0 interface ge0/7
vpn 0
  interface ge0/7
    dot1x
      control-direction in-only
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

control-policy

policy control-policy—Configure or apply a centralized control policy (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies

Command Hierarchy

Create a Centralized Control Policy

Apply a Centralized Control Policy

Syntax Description

policy-name	Control Policy Name: Name of the control policy to configure or to apply to a site list. *policy-name* can be up to 32 characters long.

Command History

Release	Modification
14.2	Command introduced.

Example

On a vSmart controller, configure a control policy that changes the TLOC address of matching prefixes:

Operational Commands

show policy commands

control-session-pps

system control-session-pps—Police the flow of DTLS control session traffic.

Note The **system control-session-pps** is a no operational command for Cisco IOS XE Catalyst SD-WAN devices.

vManage Feature Template

For all the Cisco vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  control-session-pps rate
```

Syntax Description

rate	Flow Rate Set the maximum rate of DTLS control session traffic, in packets per second (pps). Range: 1 through 65535 pps Default: 300 pps

Command History

Release	Modification
14.2	Command introduced.

Example

Change the maximum control session traffic rate to 250 pps:

```
system
  control-session-pps 250
```

Operational Commands

show running-config system

Related Topics

host-policer-pps, on page 231
icmp-error-pps, on page 232
policer, on page 379

controller-group-id

Configure the identifier of the controller group to which the vSmart controller belongs (on vSmart controllers only).

Command Hierarchy

```
system
  controller-group-id number
```

Syntax Description

number	Controller Group Identifier: Numeric identifier of the controller group to which the vSmart controller belongs. Range: 0 through 100 Default: 0

Command History

Release	Modification
16.1	Command introduced.

Examples

Configure a vSmart controller to be in controller group 1:

```
vSmart(config)# system controller-group-name 1
```

Operational Commands

show control connections

show running-config system

Related Topics

controller-group-list, on page 151
exclude-controller-group-list, on page 207
max-control-connections, on page 329
max-omp-sessions, on page 334

controller-group-list

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 vSmart Controllers that are in the same controller group. To delete the control connections from the Cisco vSmart 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 vSmart Controller groups to which a router belongs. You configure this identifier on the Cisco vSmart 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 History

Release	Modification
16.1	Command introduced.

The following example allows a router to establish control connections to the Cisco vSmart Controllers in groups 1 and 2:

```
vEdge(config)# system controller-group-list 1 2
vEdge(config)# commit and-quit
vEdge# show control connections
                                                                                PEER                    PEER
                                      CONTROLLER
PEER     PEER     PEER              SITE        DOMAIN      PEER              PRIVATE  PEER              PUBLIC
                                       GROUP
TYPE     PROTOCOL SYSTEM IP         ID          ID          PRIVATE IP        PORT     PUBLIC IP         PORT    LOCAL COLOR
      STATE           UPTIME           ID
------------------------------------------------------------------------------------------------------------------------------
vsmart   dtls     172.16.255.19     100         1           10.0.5.19         12446    10.0.5.19         12446   lte
       up                 0:00:01:56 1
vsmart   dtls     172.16.255.20     200         1           10.0.12.20        12446    10.0.12.20        12446   lte
       up                 0:00:17:34 2
```

For information on Cisco IOS XE **controller-group-list** command, see controller-group-list in the Cisco IOS XE SD-WAN Qualified Command Reference.

Operational Commands

show control affinity config

show control affinity status

show control connections

show control local-properties

Related Topics

controller-group-id, on page 150
exclude-controller-group-list, on page 207
max-control-connections, on page 329
max-omp-sessions, on page 334

controller-send-path-limit

To set the number of OMP routes that a Cisco Catalyst SD-WAN Controller can send to other Cisco Catalyst SD-WAN Controllers, use the **controller-send-path-limit** command in OMP configuration mode. To set the send path limit to default, use the **no** form of this command.

controller-send-path-limit *routes*
no controller-send-path-limit

Syntax Description

routes	Specifies the number of OMP routes that Cisco Catalyst SD-WAN Controllers can send to other Cisco Catalyst SD-WAN Controllers. Range: 4 to 128.

Command Default

None

Command Modes OMP configuration (config-omp)

Command History

Release	Modification
Cisco SD-WAN Release 20.5.1	This command was introduced.

Usage Guidelines

- It is recommended to set the route limit to default for full network visibility across controllers. This ensures that all available routes are exchanged, subject to a maximum limit of 128.
- Ensure that the OMP **send-path-limit** is set to a value equal to or greater than the number of TLOCs used for any advertised prefix.

Example

The following example shows how to set 100 as the limit for the number of routes Cisco Catalyst SD-WAN Controllers can send.

```
Device(config)# omp
Device(config-omp)# controller-send-path-limit 100
```

cost

Configure the cost of an OSPF interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          cost number
```

Syntax Description

number	Cost of the interface. Range: 1 through 65535

Command History

Release	Modification
14.1	Command introduced.

Example

Set the interface cost to be 20:

```
vEdge# show running-config vpn 1 router ospf area 0
vpn 1
 router
  ospf
   area 0
    interface ge0/0
      cost 20
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

country

Configure the country in which the vEdge WLAN router is installed (on vEdge cellular wireless routers only). Setting the country is mandatory. This configuration ensures that the router complies to local regulatory requirements, enforcing country-specific allowable channels, allowed users, and maximum power levels for the various frequency levels.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi Radio

Command Hierarchy

```
wlan radio-band
  country country
```

Syntax Description

country	Country in which the WLAN vEdge router is installed. Values: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Norway, Pakistan, Panama, Philippines, Poland, Portugal, Puerto Rico, Romania, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Kingdom, United States, Vietnam Default: United States

Example

Set the country to Canada:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 country canada
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Command History

Release	Modification
16.3	Command introduced.

Operational Commands

clear wlan radius-stats

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

channel, on page 122
channel-bandwidth, on page 124
radius, on page 407

cpu-usage

To configure the CPU-usage watermarks, use the **cpu-usage** command in the alarms configuration mode. To revert to the default watermark values, use the **no** form of this command.

cpu-usage [**high-watermark-percentage** *percentage*] [**medium-watermark-percentage** *percentage*] [**low-watermark-percentage** *percentage*] [**interval** *seconds*]

no cpu-usage

Syntax Description

high-watermark-percentage*percentage*	Specifies the high-usage watermark percentage. Range: 1 to 100 percent Default: 90 percent
medium-watermark-percentage*percentage*	Specifies the medium-usage watermark percentage. Range: 1 to 100 percent Default: 75 percent
low-watermark-percentage*percentage*	Specifies the low-usage watermark percentage. Range: 1 to 100 percent Default: 60 percent
interval*seconds*	Specifies how frequently CPU usage should be checked and reported by the device to Cisco vManage. Range: 1 to 4294967295 seconds Default: 5 seconds

Command Default

The default usage watermarks and polling interval are:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples

The following example shows a sample configuration of the CPU-usage watermarks and the polling interval:

```
config
 system
  alarms
   cpu-usage
    high-watermark-percentage 80
    medium-watermark-percentage 70
    low-watermark-percentage 50
    interval 10
```

Related Commands

Command	Description
alarms	Enters the alarms configuration mode.

crypto pki trustpoint

To declare the trustpoint that a 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*

no crypto pki trustpoint *name*

Syntax Description

name	Creates a name for the trustpoint. The name should be same for trustpoint and rsakeypair. (If you previously declared the trustpoint and want to update the characteristics, specify the name you previously created.)

Command Default

No default behavior or values.

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco SD-WAN Release 20.1.1	This command was introduced.

Usage Guidelines

Declaring Trustpoints

Use the **crypto pki trustpoint** command to declare a trustpoint, which can be a root certificate authority (CA) or a subordinate CA. Issuing the **crypto pki trustpoint** command enables the ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint using the following subcommands:

- (Mandatory) **enrollment url**: Specifies the enrollment url that can reach the CA server.
- (Mandatory) **subject-name cn**: Specifies the subject name configuration, which is sent as part of Certificate Signing Request (CSR).
- (Mandatory) **fingerprint**: Specifies the CA certificate fingerprint.
- (Mandatory) **rsakeypair label keysize**: Specifies the RSA key-pair to be used and the keysize. The keypair label should be same as the trustpoint label.
- (Mandatory) **auto-enroll renewal percentage [regenerate]**: By configuring auto-enrollment, the router can request a new certificate at some time before its own certificate (known as its identity or ID certificate) expires. The command states that IOS should perform certificate renewal at exactly the mentioned percentage of the current lifetime of the certificate. It is recommended that the value for renewal percentage should be greater than 50. The keyword, **regenerate** states that IOS should regenerate the RSA key-pair known as shadow key-pair during every certificate renewal operation. The keyword, **regenerate** is optional.
- (Mandatory) **revocation-check type**: To disable revocation checking when the PKI trustpoint policy is being used, configure **revocation-check none**. By default, **revocation-check** is enabled.
- (Optional) password: Specifies the password phrase that the CA server expects for successful certificate enrollment.

Example

The following example shows a root CA for automatic certificate renewal configuration:

```
crypto pki trustpoint Root-CA
   enrollment url http://172.16.1.1:80
  password 0 passw0rd $Passw0rd
  subject-name CN=spoke-1.cisco.com,OU=CVO
  fingerprint CC748544A0AB7832935D8CD0214A152E
  rsakeypair Root-CA 2048
  auto-enroll 80
  revocation-check crl
```

Related Commands

Command	Description
show crypto pki trustpoints status	Displays the certificate authentication and enrollment status.

crypto pki authenticate

To authenticate the certification authority (CA) by getting the certificate of the CA, use the **crypto pki authenticate** command in privileged EXEC mode.

crypto pki authenticate *trustpoint name*

Syntax Description

trustpoint name	The name of the trustpoint. The CA certificate with the trustpoint should be in a privacy-enhanced mail (PEM)-formatted file.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco SD-WAN Release 20.1.1	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support on a router.

This command authenticates the CA to the router by obtaining the certificate of the CA that contains the public key of the CA. The CA certificate associates with a trustpoint and it is verified based on the fingerprint configured on the trustpoint.

This command is not saved on the router configuration.

If the CA does not respond by a timeout period after this command is issued, the terminal control is returned so that it remains available. If this scenario happens, you must reenter the command. The CA certificate expiration dates set for beyond the year 2049 are not recognized. If the validity period of the CA certificate is set to expire after the year 2049, the following error message is displayed when authentication with the CA server is attempted:

error retrieving certificate : incomplete chain

If you receive an error message similar to this, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Example

In the following example, the router requests the certificate of CA from a specified enrollment URL. The router compares the fingerprint of the retrieved CA certificate with the fingerprint configured by the CA administrator in the trustpoint configuration. If both the fingerprints match, the CA certificate is installed.

```
Router# crypto pki authenticate Root-CA
Certificate has the following attributes:
       Fingerprint MD5: 755C9485 DDACC0BD B5ED93E6 4E8A7DEB
      Fingerprint SHA1: 4D4380EA 07392044 6A5BF891 938AC610 C0C0AA6D
Trustpoint Fingerprint: 4D4380EA 07392044 6A5BF891 938AC610 C0C0AA6D
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router#
```

Related Commands

Command	Description
show crypto pki trustpoints status	Displays the certificate authentication and enrollment status.
crypto pki trustpoint	Declares the certificate authority that the router should use.

crypto pki enroll

To obtain the certificates of a router from the certificate authority (CA), use the **crypto pki enroll** command in privileged EXEC mode.

crypto pki enroll *name*

Syntax Description

name	The name of the CA. Use the same name as used when declaring the CA using the **crypto pki trustpoint** command.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco SD-WAN Release 20.1.1	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for SCEP configuration. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

The router needs a signed certificate from the CA for each RSA key pair of a router; if you previously generated general-purpose keys, this command obtains the certificate corresponding to the general-purpose RSA key pair.

You can remove existing certificates with the **no crypto pki trustpoint** command.

The **crypto pki enroll** command is not saved in the router configuration.

Note If the router reboots after you issue the **crypto pki enroll** command but before you receive the certificates, ensure that you reissue the command.

Note If you are using a Secure Shell (SSH) service, ensure to set up specific RSA key pairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructures share the same default RSA key pair, a temporary disruption of SSH service can occur. The RSA key pair can become invalid or can change because of the CA system, in which case you cannot log in using SSH. You receive the following error message: "key changed, possible security problem.")

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA.

```
Router# crypto pki enroll Root-CA
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
Router#
```

When later, the router receives the certificate from the CA, it displays the following confirmation message:

```
Router#  Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router #
```

If necessary, the router administrator can verify the displayed fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message appears on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

Requesting certificates for a router with special-usage keys is the same as in the previous example, except that two certificates are returned by the CA. When the router receives the two certificates, the router displays the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
show crypto pki trustpoint	Displays the trustpoints that are configured on the router.

crypto pki import

To import a certificate manually via file system on a device such as bootflash, use the **crypto pki import** command in the privileged EXEC mode.

crypto pki import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto pki trustpoint** command. The certificate file should be in PEM format.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco SD-WAN Release 20.1.1	This command was introduced.

Usage Guidelines For importing a certificate, ensure that a file is available in the bootflash device. The name of the file must be, <trustpoint-name>.crt and must be in PEM format. If you use usage keys (signature and encryption keys), ensure to enter the **crypto pki import** command twice.

Example

The following example shows how to import a certificate using the CA trustpoint, "Root-CA."

```
crypto pki trustpoint
    Root-CA
  crypto pki authenticate Root-CA
  crypto pki enroll Root-CA
  crypto pki import  Root-CA certificate
```

Related Commands

Command	Description
show crypto pki trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of the CA.

custom-eflow

To define scope for eflow detection, use the **custom-eflow** command in policy elephant-flow configuration mode. To disable the configuration, use the **no** form of the command.

custom-eflow [**sequence** *sequence-num*]
no custom-eflow [**sequence** *sequence-num*]

Syntax Description

sequence	Specifies list of sequences.
sequence-num	Specify sequence value. Range: 1 to 255 Default: 1

Command Default

If custom-eflow sequences are not configured, any flow which has more packet rate than elephant-flow-rate-threshold is considered as an elephant flow.

Command Modes

Policy elephant-flow configuration (policy-elephant-flow)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

Usage Guidelines

A maximum of 8 custom-eflow sequences can be configured. If custom-eflow sequences are not configured, any flow which has more packet rate than elephant-flow-rate-threshold is considered as an elephant flow. However, even if a single custom-eflow sequence is configured, only flows matching atleast one of the custom-eflow sequences will be considered as elephant flows.

Examples

The following example shows how to configure custom-eflow sequences using the **custom-eflow** command:

```
vEdge2k(config)# policy
vEdge2k(config-policy)# elephant-flow
vEdge2k(policy-elephant-flow)# enable
vEdge2k(policy-elephant-flow)# custom-eflow
vEdge2k(policy-custom-eflow)# sequence 1
vEdge2k(config-sequence-1)#
```

das

Configure dynamic authorization service (DAS) parameters for use with IEEE 802.1X authentication so that the router can accept change of authentication (CoA) requests from a RADIUS server (on vEdge routers only).

When discussing DAS, the vEdge router (the NAS) is the server and the RADIUS server (or other authentication server) is the client.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      das
        client ip-address
        port port-number
        require-timestamp
        secret-key password
        time-window seconds
        vpn vpn-id
```

Syntax Description

secret-key *Password*	Password: Password that the the RADIUS or other authentication server uses to access the vEdge router 802.1X interface.
port *port-number*	Port Number: UDP port number for the vEdge router to use to listen for CoA requests from the RADIUS server. If you configure DAS on multiple 802.1Z interfaces on a vEdge router, you must configure each interface to use a different UDP port. Range: 1 through 65535 Default: 3799
client *ip-address*	RADIUS Server IP Address: IP address of the RADIUS authentication server or other authentication server from which to accept CoA requests.
require-timestamp	Timestamps: Require the DAS client (which is the RADIUS or other authentication server) to include an event timestamp in all CoA messages. When timestamps are required both the vEdge router and the RADIUS server check that the timestamp in the CoA request is current and within a specific time window (the default time window is 5 minutes). If it is not, the CoA request is discarded. Also, when timestamps are required, a CoA received without a timestamp is discarded immediately. By default, timestamps are not required.
time-window *seconds*	Time Window: How long a CoA request is valid. The time window is applied to CoA requests only if you have configured **require-timestamp**. When you configure timestamps, both the vEdge router and the RADIUS server check that the timestamp in the CoA request is within the time window. If the timestamp is outside this window, the CoA request is discarded. Range: 0 through 1000 seconds Default: 300 seconds (5 minutes)
vpn *vpn-id*	VPN: VPN through which the RADIUS or other authentication server is reachable.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure DAS with a network RADIUS servers to allow the vEdge router to accept CoA requests from that server. This configuration requires timestamps in the CoA requests and extends the valid CoA window to 10 minutes.

```
vEdge(config-das)# show full-configuration
vpn 0
 interface ge0/2
  dot1x
   das
    time-window       600
    require-timestamp
    client            10.1.15.150
    secret-key        $4$L3rwZmsIic8zj4BgLEFXKw==
   !
  !
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

radius, on page 407

data-policy

Configure or apply a centralized data policy based on data packet header fields (on vSmart controllers only).

Command Hierarchy

Create a Centralized Data Policy:

```
policy
  data-policy policy-name
    vpn-list list-name
      default-action action
      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
          packet-length bytes
          plp (high | low)
          protocol number
```

```
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port number
          tcp flag
        action
          cflowd (not available for deep packet inspection)
          count counter-name
          drop
          log
          tcp-optimization
          accept
            nat [pool number] [use-vpn 0] (in Releases 16.2 and earlier, not available for
 deep packet inspection)
            redirect-dns (host | ip-address)
            set
              dscp number
              forwarding-class class
              local-tloc color color [encap encapsulation]
              local-tloc-list color color [encap encapsulation] [restrict]
              next-hop ip-address
              policer policer-name
              service service-name local [restrict] [vpn vpn-id]
              service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
              tloc ip-address color color [encap encapsulation]
              tloc-list list-name
              vpn vpn-id
```

Apply a Centralized Data Policy:

```
apply-policy
  site-list list-name data-policy policy-name (all | from-service | from-tunnel)
  cflowd-template template-name
apply-policy
  site-list list-name vpn-membership policy-name
```

Syntax Description

policy-name	Data Policy Name: Name of the localized data policy to configure or to apply to a list of sites in the overlay network. The number of policy-name entries is limited to 4096. Maximum characters: 32

Command History

Release	Modification
14.1	Command introduced.
26.2.1	The number of policy-name entries limited to 4096.

Example

Configure and apply a simple data policy

```
vSmart# show running-config policy
policy
 data-policy test-data-policy
```

```
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 172.16.0.0/24
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
  site-list test-site-list
   site-id 500
  !
 !
!
vSmart# show running-config apply-policy
apply-policy
 site-list test-site-list
  data-policy test-data-policy
 !
!
```

Verify the data policy

Immediately after we activate the configuration on the vSmar controller, it pushes the policy configuration to the vEdge routers in site 500. One of these routers is vEdge5, where we see that the policy has been received:

```
vEdge5# show omp data-policy
policy-from-vsmart
 data-policy test-data-policy
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 172.16.0.0/24
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
 !
!
```

Operational Commands

show policy data-policy-filter

show policy from-vsmart

show running-config policy

Related Topics

vpn-membership, on page 541

data-security

Configure the Wi-Fi protected access (WPA) and WPA2 data protection and network access control to use for an IEEE 802.11i wireless LAN (on vEdge cellular wireless routers only).

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.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  interface vap number
    data-security 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 History

Release	Modification
16.3	Command introduced.

Example

Configure data security on VAP interfaces 1, 2, and 3:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
```

```
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

mgmt-security, on page 337
radius, on page 407
radius-servers, on page 411
wpa-personal-key, on page 549

dead-interval

Set the interval during which at least one OSPF hello packet must be received from a neighbor before declaring that neighbor to be down (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          dead-interval seconds
```

seconds	Dead Interval: Time interval during which the vEdge router must receive an OSPF hello packet from its neighbor. If no packet is received, the vEdge router assumes that the neighbor is down. The default dead interval of 40 seconds is four times the default hello interval of 10 seconds. Range: 1 through 65535 seconds Default: 40 seconds

Command History

Release	Modification
14.1	Command introduced.

Example

Set the OSPF dead interval to 30 seconds:

```
vEdge# show running-config vpn 1 router ospf area 0
vpn 1
 router
ospf
   area 0
    interface ge0/0
      dead-interval 30
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

Related Topics

hello-interval, on page 224

dead-peer-detection

Configure the parameters for detecting unreachable IKE peers through an IPsec tunnel (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    dead-peer-detection interval seconds [retries number]
```

Syntax Description

interval *seconds*	Liveness Detection Interval: How often to send an IKE Hello packet to determine whether the IKE peer is alive and reachable. The IKE peer responds to the Hello packet by sending an acknowledgement (ACK) packet to the vEdge router. Range: 0 - 30 seconds Default: 10 seconds
retries *number*	Maximum Number of Retries: How many unacknowledged IKE Hello packets to send before declaring the IKE peer to be dead. Range: 0 - 255 Default: 3

Command History

Release	Modification
17.2	Command introduced.

Example

Change the liveness detection interval to 30 seconds and the number of retries to 10:

```
vEdge(config)# vpn 1 interface ipsec1
vEdge(config-interface-ipsec1)# dead-peer-detection 30 retries 10
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

default-action

Configure the default action to take when the match portion of a policy is not met (on vEdge routers and vSmart controllers only).

vManage Feature Template

For vEdge routers and vSmart controllers:

Configuration ► Policies

Configuration ► Security (for zone-based firewall policy)

Command Hierarchy

For Application-Aware Routing

```
policy
  app-route-policy policy-name
    default-action
      sla-class sla-class-name
```

For Centralized Control Policy

```
policy
  control-policy policy-name
    default-action action
```

For Centralized Data Policy

```
policy
  data-policy policy-name
    default-action action
```

For Localized Control Policy

```
policy
  route-policy policy-name
    default-action action
```

For Localized Data Policy

```
policy
  access-list acl-name
    sequence number
      default-action action
```

For Zone-Based Firewalls

Configure on vEdge routers only.

```
policy
  zone-based-policy policy-name
    default-action action
```

Syntax Description

default-action sla-class *sla-class-name*	Default Action for Application-Aware Routing: Default SLA to apply if a data packet being evaluated by the policy matches none of the match conditions. If you configure no default action, all data packets are accepted and no SLA is applied to them.

policy control-policy *policy-name* **default-action** (**accept**|**reject**) **policy route-policy** *policy-name* **default-action** (**accept** | **reject**) **policy data-policy** *policy-name* **default-action** (**accept** | **drop**) **policy vpn-membership** *policy-name* **default-action** (**accept** | **drop**) **policy access-list** *acl-name* **default-action** (**accept** | **drop**)	Default Action for Control Policy and Data Policy: Default action to take if an item being evaluated by a policy matches none of the match conditions. If you configure no policy (specifically, if you configure no match–action sequences within a policy), the default action, by default, is to accept all items. If you configure a policy with one or more match–action sequences, the default action, by default, is to either reject or drop the item, depending on the policy type.
default-action (**drop** | **inspect** | **pass**)	Default Action for Zone-Base Firewall Policy Default action to take if a data traffic flow matches none of the match conditions. **drop** discards the data traffic. **inspect** inspects the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. **pass** allows the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

Command History

Release	Modification
14.1	Command introduced.
14.2	Add application-aware routing.
18.2	Add zone-based firewall policy.

Example

Create a centralized control policy that changes the TLOC for accepted packets:

```
policy
  control-policy change-tloc
    default-action accept
    sequence 10
      action accept
      tloc 1.1.1.2
```

Operational Commands

show running-config policy

default-information originate

Generate a default external route into an OSPF routing domain (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      default-information
        originate (always | metric metric | metric-type type)
```

Syntax Description

originate metric-type type 1	Advertise Type 1 External Routes: Advertise the default route as an OSPF Type 1 external route.
originate metric-type type 2	Advertise Type 2 External Routes: Advertise the default route as an OSPF Type 2 external route.
originate always	Always Advertise the Default Route: Always advertise the default route in an OSPF routing domain.
originate metric *metric*	Assign a Metric to the Default Route Set the metric to use to generate the default route. Range: 0 through 16777214

Command History

Release	Modification
14.1	Command introduced.
17.1	Remove default value for **originate metric**

Example

Always advertise the default route:

```
vEdge(config-ospf)# default-information originate always
vEdge(config-ospf)# show configuration
vpn 1
 router
  ospf
```

```
   default-information originate always
  !
 !
!
```

When default-information originate is configured on a vEdge router, the source route checking is not performed, and hence the DN-bit is not set. You can configure OMP to OSPF router redistribution for default route, if DN-bit is required:

```
policy
lists
  prefix-list DEFAULT_ROUTE
   ip-prefix 0.0.0.0/0
!
route-policy OMP2OSPF
sequence 10
   match
    address DEFAULT_ROUTE
   action accept
   !
  !
  default-action reject
!
vpn 1
router
  ospf
   default-information originate
   redistribute omp route-policy OMP2OSPF
!
```

Operational Commands

show ospf routes

default-vlan

Configure the VLAN for 802.1X–compliant clients that are successfully authenticated by the RADIUS server (on vEdge routers only).

If you do not configure a default VLAN on the vEdge router, successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      default-vlan vlan-id
```

Syntax Description

vlan-id	VLAN Identifier: Identifier of the VLAN for 802.1X–compliant clients that are successfully authenticated by the RADIUS server.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a default VLAN:

```
bridge 10
 name Authorize_VLAN
 vlan 10
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
vpn 0
 interface ge0/5
  dot1x
   default-vlan     10
  !
  no shutdown
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

auth-fail-vlan, on page 81
auth-reject-vlan, on page 87
bridge, on page 115
guest-vlan, on page 220
radius, on page 407

description

Configure a text description for a parameter or property.

vManage Feature Template

For all Cisco vEdge devices:

Instances of the **description** command appear in multiple configuration templates.

Command Hierarchy

Instances of the **description** command appear throughout the configuration command hierarchy on Cisco vEdge devices.

Syntax Description

text	Text Description Text description of the parameter or property. The text can be a maximum of 128 characters. If it includes spaces, enclose the entire string in quotation marks (" ").

Command History

Release	Modification
14.1	Command introduced.

Example

Configure a text description for an interface:

```
vEdge(config-interface-ge0/4)# description "VPN 1 interface"
vEdge(config-interface-ge0/4)# show config
vpn 1
 interface ge0/4
  description "VPN 1 interface"
 !
!
```

Operational Commands

show interface description

show running-config vpn

Related Topics

name, on page 342

device-groups

Configure one or more groups to which the vEdge device belongs.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  device-groups [group-name]
```

Syntax Description

group-name [*group-names*]	Group Names: 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 History

Release	Modification
14.2	Command introduced.

Example

Add a vEdge router to two groups: London and the United Kingdom:

```
vEdge(config)# system
vEdge(config-system)# device-groups London
vEdge(config-system)# device-groups [ "United Kingdom" ]
```

dhcp-helper

Allow an interface to act as a DHCP helper (on vEdge routers only). A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the DHCP server specified by the configured IP helper address.

You can configure a DHCP helper only on service-side interfaces. These are interfaces in any VPN except VPN 0 (the WAN-side transport VPN) and VPN 512 (the out-of-band management VPN).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn id
  interface interface-name
    dhcp-helper ip-addresses
```

Syntax Description

ip-addresses	IP Address of DHCP Server IP addresses of one or more DHCP servers. You can configure up to eight IP addresses in a single **dhcp-helper** command. The addresses cannot be broadcast addresses.

Command History

Release	Modification
14.1	Command introduced.
14.3	Add support for four IP addresses on a single DHCP helper interface.
17.2.2	Add support for eight IP addresses on a single DHCP helper interface.

Example

Configure the IP address of a DHCP server to allow an interface to be a DHCP helper:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-helper 10.22.11.1
vEdge(config-interface-ge0/4)# commit and-quit
 Commit complete.
vEdge# show running-config vpn 1 interface ge0/4
vpn 1
 interface ge0/4
  description "VPN 1 interface"
  ip address 10.20.25.16/24
  dhcp-helper 10.22.11.1
  no shutdown
 !
!
```

Configure multiple DHCP helpers:

```
vEdge(config-interface-ge0/4)# dhcp-helper 10.20.24.16 10.20.24.17 10.20.24.18 10.20.24.19
vEdge(config-interface-ge0/4)# show full-configuration
vpn 1
 interface ge0/4
  ip address 10.20.24.15/24
  dhcp-helper 10.20.24.16 10.20.24.17 10.20.24.18 10.20.24.19
```

```
  no shutdown
 !
!
```

Operational Commands

show running-config vpn interface

Related Topics

dhcp-server, on page 181

dhcp-server

Enable DHCP server functionality on a vEdge router so it can assign IP addresses to hosts in the service-side network (on vEdge routers only).

You can configure a DHCP helper only on service-side interfaces. These are interfaces in any VPN except VPN 0 (the WAN-side transport VPN) and VPN 512 (the out-of-band management VPN).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      address-pool prefix/length
      admin-state (down | up)
      exclude ip-address
      lease-time seconds
      max-leases number
      offer-time seconds
      options
        default-gateway ip-address
        dns-servers ip-address
        domain-name domain-name
        interface-mtu mtu
        tftp-servers ip-address
      static-lease mac-address ip ip-address host-name hostname
```

Syntax Description

None

Command History

Release	Modification
14.3	Command introduced.

Example

Configure the interface to be the DHCP server for the addresses covered by the IP prefix 10.0.100.0/24:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server address-pool 10.0.100.0/24
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   address-pool 10.0.100.0/24
  !
 !
!
```

Operational Commands

clear dhcp server-bindings

show dhcp interface

show dhcp server

Related Topics

allow-service, on page 63
dhcp-helper, on page 179

dialer down-with-vInterface

To track a Point-to-Point Protocol (PPP) session over a dialer interface on Cisco IOS XE Catalyst SD-WAN devices, use the **dialer down-with-vInterface** in the interface configuration mode. It specifies the status of the dialer interface that uses to connect to a specific destination subnetwork.

dialer down-with-vInterface

Command Default The dialer interface is disabled.

Command Modes Interface configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.

Example

The following is a sample output from the show dialer command for an asynchronous interface:

```
Device# show interface dialer1

Dialer1 is down, line protocol is down (spoofing)
  Hardware is Unknown
```

```
Internet address will be negotiated using IPCP
MTU 1500 bytes, BW 56 Kbit/sec, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Closed, loopback not set
Keepalive set (10 sec)
DTR is pulsed for 1 seconds on reset
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:50:36
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes
   538 packets output, 7524 bytes
```

direction

Configure the direction in which a NAT interface performs address translation (on vEdge routers only). For each NAT pool interface, you can configure only one direction.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface natpoolnumber
    nat
      direction (inside | outside)
```

Syntax Description

(**inside** | **outside**)	Direction To Perform Network Address Translation: Direction in which to perform network address translation. It can be one of the following: • **inside**—Translate the source IP address of packets that are coming from the service side of the vEdge router and that are destined to transport side of the router. This is the default. • **outside** —Translate the source IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined to a service-side device.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a vEdge router to NAT a service-side and a remote IP address:

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
    static source-ip 10.1.17.3 translate-ip 10.15.1.4 inside
    static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
    no overload
  !
  direction inside
  no shutdown
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

Related Topics

encapsulation, on page 202

discard-rejected

Have OMP discard routes that have been rejected on the basis of policy (on vSmart controllers only). By default, rejected routes are not discarded.

vManage Feature Template

For vSmart controllers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  discard-rejected
```

Syntax Description

None

Command History

Release	Modification
15.4	Command introduced.

Example

Configure a vSmart controller to discard routes that have been rejected by a policy:

```
vSmart# show running-config omp
omp
 no shutdown
 discard-rejected
 graceful-restart
 timers
  holdtime 15
 exit
!
```

Operational Commands

show omp peers

show omp routes

show omp services

show omp summary

show omp tlocs

disk-speed

To configure watermarks for the disk read and write speeds for disk partitions on a Cisco vManage server, use the **disk-speed** command in the alarms configuration mode. To remove the configuration, use the **no** form of this command.

disk-speed *disk-partition* [**read-high-watermark-kBps** *speed*] [**read-medium-watermark-kBps** *speed*] [**low-watermark-percentage** *percentage*] [**interval** *seconds*]

no disk-speed *disk-partition*

Syntax Description

disk-partition	Specifies the disk partition for which the read and write speed watermarks should be applied. (Use '?' to view available disk partitions.)
high-watermark-percentage*percentage*	Specifies the high-usage watermark percentage. Range: 1 to 100 percent Default: 90 percent

medium-watermark-percentage*percentage*	Specifies the medium-usage watermark percentage. Range: 1 to 100 percent Default: 75 percent
low-watermark-percentage*percentage*	Specifies the low-usage watermark percentage. Range: 1 to 100 percent Default: 60 percent
interval*seconds*	Specifies how frequently disk usage should be checked and reported by the device to Cisco vManage. Range: 1 to 4294967295 seconds Default: 5 seconds

Command Default

By default, watermarks for disk read and write speeds are not configured.

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples

The following example shows a sample configuration of the disk read and write speed watermarks and the polling interval:

```
config
 system
  alarms
   disk-speed /dev/nvme1n1
    read-high-watermark-kBps 1000
    read-medium-watermark-kBps 500
    read-low-watermark-kBps 100
    write-high-watermark-kBps 1000
    write-medium-watermark-kBps 500
    write-low-watermark-kBps 100
    interval 100
```

Related Commands

Command	Description
alarms	Enters the alarms configuration mode.

disk-usage

To configure the disk-usage watermarks, use the **disk-usage** command in the alarms configuration mode. To revert to the default watermark values, use the **no** form of this command.

disk-usage *file-system-path* [**high-watermark-percentage** *percentage*] [**medium-watermark-percentage** *percentage*] [**low-watermark-percentage** *percentage*] [**interval** *seconds*]

no disk-usage *file-system-path*

Syntax Description

file-system-path	Specifies the file system path for which the disk usage watermarks should be applied. (Use '?' to view available file system paths.)
high-watermark-percentage*percentage*	Specifies the high-usage watermark percentage. Range: 1 to 100 percent Default: 90 percent
medium-watermark-percentage*percentage*	Specifies the medium-usage watermark percentage. Range: 1 to 100 percent Default: 75 percent
low-watermark-percentage*percentage*	Specifies the low-usage watermark percentage. Range: 1 to 100 percent Default: 60 percent
interval*seconds*	Specifies how frequently disk usage should be checked and reported by the device to Cisco vManage. Range: 1 to 4294967295 seconds Default: 5 seconds

Command Default

The default usage watermarks and polling interval are:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples

The following example shows a sample configuration of the disk-usage watermarks and the polling interval:

```
config
 system
  alarms
   disk-usage /tmp
```

```
high-watermark-percentage 80
medium-watermark-percentage 70
low-watermark-percentage 50
interval 10
```

Related Commands

Command	Description
alarms	Enters the alarms configuration mode.

distance

Define the OSPF route administration distance based on route type (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      distance
        external number
        inter-area number
        intra-area number
```

Syntax Description

external *number*	Distance for External Routes: Set the OSPF distance for routes learned from other domains. Range: 0 through 255 Default: 110
inter-area *number*	Distance for Interarea Routes Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
inter-area *number*	Distance for Intra-Area Routes Set the distance for routes within an area. Range: 0 through 255 Default: 110

Command History

Release	Modification
14.1	Command introduced.

Example

Change the OSPF distance for routes learned from other domains:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 router ospf
vEdge(config-ospf)# distance external 50
vEdge(config-ospf)# show config
vpn 1
 router
  ospf
   distance external 50
  !
 !
!
```

Operational Commands

show ospf routes

dns

Configure the address of a DNS server within a VPN.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  dns ip-address (primary | secondary)
```

Syntax Description

ip-address	Address of DNS Server: IPv4 or IPv6 address of a DNS server reachable from the vEdge device.
(**primary** | **secondary**)	Primary or Secondary Server: Specify whether the DNS server is the primary server or a backup. Default: **primary**

Command History

Release	Modification
14.1	Command introduced.
16.3	Add support for IPv6 DNS server addresses.

Example

Configure a DNS server in VPN 3:

```
vEdge(config)# vpn 3 dns 1.2.3.4 primary
vEdge(config-vpn-3)# show configuration
vpn 3
 dns 1.2.3.4 primary
!
```

Operational Commands

show running-config vpn

domain-id

Configure the identifier for the vEdge device overlay network domain (available on vSmart controllers and vEdge routers).

Command Hierarchy

```
system
  domain-id domain-id
```

Syntax Description

domain-id	Domain Identifier A numeric identifier for the vEdge device overlay network domain. The domain identifier must be the same for all vEdge devices that reside in the same domain. Currently, the vEdge software supports only a single domain. Range: 1 through 4294967295 (a 32-bit integer) Default: 1 (value that is configured when the vSmart controller or vEdge router is first booted)

Command History

Release	Modification
14.1	Command introduced.
14.2	Domain ID default changed to 1.

Example

Configure the domain identifier to be 2:

```
vSmart# show running-config system
system
  system-ip 1.1.1.9
  domain-id 2
  site-id   50
  vbond 10.0.4.12
!
```

Operational Commands

show control local-properties

dot1x

Configure port-level 802.1X parameters on a router interface in VPN 0 (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      accounting-interval minutes
      acct-req-attr attribute-number (integer integer | octet octet | string string)
      auth-fail-vlan vlan-id
      auth-order (mab | radius)
      auth-reject-vlan vlan-id
      auth-req-attr attribute-number (integer integer | octet octet | string string)
      control-direction direction
      das
        client ip-address
        port port-number
        require-timestamp
        secret-key password
        time-window seconds
        vpn vpn-id
      default-vlan vlan-id
      guest-vlan vlan-id
      host-mode (multi-auth | multi-host | single-host)
      mac-authentication-bypass
        allow mac-addresses
        server
      nas-identifier string
      nas-ip-address ip-address
      radius-servers tag
      reauthentication minutes
      timeout
        inactivity minutes
      wake-on-lan
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Configure IEEE 802.1X on one router interface. In this example, the bridging domain numbers match the VLAN numbers, which is a recommended best practice. Also, the bridging domain name identifies the type of 802.1X VLAN.

```
system
 ...
 radius
  server 10.1.15.150
   tag              freerad1
   source-interface ge0/0
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         1
  exit
  server 10.20.24.150
   auth-port        2000
   acct-port        2001
   tag              freerad2
   source-interface ge0/4
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         2
  exit
 !
!
bridge 1
 name Untagged_bridge
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 10
 name Authorize_VLAN
 vlan 10
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 20
 name Guest_VLAN
 vlan 20
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 30
 name Critical_VLAN
 vlan 30
```

```
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
bridge 40
 name Restricted_VLAN
 vlan 40
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
   encapsulation ipsec
   ...
  !
  no shutdown
 !
 interface ge0/1
  ip address 60.0.1.16/24
  no shutdown
 !
 interface ge0/2
  ip address 10.1.19.15/24
  no shutdown
 !
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
 !
 interface ge0/5
  dot1x
   auth-reject-vlan 40
   auth-fail-vlan   30
   guest-vlan       20
   default-vlan     10
   radius-servers   freerad1
  !
  no shutdown
 !
 interface ge0/7
  ip address 10.0.100.15/24
  no shutdown
 !
!
vpn 1
 interface ge0/2.1
  ip address 10.2.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb1
  ip address 56.0.1.15/24
  mac-address 00:00:00:00:aa:01
  no shutdown
  dhcp-server
   address-pool 56.0.1.0/25
   offer-time   600
   lease-time   86400
   admin-state  up
```

```
   options
    default-gateway 56.0.1.15
   !
  !
 !
!
vpn 10
 interface ge0/2.10
  ip address 10.10.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb10
  ip address 56.0.10.15/24
  mac-address 00:00:00:00:aa:10
  no shutdown
  dhcp-server
   address-pool 56.0.10.0/25
   offer-time   600
   lease-time   86400
   admin-state  up
   options
    default-gateway 56.0.10.15
   !
  !
 !
!
vpn 20
 interface ge0/2.20
  ip address 10.20.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb20
  ip address 56.0.20.15/24
  mac-address 00:00:00:00:aa:20
  no shutdown
 !
!
vpn 30
 interface ge0/2.30
  ip address 10.30.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb30
  ip address 56.0.30.15/24
  mac-address 00:00:00:00:aa:30
  no shutdown
 !
!
vpn 40
 interface ge0/2.40
  ip address 10.40.19.15/24
  mtu      1496
  no shutdown
 !
 interface irb40
  ip address 56.0.40.15/24
  mac-address 00:00:00:00:aa:40
  no shutdown
 !
!
vpn 512
```

```
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius show system statistics

Related Topics

radius, on page 407

duplex

Configure whether the interface runs in full-duplex or half-duplex mode.

On all vEdge router models, all interfaces support 1-Gigabit Ethernet SFPs. These SFPs can either be copper or fiber. For fiber SFPs, the supported speeds are 1 Gbps full duplex and 100 Mbps 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, you must disable autonegotiation and then use the **speed** and **duplex** commands to set the appropriate interface link characteristics.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface geport/slot
    duplex (full | half)
```

Syntax Description

(**full** | **half**)	Duplex Mode: Set the interface to run in full-duplex or half-duplex mode. Default: **full**

Command History

Release	Modification
14.1	Command introduced.
15.3	Support for autonegotiation added.

Example

Configure an interface to run in half-duplex mode:

```
vpn 0
 interface ge0/0
   no autonegotiate
   duplex half
```

Operational Commands

show interface

Related Topics

autonegotiate, on page 96
speed, on page 458

ebgp-multihop

Attempt BGP connections to and accept BGP connections from external peers on networks that are not directly connected to this network (on vEdge routers only).

This feature is disabled by default. If you configure it, use the **no ebgp-multihop** command to return to the default.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        ebgp-multihop [ttl]
```

Syntax Description

ttl	Time to Live for BGP Connections to External Peers: Set the time to live (TTL) for BGP connections to external peers. Range: 0 to 255 Default: 1

Command History

Release	Modification
14.1	Command introduced.

Example

Enable EBGP multihop:

```
vEdge# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
  bgp 123
   neighbor 1.10.10.10
    no shutdown
    remote-as 456
    ebgp-multihop
    !
   !
  !
 !
!
```

Operation Commands

show bgp neighbor

ecmp-hash-key

Determine how equal-cost paths are chosen (on vEdge routers only). By default, a combination of the source IP address, destination IP address, protocol, and DSCP field is used as the ECMP hash key to determine which of the equal cost paths to choose.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  ecmp-hash-key layer4
```

Syntax Description

layer4	Use the Layer 4 Source and Destination Ports in the ECMP Hash Key: Use a combination of the Layer 4 source port and Layer 4 destination port, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. Note that this flag should be enabled only in networks where it can be guaranteed that there will never be IP fragmentation. Otherwise, enabling this could lead to out-of-order packets.

Command History

Release	Modification
14.1	Command introduced.

Example

Use the Layer 4 source and destination ports in the EMCP hash key:

```
vEdge(config-vpn-1)# ecmp-hash-key layer4
vEdge(config-vpn-1)# show config
vpn 1
 ecmp-hash-key layer4
!
```

Operational Commands

show running-config vpn

ecmp-limit

Configure the maximum number of OMP paths that can be installed in the vEdge router's route table (on vEdge routers only). When a vEdge router has two or more WAN interfaces and hence two or more TLOCs, it has one static route for each of the WAN next hops. All routes are installed as ECMP routes only if the next hop for the route can be resolved.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  ecmp-limit number
```

Syntax Description

number	Number of OMP Paths: Maximum number of OMP paths that can be installed in a vEdge router's route table. Range: 1 through 16 Default: 4

Command History

Release	Modification
15.2	Command introduced.
15.3.3	Installing ECMP routes only if the next hop can be resolved added.

Operational Commands

show omp routes

eco-friendly-mode

Configure a vEdge Cloud router to use its CPU minimally or not at all when the router is not processing any packets (available on vEdge Cloud routers). By default, eco-friendly mode is disabled.

Enabling eco-friendly mode is useful when you are upgrading multiple vEdge Cloud routers simultaneously, especially routers that have only one virtual CPU (vCPU). Enabling this mode allows the routers to download the software image files without timing out. (A software image download times out after 60 minutes).

Command Hierarchy

```
system
  [no] eco-friendly-mode
```

Syntax Description

None

Command History

Release	Modification
17.2	Command introduced.

Example

Enable eco-friendly mode:

```
vEdge-Cloud# config
vEdge-Cloud(config)# system eco-friendly-mode
```

Operational Commands

show running-config system

eigrp

This topic describes the commands used to configure and monitor Enhanced Interior Gateway Routing Protocol (EIGRP) routing capabilities and features within a VPN on a Cisco IOS XE router. For full EIGRP configuration information and examples, refer to the Cisco IOS IP Routing: EIGRP Configuration Guide.

vManage Feature Template

Configuration ▶ Templates ▶ EIGRP

Command Hierarchy

```
vpn vpn-id
   router
      eigrp name
         address-family ipv4 vrf vrf-name
            autonomous-system autonomous-system-number
            af-interface intf-name
               authentication key-chain keychain-name
               authentication mode {hmac-sha-256 | md5}
               hello-interval seconds
               hold-time seconds
               passive-interface
               split-horizon
               summary-address [prefix | prefix-length]
               exit-af-interface
            eigrp router-id ipv4-address
            network [prefix | mask]
            shutdown
            topology {base | topology-name tid number}
               auto-summary
               default-metric {k1 k2 k3 k4 k5}
               distribute-list {acl-num | acl-name | gateway address | prefix prefix-name
| route-map routemap-name}
               redistribute {bgp | connected | nat-route | omp | ospf | static} [route-map
 route-map-name] [metric k1 k2 k3 k4 k5]
               table-map route-map-name [filter]
```

Operational Commands

```
show eigrp address-family ipv4 vrf vrf-num neighbors [interface-name | peer-v4-address]
show eigrp address-family ipv4 vrf vrf-num accounting
show eigrp address-family ipv4 vrf vrf-num events [reverse] [starting-number] [errmsg]
show eigrp address-family ipv4 vrf vrf-num interfaces [interface-name | detail]
show eigrp address-family ipv4 vrf vrf-num timers
show eigrp address-family ipv4 vrf vrf-num topology [v4-prefix/prefixlength | active |
detail-links | route-type {connected | external | internal | local | redistributed | summary}]
show eigrp address-family ipv4 vrf vrf-num traffic
show eigrp protocols {vrf vrf-num}
show ip route vrf vrf-num eigrp
```

Example

Show configuration information for an IPv4 EIGRP route on an IOS XE router

```
ios_xe_router#show ip route vrf 1
   m     22.22.22.22 [251/0] via 11.11.11.12, 00:28:00
           55.0.0.0/32 is subnetted, 1 subnets
   D EX  55.55.55.55 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
           66.0.0.0/32 is subnetted, 1 subnets
   B     66.66.66.66 [20/0] via 192.168.1.3, 00:33:57
           192.168.1.0/32 is subnetted, 3 subnets
   D EX  192.168.1.3 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
   m     192.168.1.33 [251/0] via 11.11.11.14 (3), 00:28:01
ios_xe_router# show omp route vpn 1 55.55.55.55/32
```

Related Topics

router eigrp
address-family (EIGRP)
af-interface
authentication key-chain (EIGRP)
authentication mode (EIGRP)
hello-interval
hold-time
passive-interface (EIGRP)
split-horizon (EIGRP)
summary-address (EIGRP)
exit-af-interface
eigrp router-id
network (EIGRP)
shutdown (address-family)
auto-summary (EIGRP)
default-metric (EIGRP)
distribute-list prefix-list (IPv6 EIGRP)
redistribute eigrp
table-map
show eigrp address-family accounting
show eigrp address-family interfaces
show eigrp address-family neighbors
show eigrp address-family timers
show eigrp address-family topology
show eigrp address-family traffic
show eigrp protocols

elephant-flow

To configure elephant-flow to throttle traffic flow, use **elephant-flow** command in policy configuration mode. To disable the elephant-flow configurations, use the **no** form of this command.

elephant-flow [**custom-eflow**] [**enable**] [**max-queue-depth** *depth*] [**queue-depth** *depth*] [**rate-threshold** *threshold*]
no elephant-flow [**custom-eflow**] [**enable**] [**max-queue-depth** *depth*] [**queue-depth** *depth*] [**rate-threshold** *threshold*]

Syntax Description

custome-eflow	Define scope for eflow direction.
enable	Enable elephant-flow configurations for Cisco vEdge2k.
max-queue-depth *depth*	Specify the maximum queue depth beyond which the packets of all flows starts dropping. Range: 1000 to 500000 Default: 20000
queue-depth *depth*	Specify the queue depth beyond which the packets of elephant-flow starts dropping. Range: 1 to 100000 Default: 200
rate-threshold *threshold*	Specify rate in Kilo Packets Per Second (KPPS) above which a flow is considered as elephant flow. Range: 10 to 500 Default: 20

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

Examples

The following example shows how to configure elephant-flow configurations:

```
vEdge2k# config terminal
vEdge2k(config)# policy
vEdge2k(config-policy)# elephant-flow
vEdge2k(policy-elephant-flow)# enable
vEdge2k(policy-elephant-flow)# max-queue-depth 20000
vEdge2k(policy-elephant-flow)# rate-threshold 21
```

encapsulation

Set the encapsulation for a tunnel interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      encapsulation (gre | ipsec)
        preference number
        weight number
```

Syntax Description

(**gre** |**ipsec**)	Encapsulation: Set 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. 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. Default: None. When configuring a tunnel interface using the CLI, you must configure either an IPsec or a GRE interface. **Note** When configuring a tunnel interface using a Cisco SD-WAN Manager template, Cisco SD-WAN Manager configures the default values for IPsec and GRE. For more information on configuring a tunnel interface, see the Create a Tunnel Interface section of the *Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 20.x*.

preference *number*	Preference: Preference for directing traffic to the tunnel. A higher value is preferred. When a vEdge router has multiple tunnels (that is, multiple TLOCs), only the TLOC or TLOCs with the highest preference are chosen using inbound path selection. However, traffic is influenced in both the directions; inbound as well as outbound. If all TLOCs have the same preference and no policy is applied that affects traffic flow, traffic flows are evenly distributed among the tunnels, using ECMP. For example, when a preference of 100 on one TLOC and a preference of 50 on the other TLOC is set, the preference chosen is the TLOC with a preference of 100. **Note** The criteria set in preferences work correctly when there are no other configurations that may alter the traffic flow. For example, if preferences are used with color restrict (**color** *color* **restrict**), there is a possibility of the reverse traffic going through a different tunnel than what is expected based on the configured preferences. Range: 0 through 4294967295 ($2^{32} – 1$) Default: 0
weight *number*	Weight: 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 vEdge router 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 History

Release	Modification
20.14.1	Command introduced.
20.15.1	**preference** and **weight** commands moved from under **tunnel-interface** to under **encapsulation**.
20.15.2	Add GRE encapsulation.
20.15.3	The **encapsulation** command is optional for configuring a tunnel interface.
20.18.1	The **encapsulation** command is optional for configuring a tunnel interface.

Example

Create a GRE tunnel and direct voice traffic to it:

```
vpn 0
  interface ge1/1
    ip address 1.2.3.0/24
```

```
    tunnel-interface
      encapsulation gre
      color blue
      allow-service dhcp
      allow-service dns
      allow-service icmp
      no allow-service sshd
      no allow-service ntp
      no allow-service stun
      !
    no shutdown
    !
  !
!
policy
  data-policy direct-voice-to-gre
    vpn-list voice-vpn-list
      sequence 10
        match
          dscp 8
        !
        action accept
          set
            vpn 1
            tloc 1.2.3.4 color blue encap gre
          !
        !
      !
      default-action drop
    !
  !
  lists
    vpn-list voice-vpn-list
      vpn 1-10
    !
    site-list voice-site-list
      site-id 100-102
    !
  !
!
apply-policy site-list voice-site-list data-policy direct-voice-to-gre all
```

Operational Commands

show control connections

show omp tlocs

show omp tlocs detail (see display the configured preference and weight values)

Related Topics

bfd color, on page 106
color, on page 137

exclude

Exclude specific addresses from the pool of addresses for which the interface acts as DHCP server (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface genumber/subinterface
    dhcp-server
      exclude ip-address
```

Syntax Description

ip-address	Address To Exclude: IP address to exclude from the DHCP address pool. To specify multiple individual addresses, list them in a single **exclude** command, separated by a space (for example, **exclude 1.1.1.1 2.2.2.2 3.3.3.3**). To specify a range of addresses, separate them with a hyphen (for example, **exclude 1.1.1.1-1.1.1.10**).

Command History

Release	Modification
14.3	Command introduced.
15.1	Support for command ranges added.

Example

Exclude 10.0.100.2 from the DHCP address pool 10.0.100.0/24:

```
vm5# config
Entering configuration mode terminal
vm5(config)# vpn 1 interface ge0/4
vm5(config-interface-ge0/4)# dhcp-server exclude 10.0.100.2
vm5(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   address-pool 10.0.100.0/24
   exclude      10.0.100.2
  !
 !
!
```

Operational Commands

show dhcp interface

show dhcp server

exclude-controller-group-list

Configure the vSmart controllers that the tunnel interface is not allowed to connect to (on vEdge routers only).

On a system-wide basis, you configure all the 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 vSmart controllers that a particular tunnel interface can establish connections with. If a Cisco vEdge device is not able to establish required number of control connections from a TLOC which is minimum of max-control-connections from TLOC configuration and max-omp-sessions from system configuration, then the device will try to connect to Cisco vSmart Controller specified in `exclude-controller-group-list` command.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      exclude-controller-group-list number
```

Syntax Description

number	vSmart Controller Groups To Exclude: Identifiers of one or more 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 History

Release	Modification
16.1	Command introduced.

Example

Have the tunnel interface not use controller group list 2:

```
vpn 0
  interface ge0/2
    tunnel-interface
      exclude-controller-group-list 2
```

Operational Commands

show control affinity config

show control affinity status

show control connections

show control local-properties

Related Topics

controller-group-id, on page 150
controller-group-list, on page 151
max-control-connections, on page 329
max-omp-sessions, on page 334

flow-active-timeout

For a cflowd template, how long to collect a set of flows for a flow on which traffic is actively flowing (on vSmart controllers only). At the end of this time period, the data set is exported to the collector.

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    flow-active-timeout seconds
```

Syntax Description

seconds	Collection Time: How long to collect a set of sampled flows for a flow on which traffic is actively flowing. If you configure this time and later modify it, the changes take effect only on flows that are created after the configuration change has been propagated to the vEdge router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the **clear app cflowd flows** command. Range: 30 through 3600 seconds Default: 600 seconds (10 minutes)

Command History

Release	Modification
14.3	Command introduced.
15.3	Default timeout value changed to 10 minutes.

Example

Configure a cflowd template:

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233
 flow-active-timeout 600
 flow-inactive-timeout 90
 template-refresh 120
!
```

Operational Commands

clear app cflowd flows (on vEdge routers only)

clear app cflowd statistics (on vEdge routers only)

show policy from-vsmart (on vEdge routers only)

show running-config policy (on vSmart controllers only)

show app cflowd flows (on vEdge routers only)

show app cflowd template (on vEdge routers only)

Related Topics

flow-inactive-timeout, on page 210

flow-control

Configure flow control, which is a mechanism for temporarily stopping the transmission of data on the interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    flow-control control
```

Syntax Description

control	Flow Control Direction: Configure flow control on an interface. *control* an be **autoneg**, **both**, **egress**, **ingress**, or **none**. Default: **autoneg**

Command History

Release	Modification
14.1	Command introduced.

Example

Configure bidirectional flow control on an interface:

```
vEdge(config-interface-ge0/0)# flow-control both
vEdge-interface-ge0/0)# show config
vpn 1
 interface ge0/0
  flow-control both
  no shutdown
 !
!
```

Operational Commands

show running-config vpn interface

flow-inactive-timeout

For a cflowd template, how long to wait to send a set of sampled flows to a collector for a flow on which no traffic is flowing (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    flow-inactive-timeout seconds
```

Syntax Description

seconds	Timeout Due to Inactivity: How long to wait to send a set of sampled flows to a collector for a flow on which no traffic is flowing. If you configure this time and later modify it, the changes take effect only on flows that are created after the configuration change has been propagated to the vEdge router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the **clear app cflowd flows** command. Range: 1 through 3600 seconds Default: 60 seconds (1 minute)

Command History

Release	Modification
14.3	Command introduced.
15.3	Default timeout value changed to 1 minute.

Example

Configure a cflowd template:

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233
 flow-active-timeout 60
 flow-inactive-timeout 90
 template-refresh 120
!
```

Operational Commands

clear app cflowd flows (on vEdge routers only)

clear app cflowd statistics (on vEdge routers only)

show policy from-vsmart (on vEdge routers only)

show running-config policy (on vSmart controllers only)

show app cflowd flows (on vEdge routers only)

show app cflowd template (on vEdge routers only)

Related Topics

flow-active-timeout, on page 208

flow-sampling-interval

For a cflowd template, how many packets to wait before creating a new flow (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    flow-sampling-interval number
```

Syntax Description

number	Sampling Interval: How many packets to wait before creating a new flow. Note that if a flow already exists, flow information continues to be recorded in that flow. While you can configure any integer value for the number of packets, the software rounds the value down to the nearest power of 2. Range: 1 through 65536

Command History

Release	Modification
16.3	Command introduced.

Example

Start a new flow after 63 packets, when the 64th packet is received:

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233
 flow-active-timeout 60
 flow-inactive-timeout 90
 flow-sampling-interval 64
 template-refresh 120
!
```

Operational Commands

clear app cflowd flows (on vEdge routers only)

clear app cflowd statistics (on vEdge routers only)

show policy from-vsmart (on vEdge routers only)

show running-config policy (on vSmart controllers only)

show app cflowd flows (on vEdge routers only)

show app cflowd template (on vEdge routers only)

flow-visibility

Enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN (on vEdge routers only).

vManage Feature Template

For vEdge routers:

Configuration ► Policies ► Localized Policy

Command Hierarchy

```
policy
  flow-visibility
```

Syntax Descriptionm

None

Command History

Release	Modification
15.3	Command introduced.

Operational Commands

clear app cflowd flows

clear app cflowd statistics

show app cflowd collector

show app cflowd flow-count

show app cflowd flows

show app cflowd statistics

show app cflowd template

show policy from-vsmart

gps-location

Set the latitude and longitude of a vEdge device.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  gps-location latitude decimal-degrees
  gps-location longitude decimal-degrees
```

Syntax Description

latitude *decimal-degrees*	Set the Latitude: Set the latitude of the device, specifying the coordinate in decimal degrees.

longitude *decimal-degrees*	Set the Longitude: Set the longitude of the device, specifying the coordinate in decimal degrees.

Command History

Release	Modification
14.1	Command introduced.

Example

Set the devices geographical coordinates:

```
vEdge(config-system)# gps-location latitude 37.368140
vEdge(config-system)# gps-location longitude -121.913658
vEdge(config-system)# show configuration
system
 gps-location latitude 37.368140
 gps-location longitude -121.913658
!
```

Operational Commands

show running-config system

Related Topics

location, on page 295
location, on page 293

graceful-restart

Control graceful restart for OMP (on vEdge routers and vSmart controllers only). By default, graceful restart for OMP is enabled on all vEdge routers and vSmart controllers.

vManage Feature Template

For vEdge routers and vSmart controllers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  graceful-restart
```

Syntax Description

no omp graceful-restart **omp timers graceful-restart-timer 0**	Disable Graceful Restart. By default, OMP graceful restart is enabled on vEdge routers and vSmart controllers. Use one of these two commands to disable it. **Note** Changing the Cisco SD-WAN Controller **graceful-restart timers** result in an OMP peer flap, independent of whether or not **port-hop** is enabled. We recommend that you change Cisco SD-WAN Controller **graceful-restart timers** with redundant Cisco SD-WAN Controller peering (where only a single Cisco SD-WAN Controller configuration is changed at a time) or during a maintenance period when a data plane disruption can be tolerated.

Command History

Release	Modification
14.2	Command introduced.

Operational Commands

show omp peers detail

Related Topics

timers, on page 492

group

vpn 0 interface tunnel-interface group—Assign an identifier to an individual WAN transport tunnel.

The tunnel group is identified by a number in the range 1 to 4294967295 (default is 0). This identifier prevents the local router from forming tunnels to any other tunnel group. After a tunnel group is assigned, the local router can form tunnels to:

- Transports with matching group IDs, and
- Transports with no group ID assigned

The group ID can be used with the color restrict option if needed. If using both options, tunnels can be formed only with transports that meet both criteria: color and group ID.

Note If using group IDs, assign a group ID to all transports.

Simple Example

Scenario: A network contains three routers (A, B, and C).

Intention: Enable router A to form tunnels only with router B.

Method: To apply this restriction, assign routers A and B the same group ID (example: 100). Assign router C a different group ID (example: 200).

Result: Router A will form tunnels with router B, but not with router C.

Use Case

Group ID can be used as an alternative to restricting tunnel creation by color. It offers a good solution for sites with redundant connections to the same MPLS provider, where the head end uses two private colors (example: private1 and private2) to the same provider, but the remote sites only have one connection, and therefore only one color.

Instead of using the color restrict option, assign both private1 and private2 the same group ID at all sites. Now the remote site will form tunnels to both head end routers, but only with the matching group IDs.

Tunnels can be formed to all transports with matching group IDs, and transports with no group ID. Therefore, if using group IDs, assign a group ID to all transports. For example, use ID=100 for all public transports and ID=500 for all private transports on the same carrier. Regardless of color, tunnels are only attempted to matching transport IDs.

vManage Feature Template

For vEdge routers, vManage NMSs, and vSmart controllers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      group group-id
```

Command History

Release	Modification
19.1	Command introduced.

Operational Commands

show control connections

show bfd sessions

show omp tlocs detail

Example

Associate a group ID with a tunnel connection:

```
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
```

```
 no shutdown
!
interface loopback2
 ip address 172.16.15.15/24
 tunnel-interface
  color   metro-ethernet
  group 100
  bind    ge0/0
 !
 no shutdown
!
```

group

Configure SNMPv3 groups.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  group group-name authentication
    view string
```

Syntax Description

authentication	Group Authentication: Authentication to use for members of the group. *authentication* can be one of the following: • *auth-no-priv*—Provide authentication using the HMAC-MD5 or HMAC-SHA algorithm. • *auth-priv*—Provide authentication using the HMAC-MD5 or HMAC-SHA algorithm, and provide CBC DES 56-bit encryption. • *no-auth-no-priv*—Provide authentication based on a username.
group *group-name*	Group Name: Name of the SNMPv3 group. *group-name* can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (" ").
view *string*	SNMP View: Name of the view record to use for the group. It can be a 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (" ").

Command History

Release	Modification
16.2	Command introduced.

Operational Commands

show running-config snmp

Related Topics

user, on page 524

group

Configure the Diffie-Hellman group number to be used in the IKE key exchange (on vEdge routers only). IKE key exchange is done in a Diffie-Hellman exchange.

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ike
      group number
```

Syntax Description

number	Group Number Diffie-Hellman group number to use in key exchange. The number to use depends on the length of the Diffie-Hellman key. It can be one of the following values: • 2—Use the 1024-bit more modular exponential (MODP) Diffie-Hellman group. • 14—Use the 2048-bit MODP Diffie-Hellman group. • 15—Use the 3072-bit MODP Diffie-Hellman group. • 16—Use the 4096-bit MODP Diffie-Hellman group. Default: 16

Command History

Release	Modification
17.2	Command introduced.

Example

Change the IKEv1 Diffie-Hellman group number to 15:

```
vEdge(config)# vpn 1 interface ipsec1 ike
vEdge(config-ike)# group 15
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

mode, on page 338

guard-interval

Specify the guard interval (on vEdge cellular wireless routers only). The guard interval allows reflections from the previous data transmission to settle before transmitting a new symbol.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi Radio

Command Hierarchy

```
wlan radio-band
  guard-interval nanoseconds
```

Syntax Description

nanoseconds	Guard Interval: Set the guard interval. It can be one of the following values: • 400—Short guard interval (SGI), which is 400 nanoseconds. The short guard interval can increase throughput, but it can also increase the error rate because of increased sensitivity to RF reflections. This is the default value for 5-GHz radio frequencies. • 800—Normal guard interval, which is 800 nanoseconds. This is the default value for 2.4-GHz radio frequencies.

Command History

Release	Modification
16.3	Command introduced.

Example

Explicitly configure the short guard interval for a 5-GHz radio band:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 guard-interval 400
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

guest-vlan

Configure a guest VLAN to provide network access to limited services for non-802.1X-enabled clients (on vEdge routers only). These clients are placed in the guest VLAN only if MAC authentication bypass is not enabled.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      guest-vlan vlan-id
```

Syntax Description

vlan-id	VLAN Identifier: Identifier of the VLAN into which to place non-802.1X–enabled clients. Range: 1 through 4094

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a guest VLAN:

```
bridge 20
 name Guest_VLAN
 vlan 20
 interface ge0/5
  no native-vlan
  no shutdown
 !
!
vpn 0
 interface ge0/5
  dot1x
   guest-vlan       20
  !
  no shutdown
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

auth-fail-vlan, on page 81
auth-reject-vlan, on page 87
bridge, on page 115
default-vlan, on page 176
mac-authentication-bypass, on page 312
radius, on page 407

hello-interval

Configure the keepalive interval between Hello packets sent on a DTLS or TLS WAN transport connection.

vManage Feature Template

Configuration ► Templates ► VPN Interface Cellular (for cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      hello-interval milliseconds
```

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 that 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: • Controller-to-Controller/Controller-to-Manager tunnels: For a tunnel connection between two controller devices, the tunnel uses the lower hello interval and the higher tolerance interval for the connection between the two devices. This choice is made in case one of the controllers has a slower WAN connection. The hello interval and tolerance times are chosen separately for each pair of controller devices. • Router-to-Controller tunnels: For a tunnel connection between a router and any controller device, the tunnel uses the hello interval and tolerance times configured on the router. 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 router and a controller device. • Controller/Manager-to-Validator tunnels: For any tunnel where one of the Controller/Manager peers is a Validator, the negotiated hello interval is the maximum of the Validator's fixed hello interval (15,000 ms) and the peer's configured interval. Similarly, the negotiated hello tolerance is the maximum of the Validator's fixed hello tolerance (150 seconds) and the peer's configured tolerance. 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. For more information on low-bandwidth links, refer to the low-bandwidth-link command.

Command History

Release	Modification
15.2	Command introduced.
16.2	Maximum interval changed from 60 seconds to 10 minutes.
16.2.1	Add requirement that hello tolerance must be at least 2 times the hello interval.

Example

Decrease the amount of keepalive traffic sent between a router and Cisco SD-WAN controller devices:

```
vpn 0
 interface ge0/0
  tunnel-interface
   color lte
   encapsulation ipsec
   hello-interval 600000
   hello-tolerance 600
```

Operational Commands

To display the negotiated hello interval and hello tolerance values:

show control connections detail

show orchestrator connections detail

Related Topics

bfd color, on page 106
hello-tolerance, on page 225

hello-interval

Modify the PIM hello message interval for an interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      interface interface-name
        hello-interval seconds
```

Syntax Description

seconds	Hello Interval Time: How often to send PIM hello messages. Hello messages advertise that PIM is enabled on the router. Range: 1 through 3600 seconds Default: 30 seconds

Command History

Release	Modification
14.2	Command introduced.

Example

Change the PIM hello interval to 60 seconds:

```
vm1# show running-config vpn 1 router pim vpn 3
 router
  pim
   interface ge3/0
    hello-interval 60
   exit
  exit
 !
!
```

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show pim interface

show pim neighbor

show omp multicast-auto-discover

show omp multicast-routes

hello-interval

Set the interval at which the router sends OSPF hello packets (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          hello-interval seconds
```

Syntax Description

seconds	Hello Interval: Time interval at which the vEdge router sends OSPF hello packets to its neighbors. Range: 1 through 65535 seconds Default: 10 seconds

Command History

Release	Modification
14.1	Command introduced.

Example

Set the OSPF hello interval to 15 seconds:

```
vEdge# show running-config vpn 1 router ospf area 0
vpn 1
 router
  ospf
   area 0
    interface ge0/0
      hello-interval 15
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

Related Topics

dead-interval, on page 170

hello-tolerance

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.

vManage Feature Template

For al vEdge devices:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      hello-tolerance seconds
```

Syntax Description

seconds	Hello Tolerance Interval: 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 that 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 two controller devices, the tunnel uses the lower hello interval and the higher tolerance interval for the connection between the two devices. (Controller devices are vBond controllers, vManage NMSs, and vSmart controllers.) This choice is made in case one of the controllers has a slower WAN connection. The hello interval and tolerance times are chosen separately for each pair of controller devices. • For a tunnel connection between a vEdge router and any controller device, the tunnel uses the hello interval and tolerance times configured on the router. 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 vEdge router and a controller device. Range: 12 through 6000 seconds (10 minutes) Default: 12 seconds

Command History

Release	Modification
15.2	Command introduced.
16.2	Maximum tolerance increased from 1 minute to 10 minutes.

Release	Modification
16.2.1	Add requirement that hello tolerance must be at least 2 times the hello interval.

Example

Decrease the amount of keepalive traffic sent between a vEdge router and Cisco SD-WAN controller devices:

```
vEdge(config)# vpn 0 interface ge0/0 tunnel-interface color lte
vEdge(config-tunnel-interface)# encapsulation ipsec
vEdge(config-tunnel-interface)# hello-interval 600000
vEdge(config-tunnel-interface)# hello-tolerance 600
```

Operational Commands

show control connections detail

show orchestrator connections detail

Related Topics

bfd color, on page 106
hello-interval, on page 221

hold-time

vpn 0 interface tunnel-interface hold-time—Set the delay before switching back to the primary tunnel interface from a circuit of last resort (only on vEdge routers with cellular modules). This delay is to ensure that the primary interface is once again fully operational and is not still flapping.

Command Hierarchy

```
vpn 0
  interface cellularnumber
    tunnel-interface
      hold-time milliseconds
```

Syntax Description

Delay Time *milliseconds*	Delay before switching over from using the last-resort circuit back to using the primary tunnel interface. This delay is to ensure that the primary interface is once again fully operational and is not still flapping. Range: 100 through 300000 milliseconds (0.1 through 300 seconds) Default: 7000 milliseconds (7 seconds)

Command History

Release	Modification
16.2	Command introduced.

Example

Change the hold time for the circuit of last resort to 10 seconds:

```
vEdge# show running-config vpn 0 interface cellular0
vpn 0
interface cellular0
  ip dhcp-client
  tunnel-interface
   hold-time 10000
   encapsulation ipsec
   color lte
   last-resort-circuit
   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
  !
  clear-dont-fragment
  mtu                1428
  profile            1
  no shutdown
!
!
```

Operational Commands

show running-config vpn 0

host

Configure a static mapping between a hostname and an IPv4 or IPv6 address in the hostname cache.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  host string ip ip-address
```

Syntax Description

string	Hostname: Name of the vEdge router within the VPN. The name can be a maximum of 128 characters.

ip-address	IP Address: IPv4 or IPv6 address to associate with the router. You can associate up to 8 total IP addresses with a hostname.

Command History

Release	Modification
14.1	Command introduced.
16.3	Add support for IPv6 addresses.

Example

Configure a static hostname in VPN 1:

```
vEdge(config)# vpn 1 host my-hostname ip 1.2.3.4
vEdge(config-vpn-1)# show configuration
vpn 1
  host my-hostname ip 1.2.3.4
!
```

Configure one IPv4 and one IPv6 address for a host:

```
vEdge# show running-config vpn 0
vpn 0
 host my-vEdge ip 10.0.12.26 2001::a00:c1a
...
```

Operational Commands

show running-config vpn

host-mode

Set whether an 802.1X interface grants access to a single client or to multiple clients (on vEdge routers only).

By default, only one authenticated client is allowed on an 802.1X port.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      host-mode (multi-auth | multi-host | single-host)
```

Syntax Description

multi-auth	Multiple Authenticated Clients: A single 802.1X interface grants access to multiple authenticated clients on data VLANs.
multi-host	Multiple Clients: A single 802.1X interface grants access to multiple clients. Only one of the attached clients must be authorized for the interface to grant access to all clients. If the interface becomes unauthorized, the vEdge router denies network access to all attached clients.
single-host	Single Client: The 802.1X interface grants access only to the first authenticated client. All other clients attempting access are denied and dropped.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure the 802.1X interface to grant access to multiple clients:

```
vpn 0
  interface ge0/0
    dot1x
      multi-host
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

radius, on page 407

host-name

Configure a name for the vEdge device. This name is prepended to the device's prompt in the shell.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  host-name string
```

Syntax Description

string	Hostname: Specify the name of the host. The text can be a maximum of 32 characters. If it includes spaces, enclose the entire string in quotation marks (" ").

Command History

Release	Modification
14.1	Command introduced.

Example

Configure the hostname on a vEdge device:

```
vEdge(config)# system host-name vsmart1
vEdge(config)# commit and-quit
Commit complete.
vsmart1#
```

Operational Commands

show running-config system

host-policer-pps

For a policer, configure the rate to deliver packets to the control plane (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  host-policer-pps rate
```

Syntax Description

rate	Packet Delivery Rate: Maximum rate at which a policer delivers packets to the control plane, in packets per second (pps). Range: 1000 through 25000 pps Default: 20000 pps

Command History

Release	Modification
15.4	Command introduced.
16.3	Increase range from 20000 pps to 25000 pps, and change default from 5000 pps to 20000 pps.

Example

Change the maximum packet delivery message rate to 1000 pps:

```
system
  host-policer-pps 1000
```

Operational Commands

show running-config system

Related Topics

control-session-pps, on page 149
icmp-error-pps, on page 232
policer, on page 379

icmp-error-pps

For a policer, configure how many ICMP error messages can be generated or received per second (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  icmp-error-pps rate
```

Syntax Description

icmp-error-pps 0	Disable ICMP Error Message Generation: Configure a value of 0 to have a policer generate no ICMP error messages.
rate	ICMP Error Message Generation Rate: How many ICMP error messages a policer can generate or receive, in packets per second (pps). Range: 1 through 200 pps Default: 100 pps

Command History

Release	Modification
15.4	Command introduced.

Example

Change the maximum ICMP error message rate to 200 pps:

```
system
  icmp-error-pps 200
```

Operational Commands

show running-config system

Related Topics

control-session-pps, on page 149
host-policer-pps, on page 231
policer, on page 379

icmp-redirect-disable

Disable ICMP redirect messages on an interface (on vEdge routers only). By default, an interface allows ICMP redirect traffic.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPPConfiguration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id interface interface-name
        icmp-redirect-disable
```

Syntax Description

None

Example

Disable ICMP redirect traffic, and drop all ICMP redirect packets:

```
vEdge(config-vpn-0)# interface ge0/0
vEdge(config-interface-ge0/0)# icmp-redirect-disable
```

Operational Commands

show interface

Related Topics

allow-service, on page 63

idle-timeout

Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires.

This command sets the CLI idle timeout on a systemwide basis, and it overrides the idle timeout you set from the CLI with the **idle-timeout** CLI operational command.

Command Syntax

```
system
  idle-timeout minutes
```

Syntax Description

minutes	Timeout Value: Number of minutes that the CLI is idle before the user is logged out of the CLI. A value of 0 (zero) sets the time to infinity, so the user is never logged out. Range: 0 through 300 minutes (5 hours) Default: CLI session does not time out

Command History

Release	Modification
17.2.2	Command introduced.

Example

Configure CLI sessions to time out after 5 hours:

```
vEdge(config)# system idle-timeout 300
```

Operational Commands

show running-config system

Related Topics

idle-timeout, on page 639

igmp

Configure IGMP (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► IGMP

Command Hierarchy

```
vpn vpn-id
  router
    igmp
      interface interface-name
        join-group group-address
        [no] shutdown
```

Syntax Description

None

Command History

Release	Modification
14.3	Command introduced.

Example

Enable IGMP in VPN 1:

```
vm5(config-igmp)# show full-configuration
vpn 1
 router
  igmp
   interface ge0/4
   exit
   interface ge0/5
    join-group 239.239.239.239
    exit
```

```
   exit
  exit
 !
!
```

Operational Commands

clear igmp interface

clear igmp protocol

clear igmp statistics

show igmp groups

show igmp interface

show igmp statistics

show igmp summary

ike

To configure the Internet Key Exchange (IKE) protocol parameters on edge devices, use the **ike** command in global configuration mode. Cisco SD-WAN supports only IKE version 2 as defined in RFC 7296.

Command Hierarchy

Command Syntax on vEdge Devices:

```
vpn vpn-id
  interface ipsecnumber
    ike
      authentication-type type
        local-id id
        pre-shared-secret password
        remote-id id
      cipher-suite suite
      group number
      mode mode
      rekey seconds
      version number
```

Command Syntax on Cisco IOS XE SD-WAN Devices:

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

Syntax Description

version number	IKE Version: Specify the version of the IKE protocol to use. Cisco SD-WAN supports only IKE version 2 as defined in RFC 7296. Values: 1, 2 Default: 1 **Note** The IKEv1 is changed to IKEv2 protocol, if it is already in use on the older versions. We recommend to use IKEv2 to avoid packet loss.

Command History

Release	Modification
17.2	Command introduced.

Example

The following example shows the IKE configuration on vEdge devices:

```
vEdge# show running-config vpn 1 interface ipsec1 ike
vpn 1
  interface ipsec1
    ike
      version     2
      mode        main
      rekey       14400
      ciphersuite aes256-sha1
      group       16
      authentication-type
        pre-shared-key
        pre-shared-secret viptela
  !
!
```

The following example shows the IKE configuration on Cisco IOS XE SD-WAN devices:

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

implicit-acl-logging

Log the headers of all packets that are dropped because they do not match a service configured with an **allow-service** command (on vEdge routers only). 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, all dropped packets are logged. It is recommended that you limit the number of packets logged, by including the **log-frequency** command in the configuration. The default is to log every 512th packet.

vManage Feature Template

For vEdge routers:

Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Implicit ACL Logging field

Command Hierarchy

```
policy
  implicit-acl-logging
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Log implicitly configured packets, logging every 512th packet:

```
vEdge# show running-config policy
policy
 log-frequency 1000
 implicit-acl-logging
 ...
!
```

Operational Commands

clear app log flow-all

clear app log flows

show app log flow-count

show app log flows

Related Topics

allow-service, on page 63
log-frequency, on page 295

interface

Configure an interface within a VPN.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface IPsec

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    access-list acl-list (on vEdge routers only)
    arp (on vEdge routers only)
      ip ip-address mac mac-address
    arp-timeout seconds (on vEdge routers only)
    autonegotiate (on vEdge routers only)
    bandwidth-downstream kbps (on vEdge routers and vManage NMSs only)
    bandwidth-upstream kpbs (on vEdge routers and vManage NMSs only)
    block-non-source-ip (on vEdge routers only)
    clear-dont-fragment
    dead-peer-detection interval seconds retries number
    description text
    dhcp-helper ip-address (on vEdge routers only)
    dhcp-server (on vEdge routers only)
      address-pool prefix/length
      exclude ip-address
      lease-time seconds
      max-leases number
      offer-time minutes
      options
```

```
    default-gateway ip-address
    dns-servers ip-address
    domain-name domain-name
    interface-mtu mtu
    tftp-servers ip-address
  static-lease mac-address ip ip-address host-name hostname
dot1x
  accounting-interval seconds
  acct-req-attr attribute-number (integer integer | octet octet | string string)
  auth-fail-vlan vlan-id
  auth-order (mab | radius)
  auth-reject-vlan vlan-id
  auth-req-attr attribute-number (integer integer | octet octet | string string)
  control-direction direction
  das
    client ip-address
    port port-number
    require-timestamp
    secret-key password
    time-window seconds
    vpn vpn-id
  default-vlan vlan-id
  guest-vlan vlan-id
  host-mode (multi-auth | multi-host | single-host)
  mac-authentication-bypass
    allow mac-addresses
    server
  nas-identifier string
  nas-ip-address ip-address
  radius-servers tag
  reauthentication minutes
  timeout
    inactivity minutes
  wake-on-lan
duplex (full | half)
flow-control (bidirectional | egress | ingress)
icmp-redirect-disable
ike
  authentication-type type
    local-id id
    pre-shared-secret password
    remote-id id
  cipher-suite suite
  group number
  mode mode
  rekey-interval seconds
  version number
(ip address prefix/length | ip dhcp-client [dhcp-distance number])
(ipv6 address prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-commit])

ip address-list prefix/length (on vSmart containers only)
ip secondary-address ipv4-address (on vEdge routers only)
ipsec
  cipher-suite suite
  perfect-forward-secrecy pfs-setting
  rekey-interval seconds
  replay-window number
keepalive seconds retries (on vEdge routers only)
mac-address mac-address
mtu bytes
nat (on vEdge routers only)
  block-icmp-error
  direction (inside | outside)
  log-translations
```

```
      [no] overload
      port-forward port-start port-number1 port-end port-number2
        proto (tcp | udp) private-ip-address ip address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
     static source-ip ip-address1 translate-ip ip-address2 source-vpn vpn-id protocol (tcp
 | udp) source-port number translate-port number
      tcp-timeout minutes
      udp-timeout minutes
   pmtu (on vEdge routers only)
   policer policer-name (on vEdge routers only)
   ppp (on vEdge routers only)
     ac-name name
     authentication (chap | pap) hostname name password password
   pppoe-client (on vEdge routers only)
     ppp-interface name
   profile profile-id (on vEdge routers only)
   rewrite-rule name (on vEdge routers only)
   shaping-rate name (on vEdge routers only)
   shutdown
   speed speed
   static-ingress-qos number (on vEdge routers only)
   tcp-mss-adjust bytes
   technology technology (on vEdge routers only)
   tloc-extension interface-name (on vEdge routers only)
   tracker tracker-name (on vEdge routers only)
   tunnel-interface
     allow-service service-name
     bind geslot/port (on vEdge routers only)
     carrier carrier-name
     color color [restrict]
     connections-limit number
     encapsulation (gre | ipsec) (on vEdge routers only)
       preference number
       weight number
     hello-interval milliseconds
     hello-tolerance seconds
     low-bandwidth-link (on vEdge routers only)
     max-control-connections number (on vEdge routers only)
     nat-refresh-interval seconds
     vmanage-connection-preference number (on vEdge routers only)
   tunnel-destination ip-address (GRE interfaces; on vEdge routers only)
   tunnel-destination (dns-name | ipv4-address) (IPsec interfaces; on vEdge routers only)
   (tunnel-source ip-address | tunnel-source-interface interface-name) (GRE interfaces;
on vEdge routers only)
   (tunnel-source ip-address | tunnel-source-interface interface-name) (IPsec interfaces;
 on vEdge routers only)
   upgrade-confirm minutes
   vrrp group-name (on vEdge routers only)
     priority number
     timer seconds
     track-omp
```

Syntax Description

interface-name	Interface Name: Name of the interface. On vSmart controllers, interface-name can have one of the following formats: **eth** *slot*/*port*, **loopback** *string*, or **mgmt** *number*. If you specify the interface name in any other format, the CLI reports a failure when you issue the **validate** or **commit** command. No error is reported as you are typing the interface configuration command. On vEdge routers, interface-name can have one of the following formats: **ge** *slot*/*port*, **gre** *number*, **ipsec** *number*, **loopback** *string*, **mgmt** *number*, **natpool** *number*, or **ppp** *number*. If you specify the interface name in any other format, the CLI reports a failure when you issue the validate or commit command. No error is reported as you are typing the interface configuration command. For GRE interfaces, number can be 1 through 255. For IPsec interfaces, number can be 1 through 255. For loopback interfaces, string can be any alphanumeric value and can include underscores (_) and hyphens (–). The total interface name can be a maximum of 16 characters long (including the string "loopback"). For NAT pool interfaces, number can be 1 through 31. For IEEE 802.1Q VLANs, interface-name can have the format **ge** *slot*/*port*.*vlan-number*, where *vlan-number* can be in the range 1 through 4094. To enable VLAN interfaces, activate the physical interface in VPN 0, and then enable the VLAN in the desired VPN. You can place the VLANs associated with a physical interface into multiple VPNs. You can configure up to 512 interfaces on a vEdge device. This number includes physical interfaces, loopback interfaces, and subinterfaces. A particular interface can be present only in one VPN.

Command History

Release	Modification
14.1	Command introduced.
15.3	Add support for natpool interface type.
15.3.3	Add support for ppp interfaces.
15.4.1	Add support for GRE interfaces.
17.1	Add support for IPsec interfaces.

Example

Configure a tunnel interface in VPN 0 on a vEdge router:

```
vEdge# show running-config vpn 0
vpn 0
```

```
 interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
   color lte
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
  !
  speed        100
  no shutdown
  shaping-rate 100000
 !
!
```

Configure an interface in VPN 0 on a vEdge router with the PPPoE client:

```
vpn 0
 interface ge0/1
  pppoe-client ppp-interface ppp1
  no shutdown
 !
!
```

Operational Commands

show interface

show interface arp-stats

show interface errors

show interface packet-sizes

show interface port-stats

show interface queue

show interface statistics

show tunnel gre-keepalives

show tunnel statistics gre

interface

Associate an interface with a bridging domain (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Bridge

Command Hierarchy

```
bridge bridge-id
  interface interface-name
    description text
    native-vlan
    [no] shutdown
    static-mac-address mac-address
```

Syntax Description

[no] shutdown	Enable or Disable the Interface: By default, an interface in a bridge domain is disabled. To enable it, include the **no shutdown** command.
description *text*	Interface Description: Text description of the interface. If *text* contains spaces, enclose it in quotation marks.
interface-name	Interface Name: Name of the interface to associate with the bridging domain. Specify *interface-name* in the format **ge** *slot* /*port*.
native-vlan	Native VLAN: Treat untagged traffic as belonging to the VLAN in that particular bridge. Only one VLAN associated with an interface can be configured to run as native VLAN. Native VLAN is disabled by default.
static-mac-address *mac-address*	Static MAC Address Manually add static MAC address entries for an interface in a bridge domain.

Command History

Release	Modification
15.3	Command introduced.

Example

Configure three bridge domains on a vEdge router:

```
vEdge# show running-config bridge
bridge 1
 vlan 1
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/5
  no native-vlan
  no shutdown
 !
 interface ge0/6
```

```
  no native-vlan
  no shutdown
 !
!
bridge 2
 vlan 2
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/5
  no native-vlan
  no shutdown
 !
 interface ge0/6
  no native-vlan
  no shutdown
 !
!
bridge 50
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/5
  no native-vlan
  no shutdown
 !
 interface ge0/6
  no native-vlan
  no shutdown
 !
!
vEdge# show bridge interface
                        ADMIN   OPER    ENCAP                RX    RX      TX    TX
BRIDGE  INTERFACE  VLAN  STATUS  STATUS  TYPE   IFINDEX  MTU  PKTS  OCTETS  PKTS  OCTETS
-------------------------------------------------------------------------------------
1       ge0/2      1     Up      Up      vlan   34       1500 0     0       2     168
1       ge0/5      1     Up      Up      vlan   36       1500 0     0       2     168
1       ge0/6      1     Up      Up      vlan   38       1500 0     0       2     168
2       ge0/2      2     Up      Up      vlan   40       1500 0     0       3     242
2       ge0/5      2     Up      Up      vlan   42       1500 0     0       3     242
2       ge0/6      2     Up      Up      vlan   44       1500 0     0       3     242
50      ge0/2      -     Up      Up      null   16       1500 0     0       2     140
50      ge0/5      -     Up      Up      null   19       1500 0     0       2     140
50      ge0/6      -     Up      Up      null   20       1500 0     0       2     140
```

Operational Commands

show bridge interface

show bridge mac

show bridge table

interface

Configure the interfaces that participate in the IGMP domain, and configure the groups for the interface to join (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► IGMP

Command Hierarchy

```
vpn vpn-id
  router
    igmp
      interface interface-name
        join-group group-address
```

Syntax Description

interface-name	Interface Name: Name of the interface to participate in the IGMP domain.

Command History

Release	Modification
14.3	Command introduced.

Example

Enable IGMP in VPN 1:

```
vm5(config-igmp)# show full-configuration
vpn 1
 router
  igmp
   interface ge0/4
   exit
   interface ge0/5
    join-group 239.239.239.239
    exit
   exit
  exit
 !
!
```

Operational Commands

clear igmp interface

clear igmp protocol

clear igmp statistics

show igmp groups

show igmp interface

show igmp statistics

show igmp summary

interface

Configure virtual access points (VAPs) for SSIDs in a WLAN (on vEdge cellular wireless routers only).

On a vEdge100wm router, you can configure up to four service set identifiers (SSIDs) on the WLAN radio. Each SSID is referred to by a virtual access point (VAP) interface. To a client, each VAP interface appears as a different access point (AP) with its own SSID.

To reduce RF congestion, it is recommended that you do not configure more than two VAP interfaces on the router.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  interface vapnumber
    data-security security
    description text
    max-clients number
    mgmt-security security
    radius-servers tag
    [no] shutdown
    ssid ssid
    wpa-personal-key password
```

Syntax Description

[no] shutdown	Disable or Enable the VAP Interface: Disable or enable the VAP interface.
vap *number*	VAP Interface: VAP instance. Range: 0 through 3
description *text*	VAP Interface Description: Text description of the VAP interface. The text can be from 4 through 64 characters long.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure four VAP interfaces, for four SSIDs:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

interface

Configure the properties of an interface in an OSPF area (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          authentication
            authentication-key key
            message-digest key
            type (message-digest | simple)
          cost number
          dead-interval seconds
          hello-interval seconds
          network (broadcast | point-to-point)
          passive-interface
          priority number
          retransmit-interval seconds
```

Syntax Description

interface-name	Interface Name: Name of the interface, in the format **ge** *slot/port* or **loopback** *number*.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure interface *ge0/0* to be in area 0:

```
vm1# show running-config vpn 1 router ospf area 0
vpn 1
 router
ospf
   area 0
    interface ge0/0
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

interface

Configure the interfaces that participate in the PIM domain, and configure PIM timers for the interfaces (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      interface interface-name
        hello-interval seconds
        join-prune-interval seconds
```

Syntax Description

interface-name	Interface Name: Name of the interface, in the format **ge** *slot*/*port*..

Command History

Release	Modification
14.2	Command introduced.

Example

Configure interface ge3/0 to participate in the PIM domain:

```
vEdge# show running-config vpn 1 router pim vpn 3
 router
  pim
   interface ge3/0
   exit
  exit
 !
!
```

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show pim interface

show pim neighbor

show omp multicast-auto-discover

show omp multicast-routes

interface gre

Configure a GRE tunnel interface interface in the transport VPN (on vEdge routers only).

GRE interfaces are logical interfaces, and you configure them just like any other physical interface. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface GRE

Command Hierarchy

```
vpn 0
  interface grenumber
    access-list acl-name
    block-non-source-ip
    clear-dont-fragment
    description text
    ip address prefix/length
    keepalive seconds retries
    mtu bytes
    [no] nat-port-overload
    policer policer-name
    rewrite-rule rule-name
    tcp-mss-adjust bytes
    tunnel-destination ip-address
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

Syntax Description

gre *number*	Interface Name Name of the GRE interface.*number* can be a value from 1 through 255.

Turning off port translation

Normally, traffic sent over IPSec/GRE tunnel to zScalar is translated using port is translation. In this scenario, each IPSec or GRE tunnel can carry only 64000 streams.

Use the **no nat-port-overload** command to turn off the port translation of traffic on GRE and IPsec tunnels. When port translation is turned off, each IPSec or GRE tunnel can carry only 64000 streams over a single IPSec/GRE tunnel.

Note Port translation can be turned off when service-side traffic does not use overlapping IP addresses. We do not recommend turning off port translation when service-side traffic uses overlapping IP address.

Note When the command is in use, the fragmentation reassembly and address reuse across VPNs is not supported.

Command History

Release	Modification
14.1	Command introduced.
15.4.1	Support for GRE interfaces added.
19.2.31	Support for nat-port-overload is added.

Example

Configure a GRE tunnel interface in VPN 0:

```
vEdge# show running-config vpn 0
vpn 0
 interface gre1
  ip address 172.16.111.11/24
  keepalive 60 10
  nat-port-overload
  tunnel-source 172.16.255.11
  tunnel-destination 10.1.2.27
  no shutdown
 !
!
```

Operational Commands

show interface

show tunnel statistics gre

interface ipsec

Configure an IKE-enabled IPsec tunnel that provides authentication and encryption to ensure secure packet transport (on vEdge routers only). You can create the IPsec tunnel in the transport VPN (VPN 0) and in any service VPN (VPN 1 through 65530, except for 512).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    dead-peer-detection interval seconds retries number
    description text
    ike
      authentication-type type
        local-id id
        pre-shared-secret password
        remote-id id
      cipher-suite suite
      group number
      mode mode
      rekey seconds
      version number
    ip address ipv4-prefix/length
    ipsec
      cipher-suite suite
      perfect-forward-secrecy pfs-setting
      rekey seconds
      replay-window number
    mtu bytes
    [no] shutdown
    [no] nat-port-overload
    tcp-mss-adjust bytes
    tunnel-destination (dns-name | ipv4-address)
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

Syntax Descrption

description *text*	Interface Description: Text description of the **ipsec** interface. The text can be a maximum of 128 characters. If it includes spaces, enclose the entire string in quotation marks (" ").
ipsec *number*	Interface Name: Number of the **ipsec** interface. Range: 1 through 255

Command History

Release	Modification
17.2	Command introduced.
18.2	Add support for IPsec tunnels in VPN 0.
19.2.31	Support for nat-port-overload is added.

Turning off port translation

Normally, traffic sent over IPSec/GRE tunnel to zScalar is translated using port is translation. In this scenario, each IPSec or GRE tunnel can carry only 64000 streams.

Use the **no nat-port-overload** command to turn off the port translation of traffic on GRE and IPsec tunnels. When port translation is turned off, each IPSec or GRE tunnel can carry only 64000 streams over a single IPSec/GRE tunnel.



Note Port translation can be turned off when service-side traffic does not use overlapping IP addresses. We do not recommend turning off port translation when service-side traffic uses overlapping IP address.



Note When the command is in use, the fragmentation reassembly and address reuse across VPNs is not supported.

Example

Configure IKEv1 on a router:

```
vEdge# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.1/30
  tunnel-source       10.1.15.15
  tunnel-destination  10.1.16.16
  dead-peer-detection interval 10 retries 3
  ike
   version     1
   mode         main
   rekey       14400
   cipher-suite aes256-sha1
   group       16
   authentication-type
    pre-shared-key
     pre-shared-secret viptela
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 512
   cipher-suite  aes256-cbc-sha1
  !
  flow-control        autoneg
  no clear-dont-fragment
  no pmtu
  mtu                 1500
  nat-port-overload
  autonegotiate
  shutdown
  arp-timeout         1200
  no block-non-source-ip
 !
!
```

Operational Commands

clear ipsec ike sessions

request ipsec ike-rekey

request ipsec ipsec-rekey

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

interface irb

Configure an interface to use for integrated routing and bridging (IRB) (on vEdge routers only).

vManage Feature Template

For vEdge routers:

Configuration ► Templates ► VPN Interface Bridge

Command Hierarchy

```
vpn vpn-id
  interface irbnumber
    access-list acl-list
    arp
      ip ip-address mac mac-address
    arp-timeout seconds
    block-non-source-ip
    clear-dont-fragment
    description text
    dhcp-helper ip-address
    dhcp-server
      address-pool prefix/length
      exclude ip-address
      lease-time seconds
      max-leases number
      offer-time minutes
      options
        default-gateway ip-address
        dns-servers ip-address
        domain-name domain-name
        interface-mtu mtu
        tftp-servers ip-address
      static-lease mac-address ip ip-address host-name hostname
    (ip address prefix/length | ip dhcp-client [dhcp-distance number])
    ip address-list prefix/length (on vSmart containers only)
    mac-address mac-address
    mtu bytes
    [no] shutdown
    static-ingress-qos number
    tcp-mss-adjust bytes
    vrrp group-name
      priority number
      timer seconds
      track-omp
```

Syntax Description

irb *number*	Interface Name: Name of the interface. *number* can from 1 through 63, and it must be the same number as the the identifier of the bridging domain that the IRB is connected to, as configured with the **bridge** command.

Command History

Release	Modification
15.3	Command introduced.

Example

Configure two IRB interfaces:

```
vEdge# show running-config vpn 1
vpn 1
interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
!
interface irb1
  ip address 1.1.1.15/24
  no shutdown
  access-list IRB_ICMP in
  access-list IRB_ICMP out
!
interface irb50
  ip address 3.3.3.15/24
  no shutdown
 !
!
vEdge# show running-config vpn 2
vpn 2
interface irb2
  ip address 2.2.2.15/24
  no shutdown
 !
!
```

Operational Commands

show interface

Related Topics

bridge, on page 115

interface ppp

Configure the Point-to-Point Protocol over Ethernet (PPPoE) (on vEdge routers only).

vManage Feature Template

For vEdge router:

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    access-list acl-list
    arp
      ip ip-address mac mac-address
    arp-timeout seconds
    autonegotiate
    clear-dont-fragment
    description text
    duplex (full | half)
    flow-control (bidirectional | egress | ingress)
    (ip address prefix/length | ip dhcp-client [dhcp-distance number])
    (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [
dhcp-rapid-commit]
    keepalive seconds retries
    mac-address mac-address
    mtu bytes
    policer policer-name
    pppoe-client
      ppp-interface name
    rewrite-rule name
    shaping-rate name
    shutdown
    speed speed
    static-ingress-qos number
    tcp-mss-adjust bytes
    tloc-extension interface-name
```

Syntax Description

ppp *number*	Interface Name: Number of the PPP interface. *number* can be from 1 through 31.

Command History

Release	Modification
15.3	Command introduced.
16.3	Add support for IPv6.

Example

Configure PPPoE:

```
vEdge# show running-config vpn 0
vpn 0
interface ge0/1
```

```
  pppoe-client ppp-interface ppp10
  no shutdown
!
interface ppp10
  ppp authentication chap
   hostname branch100@corp.bank.myisp.net
   password $4$OHHjdmsC6M8zj4BgLEFXKw==
  !
  tunnel-interface
   encapsulation ipsec
   color gold
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service ospf
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
  !
  mtu      1492
  no shutdown
 !
!
```

Operational Commands

show interface

show ppp interface

show pppoe session

integrity-type

To configure the type of integrity check performed on IPSec packets, use the **security ipsec integrity-type** command in IPsec configuration mode. To delete the authentication type, use the **no** form of this command.

integrity-type { **none** | **ip-udp-esp** | **ip-udp-esp-no-id** | **esp** }

no 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, the default integrity-type is `ip-udp-esp esp`.

Command Modes

IPSec configuration (config-ipsec)

Command History

Release	Modification
Cisco SD-WAN Release 20.6.1	This command was introduced. **Note** From Cisco SD-WAN Release 20.6.1, this command replaces the **authentication-type** command.

Usage Guidelines

Configure each integrity type separately using the **security ipsec integrity-type** command.

Example

```
Device# configure
Device(config)# security
Device(config-security)# ipsec
Device(config-ipsec)# integrity-type esp
```

ip address

Configure an interface's IPv4 address as a static address (on vEdge routers and vSmart controllers only). To configure the interface to receive its IP address from a DHCP server, use the **ip dhcp-client** command.

vManage Feature Template

For vEdge routers and vSmart controllers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface IPsec

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    (ip address ipv4-prefix/length | ip dhcp-client [dhcp-distance number])
```

Syntax Description

ipv4-prefix/length	IP Address: IPv4 address of the interface. Specify the prefix in decimal four-part dotted notation. For loopback and NAT pool interfaces, the length must be /32. The address cannot be the same as the system IP address that is configured in VPN 0.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure an interface's IP address:

```
vEdge# show running-config vpn 1 interface ge0/4
vpn 1
 interface ge0/4
  description "VPN 1 interface"
  ip address 10.20.25.16/24
  no shutdown
 !
!
```

Operational Commands

show interface

show ipv6 interface

Related Topics

ip dhcp-client, on page 262
ipv6 address, on page 272
ipv6 dhcp-client, on page 274
system-ip, on page 470
ip secondary-address, on page 269

ip address-list

Configure the IP addresses reachable by the interfaces on a container (on vContainer hosts only). You configure IP addresses in the WAN transport VPN (VPN 0) and in the management interface VPN (VPN 512) only.

Command Hierarchy

```
vpn vpn-id
  interface eth number
    ip address-list prefix/length
```

Syntax Description

interface eth *number*	Interface Name: Name of the interface on the container. The first interface is **eth1**.
ip address-list *prefix/length*	IP Address List: Network address available on the interface.
vpn *vpn-id*	VPN Identifier: VPN for the interfaces. *vpn-id* can be either 0 (for the WAN transport VPN) or 512 (for the management VPN).

Command History

Release	Modification
16.2	Command introduced.

Example

Configure IP address lists, and configure containers for three vSmart controllers on a container host:

```
vContainer# show running-config container
container
 instance first_vsmart
  image    16.2.0
  no shutdown
  memory   512
  allow-address 35.197.204.176/32 0 all
  allow-address 35.232.118.121/32 0 all
  interface eth0
   host-ip-address 10.0.1.25
  !
 !
 instance second_vsmart
  image    16.2.0
  no shutdown
  memory   512
  allow-address 35.197.204.176/32 0 all
  allow-address 35.232.118.121/32 0 all
  interface eth0
   host-ip-address 10.0.1.26
  !
 !
 instance vm10
  image    16.2.0
  no shutdown
  memory   512
  allow-address 35.197.204.176/32 0 all
  allow-address 35.232.118.121/32 0 all
  interface eth0
   host-ip-address 10.0.1.30
  !
  interface eth1
   host-ip-address 10.0.12.20
  !
  interface eth2
```

```
   host-ip-address 10.2.2.20
  !
 !
!
vpn 0
 interface eth1
  ip address-list 10.0.1.25/24
  ip address-list 10.0.1.26/24
  ip address-list 10.0.1.27/24
  ip address-list 10.0.1.30/24
  ip static-route 0.0.0.0/0 10.0.1.1
  no shutdown
 !
 interface eth2
  ip address-list 10.2.2.20/24
  ip address-list 10.2.2.25/24
  ip address-list 10.2.2.26/24
  ip address-list 10.2.2.27/24
  ip static-route 0.0.0.0/0 10.2.2.1
  no shutdown
 !
 interface eth3
  ip address-list 10.0.12.20/24
  ip static-route 0.0.0.0/0 10.0.12.13
  no shutdown
 !
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

Operational Commands

request container image install

request container image remove

show container images

show container instances

Related Topics

container, on page 145

ip dhcp-client

Configure an interface in the WAN transport VPN (VPN 0) to receive its IPv4 address from a DHCPv4 server. To configure the interface's IPv4 address as a static address, use the **ip address** command.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    (ip address ip-address/length | ip dhcp-client [dhcp-distance number])
```

Syntax Description

dhcp-distance *number*	Administrative Distance: Set the administrative distance of routes learned from a DHCP server. Range: 1 through 255 Default: 1

Command History

Release	Modification
14.1	Command introduced.

Example

Configure an interface in VPN 0 to receive its IP address from a DHCP server:

```
vEdge# show running-config vpn 0 interface ge0/7
vpn 0
 interface ge0/4
  ip dhcp-client
  no shutdown
 !
!
```

Operational Commands

clear dhcp server-bindings

clear dhcp state

show dhcp interface

show interface

show ipv6 dhcp interface

show ipv6 interface

Related Topics

ip address, on page 259
ipv6 address, on page 272
ipv6 dhcp-client, on page 274

ip gre-route

Configure a GRE-specific static route in a service VPN (a VPN other than VPN 0 or VPN 512) to direct traffic from the service VPN to a GRE tunnel (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  ip gre-route prefix/length vpn 0 interface gre number [gre number2]
```

Syntax Description

gre *number* [**gre** *number2*]	GRE Interface Name: Name of the GRE tunnel used to reach the service. If you configure two interfaces, the first is the primary GRE tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary GRE tunnel
prefix/length	Prefix of GRE Static Route: IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.

Command History

Release	Modification
15.4.3	Command introduced.

Example

Configure a GRE-specific static route so that traffic from the 58.0.1.0/24 network can reach the GRE interfaces in VPN 0:

```
vEdge# show running-config
vpn 0
  interface gre1
    ip address 10.0.111.11/24
    keepalive 60 10
    tunnel-source 10.0.5.11
    tunnel-destination 172.168.1.1
    no shutdown
  !
  interface gre2
    ip address 10.0.122.11/24
    tunnel-source 10.0.5.11
```

```
    tunnel-destination 172.168.122.11
    no shutdown
  !
!
vpn 1
  ip gre-route 58.0.1.0/24 vpn 0 interface gre1 gre2
```

Operational Commands

show interface

show tunnel gre-keepalives

show tunnel statistics

Related Topics

ip route, on page 267
keepalive, on page 279
nat, on page 346

ip ipsec-route

Configure an IPsec-specific static route in a service VPN (a VPN other than VPN 0 or VPN 512) to direct traffic from the service VPN to an IPsec tunnel (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  ip ipsec-route prefix/length vpn 0 interface ipsecnumber [ipsecnumber2]
```

Syntax Description

ipsec*number* [**ipsec***number2*]	IPsec Interface Name: Name of the IPsec tunnel interface. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.
prefix/*length*	Prefix of IPsec Static Route: IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.

Command History

Release	Modification
18.2	Command introduced.

Example

Configure an IPsec-specific static route in VPN 100 to direct traffic from that VPN to an IPsec tunnel in VPN 0. In VPN 0, the primary IPsec tunnel is the interface *ipsec1* and the secondary IPsec tunnel is *ipsec2*.

```
vEdge# show running-config vpn 0
vpn 0
 interface ipsec1
  ip address 10.0.111.1/30
  tunnel-source-interface ge0/0
  tunnel-destination      172.168.1.1
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        14
   authentication-type
    pre-shared-key
     pre-shared-secret R9VuFaRK7yxTUDtTrcK+
     local-id          admin@my-company.com
    !
   !
  !
  ipsec
   rekey                  3600
   replay-window          512
   cipher-suite           null-sha1
   perfect-forward-secrecy group-16
  !
  mtu                    1400
  tcp-mss-adjust         1300
  no shutdown
 !
 interface ipsec2
  ip address 10.0.111.5/30
  tunnel-source-interface ge0/0
  tunnel-destination      192.168.1.1
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        14
   authentication-type
    pre-shared-key
     pre-shared-secret R9VuFaRK7yxTUDtTrcK+
     local-id          admin@my-company.com
    !
   !
  !
  ipsec
   rekey                  3600
   replay-window          512
   cipher-suite           null-sha1
   perfect-forward-secrecy group-16
```

```
  !
  mtu                       1400
  tcp-mss-adjust            1300
  no shutdown
 !
!
vEdge# show running-config vpn 100
vpn 100
 ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1 ipsec2
!
```

Operational Commands

show interface

show tunnel statistics

Related Topics

ip gre-route, on page 264
ip route, on page 267
keepalive, on page 279
nat, on page 346

ip route

Configure an IPv4 static route in a VPN.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  ip route prefix/length next-hop [administrative-distance]
```

Syntax Description

prefix/length	Address of Static Route: IP address or prefix, in decimal four-part-dotted notation, and prefix length of the static route.
administrative-distance	Administrative Distance of Route: Assign an administrative distance to the route. This value is used to determine the best route when multiple paths exist to the same destination. Range: 1 through 255 Default: 1

next-hop	Next Hop towards the Destination: IP address of the next hop to reach the static route. The next hop can be one of the following • *ip-address*—IP address of the next-hop router. • **null0**—Next hop is the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **vpn 0**—Direct packets to the transport VPN. If NAT is enabled on the WAN interface, the packets can be forwarded to an Internet destination or other destination outside of the overlay network, effectively converting the vEdge router into a local Internet exit point. You must also enable NAT on a transport interface in VPN 0. **Note** Each tunnel establish control connection with the controller. For the control connection to be established, the control packet should go via the tunnel interface. If there are multiple specific routes (static/dynamically learnt) to reach the controller, the path with longest match is chosen. Hence, same outgoing interface will be used. The control connection will not be established via other interfaces. To overcome this, its recommended to configure static routes to reach the controller via each interface.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure a static route to the prefix 0.0.0.0/0 via the next hop at 10.10.0.1:

```
vpn 0
  ip route 0.0.0.0/0 10.10.0.1
```

Operational Commands

show ip routes (for IPv4 routes)

show ipv6 routes

Related Topics

ip gre-route, on page 264
ipv6 route, on page 275
nat, on page 346

ip secondary-address

Configure secondary IPv4 addresses for a service-side interface (on vEdge routers only).

You can configure secondary addresses only on interfaces whose primary address is configured with the **ip address** command. You cannot configure secondary addresses on interfaces that learn their primary address from DHCP (configured with the **ip dhcp-client** command).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    ip secondary-address ipv4-address
```

Syntax Description

ipv4-address	IP Address: IPv4 address of the interface, in decimal four-part dotted notation. You can configure secondary IPv4 addresses for **ge** and **irb** interfaces in all VPNs except for VPN 0 and VPN 512. The address cannot be the same as the system IP address that is configured in VPN 0. You can configure up to four secondary IPv4 addresses per interface.

Command History

Release	Modification
17.1	Command introduced.

Example

Configure one secondary IPv4 address:

```
vEdge# show running-config vpn 1 interface ge0/4
vpn 1
 interface ge0/4
  description "VPN 1 interface"
  ip address 10.20.25.16/24
  secondary-address 192.168.14.12/24
  no shutdown
 !
!
```

Operational Commands

ping

show interface

show ipv6 interface

Related Topics

ip address, on page 259
ip dhcp-client, on page 262
ipv6 address, on page 272
ipv6 dhcp-client, on page 274
system-ip, on page 470

ipsec

Configure the IPsec tunnel to use for IKE key exchange (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsec number
    ipsec
      cipher-suite suite
      perfect-forward-secrecy pfs-setting
      rekey seconds
      replay-window number
```

Syntax Desription

None

Command History

Release	Modification
17.2	Command introduced.

Example

View the default configuration for the IPsec tunnel used for IKE key exchange:

```
vEdge# show running-config vpn 1 interface ipsec1 ipsec
vpn 1
  interface ipsec1
  ipsec
   rekey 14400
   replay-window 512
   cipher-suite aes256-cbc-sha1
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

ike, on page 236

ipsec

Configure parameters for IPsec tunnel connections (on vEdge routers only).

Command Hierarchy

```
security
  ipsec
    authentication-type type
    rekey seconds
    replay-window number
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Shorten the IPsec rekeying interval:

```
vEdge# config
Entering configuration mode terminal
vm6(config)# security ipsec rekey ?
Possible completions:
  <600..172800 seconds>[3600]
vm6(config)# security ipsec rekey 600
```

Operational Commands

show security-info

Related Topics

request security ipsec-rekey, on page 700

iptables-enable

Enable the collection of iptable packet-filtering chains for all DTLS peers (on vSmart controllers and vManage NMSs only).

In Release 15.4, it is recommended that you do not enable iptables.

Command Hierarchy

```
system
  iptables-enable
```

Syntax Description

None

Command History

Release	Modification
15.4.3	Command introduced.
16.1	**iptables-enable** is enabled by default.

Example

Enable the use of iptables:

Enable the use of iptables:

```
vSmart(config)# system iptables-enable
```

Operational Commands

show system netfilter

ipv6 address

Configure a static IPv6 address on an interface. To configure the interface to receive its IP address from a DHCP server, use the **ipv6 dhcp-client** command.

You can configure IPv6 only on WAN transport interfaces, that is, only on interfaces in VPN 0 on vEdge routers and Cisco IOS XE SD-WAN devices.

If you configure both IPv4 and IPv6 static addresses on an interface, the IPv4 addresses take precedence and no IPv6 data plane tunnels are established.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number]
[dhcp-rapid-commit])
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Example

Configure an IPv6 WAN transport interface:

```
vEdge(config)# vpn 0 interface ge0/3
vEdge(config-interface)# ipv6 address fd00:1234::/16
vEdge(config-interface)# no shutdown
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# color green
vEdge(config-tunnel-interface)# encapsulation ipsec
vEdge(config-tunnel-interface)# commit and-quit
vEdge# show running-config vpn 0 interface ge0/3
vpn 0
 interface ge0/3
  ipv6 address fd00:1234::/16
  tunnel-interface
   encapsulation ipsec
   color green
   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
  !
  no shutdown
 !
!
```

Operational Commands

show interface

show ipv6 interface

Related Topics

ip address, on page 259
ipv6 address, on page 272
ipv6 dhcp-client, on page 274
system-ip, on page 470

ipv6 dhcp-client

Configure an interface in the WAN transport VPN (VPN 0) to receive its IPv6 address from a DHCPv6 server. To configure the interface's IPv6 address as a static address, use the **ipv6 address** command.

You can configure IPv6 only on WAN transport interfaces, that is, only on interfaces in VPN 0.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number]
[dhcp-rapid-commit])
```

Syntax Description

dhcp-distance *number*	Administrative Distance: Set the administrative distance of routes learned from a DHCP server. Range: 1 through 255 Default: 1
dhcp-rapid-commit	Rapid Commit: Enable the DHCPv6 rapid commit option to speed up the assignment of IP addresses. Rapid commit uses a two-message exchange to expedite address assignment.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure an IPv6 WAN transport interface to use a dynamic IPv6 address, and enable the rapid commit option for DHCPv6:

```
vEdge(config)# vpn 0 interface ge0/3
vEdge(config-interface)# ip6 dhcp-client
vEdge(config-interface)# no shutdown
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# color green
vEdge(config-tunnel-interface)# encapsulation ipsec
vEdge(config-tunnel-interface)# commit and-quit
vEdge# show running-config vpn 0 interface ge0/3
vpn 0
 interface ge0/3
  ipv6 dhcp-client
  ipv6 dhcp-rapid-commit
  tunnel-interface
   encapsulation ipsec
   color green
   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
  !
  no shutdown
 !
!
```

Operational Commands

clear dhcp state

show ipv6 dhcp interface

show ipv6 interface

Related Topics

ip address, on page 259
ipv6 address, on page 272

ipv6 route

Configure an IPv6 static route in a VPN (on vEdge routers only).

In Release 16.3, you can configure IPv6 only in VPN 0.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn 0
  ipv6 route prefix/length next-hop [administrative-distance]
```

Syntax Description

prefix/length	Address of Static Route: IPv6 address of the static route, written as the prefix and prefix length.
administrative-distance	Administrative Distance of Route: Assign an administrative distance to the route. This value is used to determine the best route when multiple paths exist to the same destination.*Range:* 1 through 255*Default:* 0
next-hop	Next Hop towards the Destination: IPv6 address of the next hop to reach the static route. The next hop can be one of the following: • *ipv6-address*—IP address of the next-hop router. • **null0**—Next hop is the null interface. All packets sent to this interface are dropped without sending any ICMPv6 messages.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure a static route to the prefix with a next hop of the null interface:

```
vpn 0
  ipv6 route 2001:1111:2222:3333::/64 null0
```

Operational Commands

show ip routes (for IPv4 routes)

show ipv6 routes

Related Topics

ip route, on page 267

join-group

Configure an interface on the vEdge router to initiate a request to join a multicast group (on vEdge routers only). Configuring this command does not cause the vEdge router to behave like a host.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► IGMP

Command Hierarchy

```
vpn vpn-id
  router
    igmp
      interface interface-name
        join-group group-address
```

Syntax Description

group-address	Multicast Group To Join: Address of the multicast group to join.

Command History

Release	Modification
14.3	Command introduced.

Example

Enable IGMP in VPN 1:

```
vm5(config-igmp)# show full-configuration
vpn 1
 router
  igmp
   interface ge0/4
   exit
   interface ge0/5
    join-group 239.239.239.239
    exit
   exit
  exit
 !
!
```

Operational Commands

clear igmp interface

clear igmp protocol

clear igmp statistics

show igmp groups

show igmp interface

show igmp statistics

show igmp summary

join-prune-interval

Modify the PIM join/prune message interval for an interface (on vEdge routers only). The join/prune interval sets when PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      interface interface-name
        join-prune-interval seconds
```

Syntax Description

seconds	Join/Prune Interval Time: PIM join/prune message interval. vEdge routers send join/prune messages to their upstream RPF neighbor. Range: 10 through 600 seconds Default: 60 seconds

Command History

Release	Modification
14.2	Command introduced.

Example

Change the PIM join/prune message interval to 360 seconds:

```
vEdge# show running-config vpn 1 router pim vpn 3
router
  pim
   interface ge3/0
    join-prune-interval 360
```

```
   exit
  exit
 !
!
```

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show pim interface

show pim neighbor

show omp multicast-auto-discover

show omp multicast-routes

keepalive

Configure how often a GRE interface sends keepalive packets (on vEdge routers only). The sending of keepalive packets is enabled by default.

Because GRE tunnels are stateless, the sending of keepalive packets is the only way to determine whether the remote end of the tunnel is up. The keepalive packets are looped back to the sender. Receipt of these packets by the sender indicates that the remote end of the GRE tunnel is up.

In Releases 17.1 and later, GRE interfaces behind a NAT device send keepalive messages. If you configure an IP address for the GRE interface, it is that address that sends the keepalive messages.

If the vEdge router sits behind a NAT and you have configured GRE encapsulation, you must disable keepalives. To do this, include a **keepalive 0 0** command in the configuration. You cannot disable keepalives by issuing a **no keepalive** command. This command returns the keepalive to its default settings.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface grenumber
    keepalive seconds retries
```

Syntax Description

seconds	Keepalive Time: How often the GRE interface sends keepalive packets on the GRE tunnel. Range: 0 through 65535 seconds Default: 10 seconds
retries	Keepalive Retries How many times the GRE interface tries to resend keepalive packets before declaring the remote end of the GRE tunnel to be down. With the default keepalive time of 10 seconds and the default retry of 3 times, if the router receives no looped-back keepalive packets from the remote end of the GRE tunnel, the tunnel would be declared to be down after 40 seconds. Range: 0 through 255 Default: 3

Command History

Release	Modification
15.4.1	Command introduced.
17.1	Add support for GRE interfaces to send keepalive messages.

Example

Configure the keepalive time for a GRE tunnel:

```
vEdge(config-vpn-0)# interface gre1
vEdge(config-interface-gre1)# keepalive 60 10
vEdge(config-interface-gre1)# show full configuration
vpn 0
 interface gre1
  ip address 10.0.111.11/24
  keepalive 60 10
  tunnel-source      10.0.5.11
  tunnel-destination 172.168.1.1
  no shutdown
 !
!
```

Operational Commands

show interface

show tunnel gre-keepalive

show tunnel statistics

Related Topics

tunnel-destination, on page 511
tunnel-source, on page 515

last-resort-circuit

Use the tunnel interface as the circuit of last resort (on vEdge routers). By default, this feature is disabled, and the tunnel interface is not considered to be the circuit of last resort.

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.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      [no] last-resort-circuit
```

Syntax Description

None

Command History

Release	Modification
16.2	Command introduced.

Example

Configure the **cellular0** interface to be the circuit of last resort for the vEdge router:

```
vEdge# show running-config vpn 0 interface cellular0
vpn 0
 interface cellular0
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color lte
   last-resort-circuit
   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
  !
  clear-dont-fragment
  mtu                1428
  profile            1
  no shutdown
 !
!
vEdge# show running-config bfd
bfd color lte
 hello-interval 300000
 no pmtu-discovery
!
```

Operational Commands

show control affinity config

show control local-properties

show interface

Related Topics

bfd color, on page 106

lease-time

Configure the time period for which a DHCP-assigned IP address is valid (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      lease-time seconds
```

Syntax Description

seconds	Lease Time: How long DHCP-assigned addresses are valid. Range: 60 through 4294967295 seconds

Command History

Release	Modification
14.3	Command introduced.

Example

Set the DHCP lease time to 2 hours:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server address-pool 10.0.100.0/24
vEdge(config-dhcp-server)# exclude 10.0.100.2
vEdge(config-dhcp-server)# lease-time 7200
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   address-pool 10.0.100.0/24
   exclude      10.0.100.2
   lease-time   7200
  !
 !
!
```

Operational Commands

show dhcp interfaces

show dhcp server

lists

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 (on vSmart controllers and vEdge routers only).

In the configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these list. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. Here are two examples of lists that are configured with ranges and that contain overlapping values:

- vpn-list list-1 vpn 1-10

  vpn-list list-2 vpn 6-8

- site-list list-1 site 1-10

  site-list list-2 site 5-15

For all lists except for site lists, when you configure policies that contain lists with overlapping values, or when you apply the policies, you must ensure that the lists do not contain overlapping values. To do this, you must manually audit your configurations. Cisco SD-WAN performs no validation on the contents of lists, on the policies themselves, or on how the policies are applied to ensure that there are no overlapping values. If you configure or apply policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Cisco SD-WAN when it processes the configuration. This decision is not under user control, and so the outcome is not predictable.

For site lists, for each type of policy that is applied to site lists—**app-route-policy**, **cflowd**, **control-policy**, **data-policy**—you must ensure for that policy type that the lists do not contain any overlapping sites. Each site must be unique and used only once. However, across these four different policy types, the sites in the site lists can overlap. For example, if you apply a **data-policy** to sites 100-200, you can apply a **control-policy** to sites 120-130 or to sites 190-210, and you can apply an **app-route-policy** to sites 100-125. However, you cannot apply a second **data-policy** to sites 120-130. For a configuration example that illustrates this behavior, see **apply-policy** .

vManage Feature Template

For vEdge routers and vSmart controllers:

Configuration ► Policies

Command Hierarchy

For Application-Aware Routing Policy:

```
policy
  lists
    app-list list-name
      (app application-name | app-family application-family)
    data-prefix-list list-name
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn vpn-id
```

For Centralized Control Policy:

```
policy
  lists
    color-list list-name
      color color
    prefix-list list-name
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id
```

For Centralized Data Policy

```
policy
  lists
    app-list list-name
      (app application-names | app-family application-family)
    data-prefix-list list-name
      ip-prefix prefix/length
```

```
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id
```

For Localized Control Policy

```
policy
  lists
    as-path-list list-name
      as-path path-list
    community-list list-name
      community [aa:nn | internet | local-as | no-advertise | no-export]
    ext-community-list list-name
      community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
    prefix-list list-name
      ip-prefix prefix/length
```

For Localized Data Policy (ACLs)

```
policy
  lists
    data-prefix-list list-name
      ip-prefix prefix/length
```

Syntax Description

For Application-Aware Routing Policy:

app-list *list-name* (**app** *application-name* | **app-family** *application-family*)	Application List: List of one or more applications or application families running on the subnets connected to the vEdge router. 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, specifying one application or application family in each **app** or **app-family** option. The number of app-list entries is limited to 8192. *application-name* is the name of an application family. Cisco SD-WAN software supports about 2300 different applications. To list the supported applications, use the *?* in the CLI. The number of app name entries is limited to 8192. *application-family* is the name of an application family. It can be one of the following: *antivirus*, *application-service*, *audio_video*, *authentication*, *behavioral*, *compression*, *database*, *encrypted*, *erp*, *file-server*, *file-transfer*, *forum*, *game*, *instant-messaging*, *mail*, *microsoft-office*, *middleware*, *network-management*, *network-service*, *peer-to-peer*, *printer*, *routing*, *security-service, standard*, *telephony*, *terminal*, *thin-client*, *tunneling*, *wap*, *web*, and *webmail*. The number of app-family entries is limited to 32.
data-prefix-list *list-name* **ip-prefix** *prefix/length*	Data Prefix List: List of one or more IP prefixes. The number of data-prefix-list entries is limited to 8192. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. The number of ip-prefix entries is limited to 8192.

site-list *list-name* **site-id** *site-id*	Overlay Network Site List List of one or more identifiers of sites in Cisco SD-WAN overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. To configure a range of site IDs, separate the IDs with hyphens. In application-aware routing policy, you apply a centralized control policy (with the **apply-policy** command) by site list.
vpn-list *list-name* **vpn** *vpn-id*	VPN List: List of one or more identifiers of VPNs in Cisco SD-WAN overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. The number of vpn entries is limited to 128. To configure a range of VPN IDs, separate the IDs with hyphens. In application-aware routing policy, you group policy sequences within VPN lists, with the policy **vpn-list sequence** command..

For Centralized Control Policy:

color-list *list-name* **color** *color*	Color List: List of of one or more TLOC colors. To configure multiple colors in a single list, include multiple **color** options, specifying one *color* in each option. *color* can be one of *3g*, *biz-internet*, *blue*, *bronze*, *custom1* through *custom3*, *default*, *gold*, *green*, *lte*, *metro-ethernet*, *mpls*, *private1* through *private6*, *public-internet*, *red*, and *silver*.

prefix-list *list-name* **ip-prefix** *prefix/length*	IP Prefix List: 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. Specify the IP prefixes as follows: • *prefix/length*—Exactly match a single prefix–length pair. • **0.0.0.0/0**—Match any prefix–length pair. • **0.0.0.0/0 le** *length*—Match any IP prefix whose length is less than or equal to length. For example, **ip-prefix 0.0.0.0/0 le 16** matches all IP prefixes with lengths from /1 through /16. • **0.0.0.0/0 ge** *length*—Match any IP prefix whose length is greater than or equal to *length*. For example, **ip-prefix 0.0.0.0 ge 25** matches all IP prefixes with lengths from /25 through /32. • **0.0.0.0/0 ge** *length1* **le** *length2*, or **0.0.0.0 le** *length2* **ge** *length1*—Match any IP prefix whose length is greater than or equal to *length1* and less than or equal to *length2*. For example, **ip-prefix 0.0.0.0/0 ge 20 le 24** matches all /20, /21, /22, /23, and /24 prefixes. Also, **ip-prefix 0.0.0.0/0 le 24 ge 20** matches the same prefixes. If *length1* and *length2* are the same, a single IP prefix length is matched. For example, **ip-prefix 0.0.0.0/0 ge 24 le 24** matches only /24 prefixes. In centralized control policy, you reference a prefix list in a **match route prefix-list** match condition.
site-list *list-name* **site-id** *site-id*	Site List: List of one or more identifiers of sites in Cisco SD-WAN overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. To configure a range of site IDs, separate the IDs with hyphens. In centralized control policy, you can refer to a site list in **match route site-list** and **match tloc site-list** match conditions, and you apply a centralized control policy (with the **apply-policy** command) by site list.

tloc-list *list-name* **tloc** *address* **color** *color* **encap** *encapsulation* [**preference** *value*]	TLOC List: List of one or more address of transport locations (TLOCs) in Cisco SD-WAN overlay network. For each TLOC, specify its address, color, and encapsulation. *address* is the system IP address. *color* can be one of *3g*, *biz-internet*, *blue*, *bronze*, *custom1*, *custom2*, *custom3*, *default*, *gold*, *green*, *lte*, *metro-ethernet*, *mpls*, *private1* through *private6*, *public-internet*, *red*, and *silver*. encapsulation can be *gre* or *ipsec*. Optionally, set a preference value (from 0 to $2^{32} - 1$) to associate with the TLOC address. When you apply a TLOC list in an *action accept* condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion. To configure multiple TLOCs in a single list, include multiple **tloc** options, specifying one TLOC number in each option. In centralized control policy, you can refer to a TLOC list in **match route tloc-list** and **match tloc tloc-list** match conditions, and in *action accept* conditions.
vpn-list *list-name* **vpn** *vpn-id*	VPN List: List of one or more identifiers of VPNs in Cisco SD-WAN overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. To configure a range of VPN IDs, separate the IDs with hyphens. In centralized control policy, you can refer to a VPN list in **match route vpn-list** match condition and in the *action accept export-to vpn-list* policy action.

For Centralized Data Policy:

app-list *list-name* (**app** *application-name* | **app-family** *application-family*)	Application List: List of one or more applications or application families running on the subnets connected to the vEdge router. 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, specifying one application or application family in each **app** or **app-family** option. The number of app-list entries is limited to 8192. *application-name* is the name of an application family. Cisco SD-WAN software supports about 2300 different applications. To list the supported applications, use the *?* in the CLI. The number of app entries is limited to 8192. *application-family* is the name of an application family. It can be one of the following: *antivirus*, *application-service*, *audio_video*, *authentication*, *behavioral*, *compression*, *database*, *encrypted*, *erp*, *file-server*, *file-transfer*, *forum*, *game*, *instant-messaging*, *mail*, *microsoft-office*, *middleware*, *network-management*, *network-service*, *peer-to-peer*, *printer*, *routing*, *security-service, standard*, *telephony*, *terminal*, *thin-client*, *tunneling*, *wap*, *web*, and *webmail*. The number of app-family entries is limited to 32.

data-prefix-list *list-name* **ip-prefix** *prefix/length*	Data Prefix List: List of one or more IP prefixes. The data prefix list is limited to 8192 entries. To configure multiple prefixes in a single list, include multiple**ip-prefix** options, specifying one prefix in each option. The number of ip-prefix entries is limited to 8192.
site-list *list-name* **site-id** *site-id*	Site List: List of one or more identifiers of sites in Cisco SD-WAN overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. To configure a range of site IDs, separate the IDs with hyphens. In application-aware routing policy, you apply a centralized control policy (with the **apply-policy** command) by site list.
tloc-list *list-name* **tloc** *address* **color** *color* **encap** (**gre** | **ipsec**) [**preference** *value* **weight** *value*]	TLOC List: List of one or more address of transport locations (TLOCs) in the overlay network. For each TLOC, specify its address, color, and encapsulation. *address* is the system IP address. *color* can be one of *3g*, *biz-internet*, *blue*, *bronze*, *custom1*, *custom2*, *custom3*, *default*, *gold*, *green*, *lte*, *metro-ethernet*, *mpls*, *private1* through *private6*, *public-internet*, *red*, and *silver*. encapsulation can be *gre* or *ipsec*. The number of tloc-list entries is limited to 2048. The number of tloc entries is limited to 64. Optionally, set a preference value (from 0 to $2^{32} - 1$) to associate with the TLOC address. When you apply a TLOC list in an *action accept* condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion. To configure multiple TLOCs in a single list, include multiple **tloc** options, specifying one TLOC number in each option. In centralized data policy, you can refer to a TLOC list in **match route tloc-list** and match **tloc tloc-list** match conditions, and in *action accept* conditions.
vpn-list *list-name* **vpn** *vpn-id*	VPN List: List of one or more identifiers of VPNs in Cisco SD-WAN overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. The number of vpn entries is limited to 128. To configure a range of VPN IDs, separate the IDs with hyphens. In centralized data policy, you can refer to a VPN list in a **match vpn-list** match condition in a VPN membership policy. For centralized data policy, you can include any VPNs except for VPN 0 and VPN 512. VPN 0 is reserved for control traffic, so never carries any data traffic, and VPN 512 is reserved for out-of-band network management, so also never carries any data traffic. Note that while the CLI allows you to include these two VPNs in a data policy configuration, the policy is not applied to these two VPNs.

For Localized Control Policy:

as-path *path-list*	AS Paths: List of one or more ASs that make up the AS path. 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, specifying one AS path in each option.
community [*aa:nn*] [**internet**] [**local-as**] [**no-advertise**] [**no-export**]	BGP Communities: List of one of more BGP communities. In **community**, you can specify: • *aa:nn*: Autonomous system number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one **community** in each option.
community [**rt** (*aa:nn* | *ip-address*)] [**soo** (*aa:nn* | *ip-address*)]	BGP Extended Communities: List of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa:nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa:nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple community options, specifying one **community** in each option.

ip-prefix *prefix/length*	IP Prefix: List of one or more IP prefixes and length. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Specify the IP prefixes as follows: • *prefix/length*—Exactly match a single prefix–length pair. • **0.0.0.0/0**—Match any prefix–length pair. • **0.0.0.0/0 le** *length*—Match any IP prefix whose length is less than or equal to length. For example, **ip-prefix 0.0.0.0/0 le 16** matches all IP prefixes with lengths from /1 through /16. • **0.0.0.0/0 ge** *length*—Match any IP prefix whose length is greater than or equal to length. For example, **ip-prefix 0.0.0.0 ge 25** matches all IP prefixes with lengths from /25 through /32. • **0.0.0.0/0 ge** *length1* **le** *length2*, or **0.0.0.0 le** *length2* **ge** l*length1*—Match any IP prefix whose length is greater than or equal to *length1* and less than or equal to **length2**. For example, **ip-prefix 0.0.0.0/0 ge 20 le 24** matches all /20, /21, /22, /23, and /24 prefixes. Also, **ip-prefix 0.0.0.0/0 le 24 ge 20** matches the same prefixes. If length1 and length2 are the same, a single IP prefix length is matched. For example, **ip-prefix 0.0.0.0/0 ge 24 le 24** matches only /24 prefixes.

For Localized Data Policy (ACLs):

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. The number of data-prefix-list entries is limited to 8192. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. The number of ip-prefix entries is limited to 8192. .

Command History

Release	Modification
14.1	Command introduced.
16.3	Add support for overlapping sites in different site lists, and add support for IP multicast addresses.

Release	Modification
26.2.1	For Application-Aware Routing Policy and Centralized Data Policy, the following lists are bounded: • The number of app-list entries limited to 8192. • The number of app name entries limited to 8192. • The number of app-family entries limited to 32. • The number of data-prefix-list entries limited to 8192. • The number of ip-prefix entries limited to 8192. • The number of tloc-list entries limited to 2048. • The number of tloc entries limited to 64.

Example

Configure a list of VPNs:

```
policy
  lists
    vpn-list west-coast
      vpn 20-30
      vpn 42
      vpn 45
```

Configure a list of prefixes:

```
policy
  lists
    prefix-list east
      ip-prefix 8.8.0.0/16
```

Operational Commands

show running-config policy lists

Related Topics

action, on page 34
apply-policy, on page 72
match, on page 316
policy, on page 382
sla-class, on page 455

local-interface-list

Configure Direct Internet Access (DIA) interfaces for Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only).

Note To ensure that Cloud OnRamp for SaaS is set up properly, configure it in vManage NMS, not using the CLI.

Command Hierarchy

```
vpn 0
  cloudexpress
    local-interface-list interfaces-names
```

Syntax Description

interfaces	Interfaces: List of interfaces names. Default: If no local interface is configured, Cloud OnRamp for SaaS uses interfaces configured with NAT.

Command History

Release	Modification
16.3	Command introduced.

Example

Configure Cloud OnRamp for SaaS to run on interfaces *ge0/0* and *ge0/2*:

```
vEdge# show running-config vpn 100 cloudexpress
vpn 100
 cloudexpress
  local-interface-list ge0/0 ge0/2
 !
!
```

Operational Commands

clear cloudexpress computations

show cloudexpress applications

show cloudexpress gateway-exits

show cloudexpress local-exits

show omp cloudexpress

show running-config vpn cloudexpress

location

system location—Configure a text string that describes the location of a Cisco vEdge device.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  location "string"
```

Syntax Description

string	Location description: Text string that describes the location of the device. If the name contains spaces, enclose it in quotation marks. Maximum characters: 128

Command History

Release	Modification
14.1	Command introduced.

Examples

Configuring router location

```
vEdge(config-system)# location "Main lab, row 18, rack 3"
vEdge(config-system)# commit and-quit
Commit complete.
vEdge# show running-config system
system
 host-name          vEdge
 location           "Main lab, row 18, rack 3"
 system-ip          172.16.255.15
 domain-id          1
 site-id            500
 organization-name "Cisco"
 clock timezone America/Los_Angeles
...
```

Operational Commands

show running-config system

Related Topics

gps-location, on page 213
location, on page 295

location

Configure the location of a Cisco vEdge device.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
location string
```

Syntax Description

string	Device Location: Text string that describes the location of the device. If the name contains spaces, enclose it in quotation marks (" "). Maximum characters: 255

Command History

Release	Modification
14.1	Command introduced.

Examples

Example

```
vEdge(config)# snmp location "Machine room 1, Aisle 3, Rack 7"
```

Operational Commands

show running-config snmp

Related Topics

gps-location, on page 213
location, on page 293

log-frequency

Configure how often packet flows are logged (on vEdge routers only). Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing (DPI) flow.

vManage Feature Template

For vEdge routers:

Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Log Frequency field

Command Hierarchy

```
policy
  log-frequency number
```

Syntax Description

number	Logging Frequency: How often packet flows are logged. Range: Any integer value. While you can configure any 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 is logged.

Syntax Description

string	Location description: Text string that describes the location of the device. If the name contains spaces, enclose it in quotation marks. Maximum characters: 128

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure packet flow logging to log every 16 packets. Note that the configured logging frequency value of 20 is rounded down to 16, which is the nearest power of 2. With this configuration, every sixteenth packet is logged.

```
vEdge# show running-config policy log-frequency
policy
 log-frequency 20
!
```

Operational Commands

clear app log flow-all

clear app log flows

show app log flow-count

show app log flows

Related Topics

implicit-acl-logging, on page 238

log-translations

Log the creation and deletion of NAT flows (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface natpoolnumber
    nat
      log-translations
```

Command History

Release	Modification
18.3	Command introduced.

Examples

Example 1

Configure a vEdge router to perform dynamic NAT:

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
  no shutdown
!
```

Example 2

Configure a vEdge router to perform static NAT, translating a service-side and a remote IP address:

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
```

```
    static source-ip 10.1.17.3 translate-ip 10.15.1.4 inside
    static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
    direction inside
    no overload
    log-translations
  !
  no shutdown
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

Related Topics

encapsulation, on page 202
static, on page 462

logging disk

Log event notification system log (syslog) messages to a file on the local device's hard disk. Logging to the disk, at a priority level of "information," is enabled by default. Log files are placed in the directory /var/log on the local device. They are readable by the "admin" user.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► Logging

Command Hierarchy

```
system
  logging
    disk
      enable
      file
        rotate number
        size megabytes
      priority priority
```

Syntax Description

enable	

	Enable and Disable Logging to Disk: Allow syslog messages to be recorded in a file on the local hard disk. By default, logging to a local disk file is enabled. To disable disk logging, use the **no system logging disk enable** configuration command. **Log files:** Syslog messages at or above the default or configured priority value are recorded in a number of files in the directory /var/log. For Releases 15.4 and later, syslog messages are stored in the following files: • auth.log—Login, logout, and superuser access events, and usage of authorization systems. • kern.log—Kernel messages. • messages—Consolidated log file that contains syslog messages from all sources. • vconfd—All configuration-related messages. • vdebug—All debug messages for modules whose debugging is turned on and all syslog messages above the configured priority value are saved to the file /var/log/vdebug and, in Releases 16.3 and later, in /var/log/tmplog/vdebug. Debug logging supports various levels of logging based on the module. Different modules implement the logging levels differently. For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. To enable debugging, use the debug operational command. • vsyslog—All syslog messages above the configured priority value are stored in the file /var/log/vsyslog. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved. For Releases 15.3 and earlier, syslog messages are stored in the following files: • auth.log—Login, logout, and superuser access events, and usage of authorization systems. • confd/audit.log—Captured by the audit daemon. These messages generally pertain to systemwide operations, users, files, and directories. • confd/confd.log—Configuration messages. • confd/devel.log—Development message. • confd/netconf.log—Netconf messages. • confd/snmp.log—SNMP messages. • daemon.log—System and application process messages. • devel.log—Developer messages. • kern.log—Kernel messages.

	• messages—Common log messages. • quagga/daemon.log—One log file for each routing process running on the device. Examples are bgpd.log and ospfd.log • quagga/quagga-debug.log—Routing process debug syslog messages. • tallylog—Attempted and failed login operations. • user.log—All user-level logs. • vdebug—All debug messages for modules whose debugging is turned on and all syslog messages above the configured priority value are saved to the file /var/log/vdebug. Debug logging supports various levels of logging based on the module. Different modules implement the logging levels differently. For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. To enable debugging, use the debug operational command. • vsyslog—All syslog messages above the configured priority value are stored in the file /var/log/vsyslog. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved. • wtmp—Login records. SD-WAN software does not use the following standard LINUX files, which are present in /var/log, for logging: cron.log, debug, lpr.log, mail.log, and syslog. The files in the directory xml/ are not used for message logging.
priority *priority*	Message priority: Severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. The default priority value is "informational", so, by default, all syslog messages are recorded. The priority level can be one of the following (in order of decreasing severity): • Emergency—System is unusable (corresponds to syslog severity 0). • Alert— Action must be taken immediately (corresponds to syslog severity 1). • Critical—A serious condition (corresponds to syslog severity 2). • Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • Warning—A minor error condition (corresponds to syslog severity 4). • Notice—A normal, but significant condition (corresponds to syslog severity 5). • Informational—Routine condition (the default) (corresponds to syslog severity 6).

rotate *number* **size** *megabytes*	Log File Rotation: Syslog files are rotated on an hourly basis based on the file's size. When the file size exceeds the configured value, the file is rotated, and the syslogd process isnotified. The default file size is 10 MB. You can configure this to be from 1 to 20 MB. Syslog files are discarded after a certain number of files have been created. The default is 10. You can configure this to be from 1 to 10. Debug files are also rotated and discarded following a similar scheme. However, you cannot configure the file size (10MB), nor can you configure the number of rotations (10).

Command History

Release	Modification
14.1	Command introduced.
15.4	Files used to store syslog files changed.
16.3	Debug output is placed in the /var/log/tmplog/vdebug file, not the /var/log/vdebug file.

Usage Guidelines

show logging—Display the system logging parameters that are in effect on the vEdge router:

file list /var/log—List the files in the /var/log directory.

file show /var/log/vsyslog—Display the contents of the vsyslog syslog file. Here is sample output for Releases 15.3 and earlier:

```
vSmart# file show /var/log/vsyslog
Aug  5 17:00:04 vsmart vdaemon[937]: viptela_system_personality created/modified
Aug  5 17:00:04 vsmart vdaemon[937]: viptela_config_security:549 Rekey generation interval
 3600 (Seconds)
Aug  5 17:00:04 vsmart SYSMGR[948]: %viptela-SYSMGR-6-200007: Confd Phase 2 UP
Aug  5 17:00:04 vsmart vdaemon[937]: Message Connection UP
```

For Releases 15.3 and earlier, each syslog message generated by SD-WAN has this format:

```
% date - source - module - level - MessageID: text-of-syslog-message
```

In the third line of the /var/log/vsyslog output shown above, the message source is a vSmart controller, the module is SYSMGR (the system manager), the level is 6 (informational), the message ID is 200007, and the message itself is "Confd Phase 2 UP".

In Releases 15.4 and later, each syslog message has the following format:

```
facility.source& date - source - module - MessageID: text-of-syslog-message
```

Here is an example of a syslog message (in the file, this message would be on a single line):

```
local7.info: Dec 29 16:50:56 vedge DHCP_CLIENT[324]:
%Viptela-vedge-DHCP_CLIENT-6-INFO-1300010:
Renewed address 10.0.99.14/24 for interface mgmt0
```

Examples

Change the syslog file size to 3 MB, save only three syslog files, and set the syslog priority to log only alert, and emergency conditions:

```
vEdge(config-system)# logging disk
vEdge(config-disk)# file size 3
vEdge(config-disk)# file rotate 3
vEdge(config-disk)# priority alert
vEdge(config-disk)# show configuration
system
 logging
  disk
   file size 3
   file rotate 3
   priority alert
  !
 !
!
```

Related Topics

logging server, on page 305
show crash, on page 803
show logging, on page 891

logging host

To log system messages 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 {**hostname** *ipv4-address* | *ipv4-address* | **ipv6** *ipv6-address*} [**vrf** *vrf-name*] [**transport** [**tcp** [**port** *port-no*] | **tls** [**port** *port-no* | **profile** *profile-name*] | **udp** [**port** *port-no*]]}

no logging host {**hostname** *ipv4-address* | *ipv4-address* | **ipv6** *ipv6-address*}

Table 6: Syntax Description

ipv4-address	Specifies the IP address of the host that receives the system logging (syslog) messages.
hostname	Name of the IPv4 or IPv6 host that receives the syslog messages.
vrf *vrf-name*	(Optional) Specifies a VPN routing and forwarding instance (VRF) that connects to the syslog server host. Name of the VRF that connects to the syslog server host.
ipv6	Indicates that you use an IPv6 address for a host that receives the syslog messages.
ipv6-address	IPv6 address of the host that receives the syslog messages.
transport	(Optional) Method of transport of syslog messages, which is TLS, TCP, or UDP.
tls	(Optional) Specifies that TLS transport will be used to log messages.

tcp	(Optional) Specifies that TCP transport will be used to log messages.
udp	(Optional) Specifies that UDP transport will be used to log messages.
port *port-no*	(Optional) Integer that defines port. Range: 1-65535. If you do not specify a port number, the standard Cisco default port number is used. TLS: 6514 . TCP: 601 UDP: 514
profile *profile-name*	(Optional) Name of the TLS profile.

Command Default

You cannot send system logging messages to any remote host.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced on the Cisco IOS XE Catalyst SD-WAN device.

Usage Guidelines

Standard system logging is enabled by default. If logging is disabled on your system (using the **no logging on** command), ensure that you enter the **logging on** command to reenable logging before you can use the **logging host** command.

The **logging host** command identifies a remote host (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of hosts that receive logging messages.

To specify the severity level for logging to all hosts or enforce the logging format as per RFC5424, use the **logging trap** command.

When the **no logging host** command is issued with or without the optional keywords, all logging to the specified host is disabled.

Examples

In the following example, **logging trap** command with logging format based on RFC5424 is logged to a host at 10.104.52.44:

```
Router(config)# logging trap syslog-format rfc5424
Router(config)# logging host 10.104.52.44 transport tls
```

In the following example, you can log messages to a host with an IP address of 172.16.150.63 connected through a **vpn1** VRF:

```
Router(config)# logging host 172.16.150.63 vrf vpn1
```

Related Commands

Command	Description
show crypto pki trustpoints status	Displays the truspoint that is configured in the Cisco IOS XE Catalyst SD-WAN device.
logging tls-profile *profile-name* [**ciphersuite** *ciphersuite*]	Logs system messages to syslog server through TLS profile.

logging tls-profile

To configure the TLS profile of a Cisco IOS XE Catalyst SD-WAN device, use the **logging tls-profile** command in global configuration mode. To remove a specified logging tls profile from the configuration, use the **no** form of this command.

logging tls-profile *profile-name* [**ciphersuite** *ciphersuite*]

no logging tls-profile

Table 7: Syntax Description

tls-profile *profile-name*	Indicates that you use TLS profile for Cisco IOS XE Catalyst SD-WAN device. String. Maximum: 32 characters.
ciphersuite *ciphersuite*	(Optional) Specifies the cipher suites that you can use for a connection with syslog server.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced on the Cisco IOS XE Catalyst SD-WAN device.

Example

In the following example, you can configure the TLS profile for profile1:

through a vpn1 VRF

```
Router(config)# logging tls-profile profile1
```

logging server

Log event notification syslog messages to a remote host. By default, syslog messages are also always logged to the local hard disk. To disable local logging, use the **no system logging disk enable** command.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► Logging

Command Hierarchy

```
system
  logging
    server (dns-name | hostname | ip-address)
      priority priority
      source-interface interface-name
      vpn vpn-id
```

Syntax Description

source-interface *interface-name*	Interface for System Log Messages to Use: Configure outgoing system log messages to use a specific interface. The interface name can be a physical interface or a subinterface (a VLAN-tagged interface). The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.
priority *priority*	Message priority: Severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. *priority* can be one of the following: • emergency—System is unusable (corresponds to syslog severity 0). • alert— Action must be taken immediately (corresponds to syslog severity 1). • critical—A serious condition (corresponds to syslog severity 2). • error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • warn—A minor error condition (corresponds to syslog severity 4). • notice—A normal, but significant condition (corresponds to syslog severity 5). • information—Routine condition (the default) (corresponds to syslog severity 6).
name (*dns-name* | *host-name* | *ip-address*)	Server name: DNS name, hostname, or IP address of the system on which to store syslog messages. You can configure multiple syslog servers.

vpn *vpn-id*	VPN: VPN in which the syslog server is located or through which the syslog server can be reached. Range: 0 through 65530 Default: VPN 0

Command History

Release	Modification
14.1	Command introduced.
15.2.7	Support for multiple syslog servers added.
15.4	**source-interface** command added.

Usage Guidelines

show logging —Display the system logging parameters that are in effect.

In Releases 15.3 and earlier, each syslog message generated by Cisco SD-WAN has this format:

```
%Viptela - module - level - MessageID: text-of-syslog-message
```

In Releases 15.4 and later, each syslog message has the following format:

```
facility.source date - source - module - MessageID: text-of-syslog-message
```

Examples

Configure two syslog servers, one that receives all emergency (severity 0) messages and a second that receives all messages at severity 4 (warn) and lower:

```
vEdge(config-logging)# show full-configuration
system
 logging
  disk
   enable
  !
  server log.cisco.com
   vpn      1
   priority emergency
  exit
  server log2.cisco.com
   vpn      1
   priority warn
  exit
 !
!
```

Related Topics

logging disk, on page 298

logs

Configure the logging of AAA and Netconf system logging (syslog) messages. By default, these messages are logged and placed in the auth.info and messages log files.

Each time a vManage NMS logs in to a vEdge router to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. These message can fill the log files. You might want to disable the logging of these messages to reduce the number of messages in these two log files.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
    logs
      [no] audit-disable
      [no] netconf-disable
```

Syntax Description

audit-disable	Disable the logging of AAA events. Default: These events are logged.
netconf-disable	Disable the logging of Netconf events. Default: These events are logged.

Command History

Release	Modification
17.1	Command introduced.

Example

Disable the logging of AAA and Netconf events:

```
vEdge# show running-config system aaa
system
 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.
  !
  logs
    audit-disable
    netconf-disable
 !
!
```

Operational Commands

show users

low-bandwidth-link

Characterize the tunnel interface as a low-bandwidth link. This configuration command is relevant only for a router which 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.

vManage Feature Template

Configuration ► Templates ► VPN Interface Cellular

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      [no] low-bandwidth-link
```

Command History

Release	Modification
16.3	Command introduced.
Cisco IOS XE Release 17.2	Added support for Cisco IOS XE Catalyst SD-WAN devices.

Examples

Configure a tunnel interface for an LTE interface to be a low-bandwidth link:

```
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
   color lte
   low-bandwidth-interface
  !
  no shutdown
 !
```

Operational Commands

show control local-properties | display xml | include low

mac-accounting

Generate accounting information for IP traffic (on vEdge routers only).

Command Hierarchy

```
vpn vpn-id
  interface ge number/subinterface
    mac-accounting (egress | ingress)
```

Syntax Description

(**egress** | **ingress**)	Generate Accounting Information: • egress: Generate accounting information based on the destination (egress) MAC addresses. • ingress: Generate accounting information based on the source (ingress) MAC addresses.
no mac-accounting	Disable MAC accounting.

Command History

Release	Modification
14.1	Command introduced.

Examples

Generate accounting information about the IP traffic on this interface based on the source MAC addresses of the packets:

```
vpn 0
  interface ge0/0
    mac-accounting ingress
```

Operational Commands

show running-config vpn interface

mac-address

Configure a MAC address to associate with the interface in the VPN.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    mac-address mac-address
```

Syntax Description

mac-address	MAC address. Separate the bytes in the address with colons. Note that you cannot change the default MAC address (00:00:00:00:00:00) of a loopback interface.

Command History

Release	Modification
14.1	Command introduced.

Example

Configure a MAC address on an interface:

```
vEdge(config-interface-ge0/4)# mac-address b8:e8:56:38:5e:89
```

Operational Commands

show interface vpn

mac-authentication-bypass

Enable authentication for non-802.1X–compliant clients (on vEdge routers only). These clients are authenticated based on their MAC address.

A non-802.1X–compliant client is one that does not respond to EAP identity requests from the vEdge router.

After the 802.1X interface detects a client, it waits to receive an Ethernet packet from the client. Then the router sends a RADIUS access/request frame to the authentication server that includes a username and password based on the MAC address. If authorization succeeds, the router grants the client access to the WAN or WLAN. If authorization fails, the router assigns the interface to the guest VLAN if one is configured.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      mac-authentication-bypass
        allow mac-addresses
        server
```

Syntax Description

mac-authentication-bypass	Enable Authentication for Non-802.1X–Compliant Hosts: Turn on authentication for non-802.1X–compliant clients.
allow *mac-address*	Enable Authentication for Specific Devices: Turn on authentication for one or more devices based on their MAC address, as listed in *mac-addresses*, before performing an authentication check with the RADIUS server. You can configure up to eight MAC addresses for MAC authentication bypass.
server	Enable Authentication via a RADIUS Server: Authenticate non-802.1X–compliant clients using a RADIUS server. This option enables MAC authentication bypass on the RADIUS server.

Command History

Release	Modification
16.3	Command introduced.

Examples

Enable MAC authentication bypass:

```
vpn 0
  interface ge0/0
    dot1x
      mac-authentication-bypass
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

radius, on page 407

match

To configure matching criteria for the custom-eflow sequence to be considered as elephant-flow, use the **match** command in sequence configuration mode. To disable the matching criteria, use the **no** form of the command.

match [**client-ip** *IPv4-prefix/ (IP/Length)*] [**server-ip** *IPv4-prefix/ (IP/Length)*] [**protocol** { **TCP** | **UDP** }]
no match [**client-ip** *IPv4-prefix/ (IP/Length)*] [**server-ip** *IPv4-prefix/ (IP/Length)*] [**protocol** { **TCP** | **UDP** }]

Syntax Description

client-ip *IPv4-prefix/ (IP/Length)*	IP address of the required client subnet. Specify the IPv4-prefix (IP/Length) address.
server-ip *IPv4-prefix/ (IP/Length)*	IP address of the required server subnet. Specify the IPv4-prefix (IP/Length) address.
Protocol	Transport protocol type can be UDP or TCP.

Command Default

By default, protocol, client-ip, or server-ip matching criteria are not configured for the custom-eflow sequence.

Command Modes

Sequence number configuration (config-sequence-num)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

Examples

The following example shows how to configure matching criteria using the **match** command:

```
vEdge2k(config-sequence-num)# match
vEdge2k(config-match)# protocol TCP
vEdge2k(config-match)# client-ip 10.2.3.0/24
vEdge2k(config-match)# server-ip 10.2.4.0/24
```

match

Define the properties that must be matched so that an IPv6 policy action can take effect (on vEdge routers only).

Command Hierarchy

For Localized Data Policy for IPv6

Configure on vEdge routers only.

```
policy ipv6
  access-list acl-name
    sequence number
      match
        class class-name
        destination-port number
        next-header protocol
        packet-length number
        plp (high | low)
        source-port number
        tcp flag
        traffic-class value
```

Syntax Description

For Localized Data Policy for IPv6

class *class-name*	Classification Match the specified class name. The name can be from 1 through 32 characters.
destination-port *number*	Destination Port: Match a destination port number. *number* can be 0 though 65535. Specify a single number, a list of numbers (with numbers separated by a space), or a range of numbers (with the two numbers separated with a hyphen [-]). The number of destination-port entries is limited to 31.
next-header *protocol*	Next Protocol: Match the next TCP or IP protocol in the IPv6 header. *protocol* is the number of an IPv6 protocol, and can be a value from 0 through 255. The number of next-header entries is limited to 32.

packet-length *number*	Packet Length: Match packets of the specified length. The packet length is a combination of the lengths of the IPv6 header and the packet payload. *number* can be 0 though 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]) The number of packet-length entries is limited to 32.
plp (**high** | **low**)	Packet Loss Priority: Match a packet's loss priority (PLP). By default, packets have a PLP value of **low**. To set a packet's PLP value to **high**, apply a policer that includes the **exceed remark** option.
`source-port` *number*	Source Port: Match a source port. *number* can be 0 through 65535. Specify a single number, a list of numbers (with numbers separated by a space), or a range of numbers (with the two numbers separated with a hyphen [-]). The number of source-port entries is limited to 31.
tcp *flag*	TCP Flag Match TCP flags. *flag* can be **syn**.
traffic-class *number*	Traffic Class: Match the specified traffic class value. *number* can be from 0 through 63.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added support for IPv6 ACLs.
26.2.1	Added entry number limits for destination-port, next-header, packet-length and source-port.

Examples

Configure an IPv6 ACL that changes the traffic class on TCP port 80 data traffic, and apply the ACL to an interface in VPN 0:

```
vEdge# show running-config policy ipv6 access-list
policy
 ipv6 access-list traffic-class-48-to-46
 sequence 10
  match
   destination-port 80
   traffic-class    48
  !
  action accept
   count port_80
```

```
   log
   set
    traffic-class 46
   !
  !
 !
 default-action accept
 !
!
vEdge# show running-config vpn 0 interface ge0/7 ipv6
vpn 0
 interface ge0/7
  ipv6 access-list traffic-class-48-to-46 in
 !
!
```

Operational Commands

show running-config policy

Related Topics

match, on page 316

match

Define the properties that must be matched so that an IPv4 policy action can take effect (on vEdge routers and vSmart controllers only).

policy app-route-policy vpn-list sequence match

policy access-list sequence match

policy control-policy sequence match

policy data-policy vpn-list sequence match

policy route-policy sequence match

policy zone-based-policy sequence match

vManage Feature Template

For vEdge routers and vSmart controllers:

Configuration ► Policies

Configuration ► Security (for zone-based firewall policy)

Command Hierarchy

For Application-Aware Routing Policy

Configure on vSmart controllers only.

```
policy
  app-route-policy policy-name
    vpn-list list-name
      sequence number
        match
          app-list list-name
```

```
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dns-app-list list-name
        dns (request | response)
        dscp number
        icmp-msg value
        icmp6-msg value
        plp (high | low)
        protocol number
        source-data-prefix-list list-name
        source-ip prefix/length
        source-port number
        traffic-to {access | core | service}
```

For Centralized Control Policy

Configure on vSmart controllers only.

```
policy
  control-policy policy-name
    sequence number
      match
        route
          color color
          color-list list-name
          omp-tag number
          origin protocol
          originator ip-address
          path-type {hierarchical-path | direct-path | transport-gateway-path}
          preference number
          prefix-list list-name
          region {region | region-list} [role {border-router | edge-router}]
          site-id site-id
          site-list list-name
          tloc address color color [encap encapsulation]
          tloc-list list-name
          vpn vpn-id
          vpn-list list-name
        tloc
          carrier carrier-name
          color color
          color-list list-name
          domain-id domain-id
          group-id group-id
          omp-tag number
          originator ip-address
          preference number
          site-id site-id
          site-list list-name
          tloc address color color [encap encapsulation]
          tloc-list list-name
```

For Centralized Data Policy

Configure on vSmart controllers only.

```
policy
  data-policy policy-name
    vpn-list vpn-list
      sequence number
        match
          app-list list-name
          destination-data-prefix-list list-name
          destination-ip prefix/length
          destination-port number
```

```
          dns-app-list list-name
          dns (request | response)
          dscp number
          icmp-msg value
          icmp6-msg value
          packet-length number
          plp (high | low)
          protocol number
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port number
          tcp flag
          traffic-to {access | core | service}
  vpn-membership policy-name
    sequence number
      match
        vpn vpn-id
        vpn-list list-name
```

For Localized Control Policy

Configure on vEdge routers only.

```
policy
  route-policy policy-name
    sequence number
      match
        address list-name
        as-path list-name
        community list-name
        ext-community list-name
        local-preference number
        metric number
        next-hop list-name
        omp-tag number
        origin (egp | igp | incomplete)
        ospf-tag number
        peer address
```

For Localized Data Policy

Configure on vEdge routers only.

```
policy
  access-list acl-name
    sequence number
      match
        class class-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dscp number
        icmp-msg value
        icmp6-msg value
        packet-length number
        plp (high | low)
        protocol number
        source-data-prefix-list list-name
        source-ip prefix/length
        source-port number
        tcp flag
```

For Zone-Based Firewalls

Configure on vEdge routers only.

```
policy
  zone-based-policy policy-name
    sequence number
      match
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        protocol number
        source-data-prefix-list list-name
        source-ip prefix-length
        source-port number
```

Syntax Description

For Application-Aware Routing Policy

app-id *app-id-name*	Application Identifier: Match the name of an application defined with a **policy app-id** command.
destination-data-prefix-list *list-name* **destination-ip** *prefix*/*length*	Destination Prefix: Match a destination prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of destination-ip entries is limited to 8192.
destination-port *number*	Destination Port: Match a destination port. You can 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 [-]). The number of destination-port entries is limited to 31.
dscp *number*	DSCP: Match the specified DSCP value. The number of dscp entries is limited to 32.
plp (**high** | **low**)	Packet Loss Priority: Match a packet's loss priority (PLP). By default, packets have a PLP value of **low**. To set a packet's PLP value to **high**, apply a policer that includes the **exceed remark** option.
protocol *number*	Protocol: Match the TCP or IP protocol number. The number of protocol entries is limited to 32.
source-data-prefix-list *list-name* **source-ip** *prefix*/*length*	Source Prefix : Match a source prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of source-ip entries is limited to 8192.

source-port *number*	Source Port: Match a source port. You can 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 [-]). The number of source-port entries is limited to 31.
dns-app-list *list-name* **dns** (**request** | **response**)	Split DNS: Resolve DNS requests and process DNS responses on an application-by-application basis when the vEdge router is configured as an internet exit point. To match specific applications or application families, specify the name of a list you created with the **lists app-list** command. To process DNS requests for the applications (for outbound DNS queries), specify the **dns request** match condition.To process DNS responses from DNS servers, specify the **dns response** match condition.
traffic-to {**access** | **core** | **service**}	In a Hierarchical SD-WAN architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN.

For Centralized Control Policy

color *color* **color-list** *list-name*	Color: Match an individual color or a group of colors defined with a **policy lists color-list** list.
domain-id *number*	Domain: Match the domain identifier. Currently, the domain identifier can only be 1.
omp-tag *number*	OMP Tag: Match an OMP tag value in the route. number can be a value from 0 through 4294967295.
originator *ip-address*	Originating Address: Match the IP address of the device from which the route was learned.
origin *protocol*	Originating Protocol: Match the protocol from which the route was learned. *protocol*: One of: bgp-external, bgp-internal, connected, ospf-external1, ospf-external2, ospf-inter-area, ospf-intra-area, static

path-type {*hierarchical-path* | *direct-path* | *transport-gateway-path*}	In a Hierarchical SD-WAN architecture, match a route by its path type, which can be one of the following: • *hierarchical-path*: A route that includes hops from an access region to a border router, through region 0, to another border router, then to an edge router in a different access region. • *direct-path*: A direct path route from one edge router to another edge router. • *transport-gateway-path*: A route that is re-originated by a router that has transport gateway functionality enabled.
preference *number*	Preference: Match the preference value in the route.
prefix-list *list-name*	Prefix: Match one or more IP prefixes in a list defined with a **policy lists prefix-list** list.
region {*region-id* | *region-list*} [**role** {**border-router** | **edge-router**}]	In a Hierarchical SD-WAN architecture, match routes that are originated by device(s) in specific regions, and optionally devices with a specific role (edge router or border router).
site-id *site-id* **site-list** *list-name*	Site: Match an individual Cisco SD-WAN overlay network site identifier number or a group of site identifiers defined with a **policy lists site-list** list.
tloc-list *list-name*	TLOC from a List of TLOCs: Match one of the TLOCs in the list defined with a **policy lists tloc-list** list.
tloc *address* **color** *color* [**encap** *encpasulation*] **tloc-list** *list-name*	TLOC Identified by IP Address and Color: Match an individual 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. Default: Encapsulation is ipsec. It can also be gre.
vpn *vpn-id* **vpn-list** *list-name*	VPN: Match an individual VPN identifier or the VPN identifiers in a list defined with a **policy lists vpn-list** command.

For Centralized Data Policy

destination-data-prefix-list *list-name* **destination-ip** *prefix*/*length*	Destination Prefix: Match a destination prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of destination-ip entries is limited to 8192.
destination-port *number*	Destination Port: Match a destination port. You can 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 [-]). The number of destination-port entries is limited to 31.
dscp *number*	DSCP: Match the specified DSCP value. The number of dscp entries is limited to 32.
packet-length *number*	Packet Length Match packets of the specified length. number can be 0 though 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]) The number of packet-length entries is limited to 32.
plp (**high** | **low**)	Packet Loss Priority: Match a packet's loss priority (PLP). By default, packets have a PLP value of **low**. To set a packet's PLP value to **high**, apply a policer that includes the **exceed remark** option.
protocol *number*	Protocol: Match the TCP or IP protocol number. The number of protocol entries is limited to 32.
source-data-prefix-list *list-name* **source-ip** *prefix*/*length*	Source Prefix: Match a source prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of source-ip entries is limited to 8192.
source-port *number*	Source Port: Match a source port. You can 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 [-]). The number of source-port entries is limited to 31.

dns-app-list *list-name* **dns** (**request** | **response**)	Split DNS: Resolve DNS requests and process DNS responses on an application-by-application basis when the vEdge router is configured as an internet exit point. To match specific applications or application families, specify the name of a list you created with the **lists app-list** command. To process DNS requests for the applications (for outbound DNS queries), specify the **dns request** match condition.To process DNS responses from DNS servers, specify the **dns response** match condition.
tcp *flag*	TCP Flag: Match TCP flags. flag can be syn.
traffic-to {**access** | **core** | **service**}	In a Hierarchical SD-WAN architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN.

For Localized Control Policy

as-path *list-name*	BGP AS Path: AS path or paths in the route. list-name is the name of an AS path list defined with a **policy lists as-path-list** command.
community *list-name*	BGP Community: 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.
ext-community *list-name*	BGP Extended Community: BGP extended community or communities in the route. list-name is the name of a BGP extended community list defined with a **policy lists ext-community-list** command.
bgp *origin*	BGP Origin Code: BGP origin code. origin can be egp, igp, or complete. Default: egp
local-preference *number*	Local Preference: BGP local preference value. number can be a value from 0 through 4294967295.
next-hop *list-name*	Next Hop: Next hop in the route. list-name is the name of an IP prefix list defined with a **policy lists prefix-list** command.
omp-tag *number*	OMP Tag: OMP tag number for use by BGP or OSPF. number can be a value from 0 through 4294967295.

ospf-tag *number*	OSPF Tag: OSPF tag value. number can be a value from 0 through 4294967295.
peer *ip-address*	Peer Address: IP address of the peer.
address *list-name*	Prefix from which Route Was Learned: IP prefix or prefixes from which the route was learned. list-name is the name of an IP prefix list defined with a **policy lists prefix-list** command.
metric *number*	Route Metric: Metric in the route. number can be a value from 0 through 4294967295.

For Localized Data Policy

class *class-name*	Classification: Match the specified class name.
destination-data-prefix-list *list-name* **destination-ip** *prefix*/*length*	Destination Prefix: Match a destination prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of destination-ip entries is limited to 8192.
destination-port *number*	Destination Port: Match a destination port. You can 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 [-]). The number of destination-port entries is limited to 31.
dscp *number*	DSCP: Match the specified DSCP value. The number of dscp entries is limited to 32.
packet-length *number*	Packet Length Match packets of the specified length. The packet length is a combination of the lengths of the IPv4 header and the packet payload. number can be 0 though 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]). The number of packet-length entries is limited to 32.

plp (**high** | **low**)	Packet Loss Priority: Match a packet's loss priority (PLP). By default, packets have a PLP value of **low**. To set a packet's PLP value to **high**, apply a policer that includes the **exceed remark** option.
protocol *number*	Protocol: Match the TCP or IP protocol number. The number of protocol entries is limited to 32.
source-data-prefix-list *list-name* **source-ip** *prefix*/*length*	Source Prefix: Match a source prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command. The number of source-ip entries is limited to 8192.
source-port *number*	Source Port: Match a source port. You can 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 [-]). The number of source-port entries is limited to 31.
tcp *flag*	TCP Flag: Match TCP flags. flag can be syn.

For Zone-Based Firewall Policy

destination-data-prefix-list *list-name* **destination-ip** *prefix*/*length*	Destination Prefix: Match a destination prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command.
destination-port *number*	Destination Port: Match a destination port. You can 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 [-]).
protocol *number*	Protocol: Match the TCP or IP protocol number.
source-data-prefix-list *list-name* **source-ip** *prefix*/*length*	Source Prefix: Match a source prefix. You can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a **policy lists prefix-list** command.

source-port *number*	Source Port: Match a source port. You can 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 [-]).

Command History

Release	Modification
14.1	Command introduced.
15.4	Added omp-tag match condition for localized control policy, and rename tag to omp-tag.
16.1	Added packet-length match condition for centralization and localized data policy.
16.3	Added plp match condition for application-aware routing policy, centralized data policy, and localized data policy.
17.1	Added ospf-tag match condition for localized control policy.
18.2	Added zone-based firewall policy.
Cisco IOS XE Release 17.4.1 Cisco SD-WAN Release 20.4.1	Added support to display ICMP messages when a protocol value is 1 or 58 for a match condition.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco SD-WAN Release 20.8.1	Added path-type, region, role, and traffic-to match conditions.
26.2.1	Added entry limits for destination-ip, destination-port, dscp, packet-length, protocol, source-ip, and source-port in some policies.

Examples

Create an access list match condition that matches a destination IP address in a data packet:

```
vEdge(config-match)# show config
policy
access-list test-access-list
  sequence 10
   match
    destination-ip 172.16.0.0/16
   !
  !
 !
!
```

Configure a route policy that matches a list of VPNs:

```
vSmart(config-match-route)# show config
policy
lists
  vpn-list my-vpn-list
   vpn 1
  !
!
control-policy my-control-policy
  sequence 10
   match route
    vpn-list my-vpn-list
   !
  !
 !
!
```

Match a destination prefix in VPN 1:

```
vSmart(config-policy)# show config
policy
 data-policy my-data-policy
  vpn-list my-vpn-list
   sequence 10
    match
     destination-ip 55.0.1.0/24
    !
    action drop
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list my-vpn-list
   vpn 1
  !
 !
!
```

Create a route policy match condition that matches the prefix from which a route was learned:

```
vEdge(config-match)# show config
policy
 lists
  prefix-list my-prefix-list
   ip-prefix 10.0.100.0/24
   ip-prefix 55.0.1.0/24
   ip-prefix 57.0.1.0/24
  !
 !
 route-policy my-route-policy
  sequence 10
   match
    address my-prefix-list
   !
  !
 !
!
```

Display ICMP messages when protocol value is 1 or 58 for a match condition:

```
vEdge(config-match)# show configpolicy
access-list acl_1
sequence 100
match
protocol 1
icmp-msg administratively-prohibited
!
action accept
count administratively-prohibited
!
!
```

Operational Commands

show running-config policy

Related Topics

action, on page 34
apply-policy, on page 72
lists, on page 283
match, on page 314
policy, on page 382

max-clients

Configure the maximum number of clients allowed to connect to the WLAN (on vEdge routers only).

Command Hierarchy

```
wlan radio-band
  interface vapnumber
    max-clients number
```

Syntax Description

number	Maximum Number of WLAN Clients: Maximum number of clients allowed to connect to the WLAN. It is recommended that you do not configure more than 50 clients across all the VAPs. Range: 1 through 50 Default: 25

Command History

Release	Modification
16.3	Command introduced.

Examples

Allow 30 clients to connect to the corporate network and 10 to the guest network :

```
vEdge# show running-config wlan
wlan 5GHz
 country "United States"
 interface vap0
  ssid             CorporateNetwork
  data-security    wpa/wpa2-enterprise
  radius-server radius_server1
  max-clients      30
  no shutdown
 !
 interface vap1
  ssid             GuestNetwork
  data-security    wpa/wpa2-personal
  wpa-personal-key GuestPassword
  max-clients      10
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

max-control-connections

Configure the maximum number of Cisco Catalyst SD-WAN Controllers that the vEdge router is allowed to connect to (on vEdge routers only). When **max-control-connections** is configured (without affinity), vEdge routers establish control connection with Cisco Catalyst SD-WAN Controllers having higher System-IP.

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).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      max-control-connections number
```

Syntax Description

number	Maximum Number of Controllers Set 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: Maximum number of OMP sessions configured with the **system max-omp-sessions** command.

Command History

Release	Modification
15.4	Command introduced. This command replaces the **max-controllers** command.
16.1	Maximum number of controllers changed from 8 to 100, and default value changed from 2 to maximum number of configured OMP sessions.

Examples

Change the maximum number of vSmart controller connections to 4:

```
system
  max-control-connections 4
```

Operational Commands

show control affinity config

show control affinity status

show control connections

show control local-properties

Related Topics

controller-group-id, on page 150
controller-group-list, on page 151
exclude-controller-group-list, on page 207
max-omp-sessions, on page 334

max-controllers

Configure the maximum number of vSmart controllers that the vEdge router is allowed to connect to (on vEdge routers only).

Starting in Release 15.4, this command is deprecated. Use the **max-control-connections** command instead.

Command Hierarchy

```
system
  max-controllers number
```

Syntax Description

number	Maximum Number of Controllers Set the maximum number of vSmart controllers that the vEdge router can connect to. These connections are DTLS or TLS control plane tunnels. Range: 1 through 8 Default: 2

Command History

Release	Modification
14.3	Command introduced.
15.4	This command is deprecated. Use the **max-control-connections** command instead.

Examples

Change the maximum number of vSmart controller connections to 4:

```
system
  maximum-controllers 4
```

Operational Commands

show control connections

max-leases

Configure the maximum number of dynamic IP addresses that the DHCP server can offer (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      max-leases number
```

Syntax Description

number	Number of Leases: Number of IP addresses that can be assigned on this interface. Range: 0 through 4294967295

Command History

Release	Modification
14.3	Command introduced.

Examples

Change the maximum number of leases to 500:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server max-leases 500
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   max-leases   500
  !
 !
!
```

Operational Commands

show dhcp interfaces

show dhcp server

max-macs

Set the maximum number of MAC addresses that a bridging domain can learn (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Bridge

Command Hierarchy

```
bridge bridge-id
  max-macs number
```

Syntax Description

number	MAC Addresses: Maximum number of MAC addresses that the bridging domain can learn. Range: 0 through 4096 Default: 1024

Command History

Release	Modification
15.3	Command introduced.

Examples

Set the maximum number of MAC addresses that the bridging domain can learn to 512:

```
vEdge(config)# bridge 1
vEdge(config-bridge-1)# max-macs 512
```

Operational Commands

show bridge interface

show bridge mac

show bridge table

max-metric

Configure OSPF to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      max-metric
        router-lsa (administrative | on-startup seconds)
```

Syntax Description

router-lsa administrative	Advertise Administratively: Force the maximum metric to take effect immediately, through operator intervention.
router-lsa on-startup *seconds*	Advertise the Maximum metric When the Router Starts Up: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 0, 5 through 86400 seconds Default: 0 seconds (the maximum metric is advertised immediately when the router starts up)

Command History

Release	Modification
14.1	Command introduced.

Examples

Have the maximum metric take effect immediately:

```
vEdge(config-ospf)# max-metric router-lsa administrative
vEdge(config-ospf)# show configuration
vpn 1
 router
  ospf
   max-metric router-lsa administrative
  !
 !
!
```

Operational Commands

show ospf routes

max-omp-sessions

Configure the maximum number of OMP sessions that a vEdge router can establish to vSmart controllers (on vEdge routers only). A vEdge router establishes a single OMP session to each vSmart controller. Even when a vEdge router has multiple tunnel connections to the same vSmart 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), vEdge routers establish OMP peering with vSmarts controllers having higher System-IP.

In an overlay network with redundant vSmart controllers, configure the maximum number of OMP sessions to manage the scale of the overly network, by limiting the number of vSmart controllers that an individual vEdge router can establish control connections with.

This command provides system-wide control over the maximum number of control connections that a vEdge router can establish to vSmart 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 router's tunnel interfaces.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  max-omp-sessions number
```

Syntax Description

number	Maximum Number of OMP Sessions: Set the maximum number of OMP sessions that a vEdge router can establish to vSmart controllers. These connections are DTLS or TLS control plane tunnels. Range: 0 through 100 Default: 2

Command History

Release	Modification
16.1	Command introduced.

Examples

Change the maximum number of vSmart controller connections to 4:

```
system
  max-omp-sessions 4
```

Operational Commands

show control affinity config

show control affinity status

show control connections

show control local-properties

Related Topics

controller-group-id, on page 150
controller-group-list, on page 151
exclude-controller-group-list, on page 207

max-control-connections, on page 329

memory-usage

To configure the memory-usage watermarks, use the **memory-usage** command in the alarms configuration mode. To revert to the default watermark values, use the **no** form of this command.

memory-usage [**high-watermark-percentage** *percentage*] [**medium-watermark-percentage** *percentage*] [**low-watermark-percentage** *percentage*] [**interval** *seconds*]

no memory-usage

Syntax Description

high-watermark-percentage*percentage*	Specifies the high-usage watermark percentage. Range: 1 to 100 percent Default: 90 percent
medium-watermark-percentage*percentage*	Specifies the medium-usage watermark percentage. Range: 1 to 100 percent Default: 75 percent
low-watermark-percentage*percentage*	Specifies the low-usage watermark percentage. Range: 1 to 100 percent Default: 60 percent
interval*seconds*	Specifies how frequently memory usage should be checked and reported by the device to Cisco vManage. Range: 1 to 4294967295 seconds Default: 5 seconds

Command Default

The default usage watermarks and polling interval are:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

Command Modes

Alarms configuration (config-alarms)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples

The following example shows a sample configuration of the memory-usage watermarks and the polling interval:

```
config
 system
  alarms
   memory-usage
    high-watermark-percentage 80
    medium-watermark-percentage 70
    low-watermark-percentage 50
    interval 10
```

Related Commands

Command	Description
alarms	Enters the alarms configuration mode.

mgmt-security

Configure the encryption of management frames sent on the wireless LAN (on vEdge cellular wireless routers only). Management frame encryption is defined in the IEEE 802.11w standard, which defines protected management frames (PMFs).

You can configure the encryption of management frames only if you have configured a data security method value other than **none**.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  interface vapnumber
    mgmt-security security
```

Syntax Description

security	Encryption of Management Frames Whether encryption of management frames is performed on wireless WANs. Values: none, optional, required Default: none

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure management frame encryption for VAP 3:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
...
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

data-security, on page 168

mode

Configure the mode to use in IKEv1 Diffie-Hellman key exchanges (on vEdge routers only).

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ike
      mode mode
```

Syntax Description

mode	Exchange Mode: Mode to use for IKEv1 Diffie-Hellman key exchanges. It can be one of the following: • aggressive: Use IKE aggressive mode to establish an IKE SA. In this mode, an SA is established with the exchange of only three negotiation packets. • main: Use IKE main mode to establish an IKE SA. In this mode, a total of six negotiation packets are exchanged to establish the SA. This is the default.

Command History

Release	Modification
17.2	Command introduced.

Examples

Configure aggressive mode for IKEv1 key exchanges:

```
vEdge(config)# vpn 1 interface ipsec1 ike
vEdge(config-ike)# mode aggressive
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

group, on page 218

mtu

Set the maximum MTU size of packets on the interface.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    mtu bytes
```

Syntax Description

bytes	MTU Size: MTU size, in bytes. For cellular interfaces, the maximum MTU is 1428 bytes. For IRB interfaces, the maximum MTU is 1500 bytes. For PPP interfaces, the maximum MTU is 1492 bytes. Range: 576 through 2000 bytes Default: 1500

Command History

Release	Modification
14.1	Command introduced.
16.3	Maximum MTU changed from 1804 bytes to 2000 bytes.

Example

Reduce the MTU size to support subinterfaces:

```
vpn 0
  interface ge0/0
    mtu 1496
```

Operational Commands

show interface

Related Topics

bfd color, on page 106
pmtu, on page 378
tcp-mss-adjust, on page 477

multicast-buffer-percent

Configure the amount of interface bandwidth that multicast traffic can use (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  multicast-buffer-percent percentage
```

Syntax Description

percentage	Interface Bandwidth: Set the percentage of interface bandwidth that multicast traffic can use. Range: 5 through 100 percent Default: 20 percent

Command History

Release	Modification
16.1	Command introduced.

Examples

Change the interface bandwidth available for multicast traffic to 50 percent:

```
system
  multicast-buffer-percent 50
```

Operational Commands

show running-config system

multicast-replicator

Configure a vEdge router to be a multicast replicator (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Multicast

Command Hierarchy

```
vpn vpn-id
  router
    multicast-replicator local [threshold number]
```

Syntax Description

local	Establishment of a Replicator: Configure the local router as a multicast replicator.

number	Replication Threshold: Number of joins per group that the router can accept. For each join, the router can accept 256 outgoing tunnel interfaces (OILs). Range: 0 through 1000 Default: 0. A value of 0 means that the router can accept any number of (*,G) and (S,G) joins.

Command History

Release	Modification
14.2	Command introduced.

Examples

Configure a vEdge router to be a multicast replicator:

```
vm1# show running-config vpn 1 router
 multicast-replicator local
!
```

Operational Commands

show multicast replicator

show multicast rfp

show multicast topology

show multicast tunnel

show omp multicast-auto-discover

show omp multicast-routes

show pim interface

show pim neighbor

show pim statistics

name

Provide a text description for the VPN (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  name string
```

Syntax Description

string	VPN Name: Text name or description of the VPN. If it includes spaces, enclose the entire string in quotation marks (" "). Maximum characters: 32

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure a description for VPN 1:

```
vpn 1
  name "Customer A VPN"
```

Operational Commands

show running-config vpn

name

Provide a text name for the Cisco vEdge device.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  name string
```

Syntax Description

string	Device Name: Name of the Cisco vEdge device. If it contains spaces, enclose the string in quotation marks (" "). Maximum characters: 255

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the SNMP name of this Cisco vEdge device:

```
vEdge(config)# snmp name "Engineering vEdge Router"
```

Operational Commands

show running-config snmp

nas-identifier

Configure the NAS identifier of the local router, to send to the RADIUS server during an 802.1X session (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    dot1x
      nas-identifier string
```

Syntax Description

string	NAS Identifier: NAS identifier of the local router. String 1 to 255 characters long.

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure a NAS identifier and IP address to send to the RADIUS server:

```
vEdge# show running-config vpn 0 dot1x
vpn 0
 interface ge0/0
  dot1x
   nas-identifier vedge@viptela.com
   nas-ip-address 1.2.3.4
  !
 !
!
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

acct-req-attr, on page 32
auth-req-attr, on page 88
nas-ip-address, on page 345
radius, on page 407
radius-servers, on page 411

nas-ip-address

Configure the NAS IP address of the local router, to send to the RADIUS server during an 802.1X session (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
```

```
dot1x
  nas-ip-address ip-address
```

Syntax Description

ip-address	IP Address: NAS IP address to send to the RADIUS server.

Examples

Configure a NAS identifier and IP address to send to the RADIUS server:

```
vEdge# show running-config vpn 0 dot1x
vpn 0
 interface ge0/0
  dot1x
   nas-identifier vedge@viptela.com
   nas-ip-address 1.2.3.4
  !
 !
!
```

Release Information

Release	Modification
16.3	Command introduced.

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

acct-req-attr, on page 32
auth-req-attr, on page 88
nas-identifier, on page 344
radius, on page 407
radius-servers, on page 411

nat

Configure a vEdge router to act as a NAT device (on vEdge routers only).

In the transport VPN (VPN 0), you can configure multiple NAT interfaces. In this configuration traffic is load-balanced, via ECMP, among the interfaces.

You can configure a NAT on a physical interface or on a **natpool** interface. You cannot configure NAT on a loopback interface. Note that for a **natpool** interface, you can configure only the interface's IP address, **shutdown** and **no shutdown** command, and the **nat** command and its subcommands. You cannot configure another other interface commands.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface [genumber/slot | natpoolnumber]
    nat
      block-icmp-error
      direction (inside | outside)
      log-translations
      natpool range-start ip-address1 range-end ip-address2
      [no] overload
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
private-ip-address ip-address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
     static source-ip ip-address1 translate-ip ip-address2 source-vpn vpn-id protocol (tcp
 | udp) source-port number translate-port number
      tcp-timeout minutes
      udp-timeout minutes
```

Syntax Description

None

Examples

Configure a vEdge router to act as a NAT:

```
vEdge# config
vEdge(config)# vpn 1 interface ge0/4 nat
```

Command History

Release	Modification
14.2	Command introduced.
15.1	Multiple NAT interfaces can be configured.
16.3	Added support for 1:1 static NAT and dynamic NAT.

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

Related Topics

encapsulation, on page 202
action, on page 48
ip gre-route, on page 264
ip route, on page 267

nat-refresh-interval

Configure the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. This interval is how often a tunnel interface sends a refresh packet to maintain the UDP packet streams that traverse a NAT.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      nat-refresh-interval seconds
```

Syntax Description

seconds	NAT Refresh Interval: 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 History

Release	Modification
16.1.1	Command introduced.

Examples

Change the NAT refresh interval to 30 seconds:

```
vEdge# show running-config vpn 0 interface ge0/2 tunnel-interface
vpn 0
 interface ge0/2
  tunnel-interface
   encapsulation ipsec
   color lte
   nat-refresh-interval 30
   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
  !
 !
!
```

Operational Commands

show running-config

natpool

Configure a pool of addresses to use in NAT translation (on vEdge routers only).

You configure NAT port forwarding on interfaces in the WAN transport VPN (VPN 0).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    nat
      natpool range-start ip-address1 range-end ip-address2
```

Syntax Description

range-start *ip-address1* **range-end** *ip-address2*	NAT Pool Address Range: Define the range of IP addresses to use for the NAT address pool. *ip-address1* must be less than or equal to *ip-address2*. The pool can contain a maximum of 32 IP addresses. The addresses must be in the same subnet as the interface's IP address.

Command History

Release	Modification
18.3	Command introduced.

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

neighbor

Configure a BGP neighbor (on vEdge routers only). For each neighbor, you must configure the remote AS number and enable the session by including the **no shutdown** command. All other configuration parameters are optional.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        address-family ipv4-unicast
          maximum-prefixes number [threshold] [restart minutes | warning-only]
          route-policy policy-name (in | out)
        capability-negotiate
        description string
        ebgp-multihop ttl
        next-hop-self
        password md5-digest-string
        remote-as remote-as-number
        send-community
        send-ext-community
        [no] shutdown
        timers
          advertisement-interval number
          connect-retry seconds
```

```
        holdtime seconds
        keepalive seconds
      update-source ip-address
```

Syntax Description

ip-address	Neighbor Address: IP address of the BGP neighbor.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure a BGP neighbor:

```
vEdge# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
bgp 123
   neighbor 1.10.10.10
    no shutdown
    remote-as 456
    !
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

network

Set the OSPF network type (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          network (broadcast | point-to-point)
```

Syntax Description

(**broadcast** | **point-to-point**)	Network Type: Set the OSPF type of network to which the interface is connect. A broadcast network is a WAN or similar network. In a point-to-point network, the interface connects to a single remote OSPF router. Default: **broadcast**

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure an interface as a point-to-point interface:

```
vm1# show running-config vpn 1 router ospf area 0
vpn 1
 router
ospf
   area 0
    interface ge0/1
      point-to-point
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

next-hop-self

Configure the router to be the next hop for routes advertised to the BGP neighbor (on vEdge routers only).

This feature is disabled by default. If you configure it, use the **no next-hop-self** command to return to the default.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
```

```
neighbor ip-address
  next-hop-self
```

Syntax Description

None

Examples

Configure the local vEdge router to be the next hop to its BGP neighbor:

```
vm1# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
bgp 123
  neighbor 1.10.10.10
    no shutdown
    remote-as 456
   next-hop-self
    !
   !
  !
 !
!
```

Command History

Release	Modification
14.1	Command introduced.

Operational Commands

show bgp routes

node-type

Configure a node type for Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only).

Note To ensure that Cloud OnRamp for SaaS is set up properly, configure it in vManage NMS, not using the CLI.

Command Hierarchy

```
vpn vpn-id
  cloudexpress
    node-type type
```

Syntax Description

type	Interface Node Type: Node type for Cloud OnRamp for SaaS on this interface. Values: client, gateway Default: client

Examples

Configure Cloud OnRamp for SaaS to act as a client in VPN 100:

```
vEdge# show running-config vpn 100 cloudexpress
vpn 100
 cloudexpress
  node-type client
 !
!
```

Command History

Release	Modification
16.3	Command introduced.

Operational Commands

clear cloudexpress computations

show cloudexpress applications

show cloudexpress gateway-exits

show cloudexpress local-exits

show omp cloudexpress

show running-config vpn cloudexpress

nssa

Configure an OSPF area to be an NSSA (a not-so-stubby area) (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
```

```
area number
  nssa
    no-summary
    translate (always | candidate | never)
```

Syntax Description

translate (**always** | **candidate** | **never**)	LSA Translation: Allow vEdge routers that are ABRs (area border routers) to translate Type 7 LSAs to Type 5 LSAs. Type 7 LSAs carry external route information within an NSSA, and with the exception of the link-state type, they have the same syntax as Type 5 LSAs, which are OSPF external LSAs. Type 7 LSAs originate in and are advertised throughout an NSSA; NSSAs do not receive or originate Type 5 LSAs. Type 7 LSAs are advertised only within a single NSSA and are not flooded into the backbone area or into any other area by ABRs. The information that Type 7 LSAs contain can be propagated into other areas if the LSAs are translated into Type 5 LSAs, which can then be flooded to all Type 5-capable areas. Because NSSAs do not receive full routing information and must have a default route to route to AS-external destinations, an NSSA ABR can originate a default Type 7 LSA (IP address of 0.0.0.0/0) into the NSSA. The default route originated by an NSSA ABR is never translated into a Type 5 LSA. However, a default route originated by an NSSA internal AS boundary router (a router that is not also an ABR) may be translated into a Type 5 LSA. • **always**—The router always acts as the translator for Type 7 LSAs. That is, no other router, even if it is an ABR, can be the translator. If two ABRs are configured to always be the translator, only one of them actually ends up doing the translation. • **candidate**—The router offers translation services, but does not insist on being the translator. • **never**—Translate no Type 7 LSAs.
no-summary	Summary Routes: Do not inject OSPF summary routes into the NSSA.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure area 1 to be an NSSA:

```
vm1# show running-config vpn 1 router ospf
vpn 1
 router
  ospf
   redistribute static
   redistribute omp
   area 0
    interface ge0/0
    exit
```

```
   exit
   area 1
    nssa
   exit
  !
 !
!
```

Operational Commands

show ospf process

ntp

Configure Network Time Protocol (NTP) servers and MD5 authentication keys for the NTP servers.

Configuring NTP on a Cisco vEdge device or controller allows that device or controller to contact NTP servers to synchronize time. Other devices are allowed to ask a Cisco vEdge device for the time, but no devices are allowed to use the Cisco vEdge device as an NTP server.

vManage Feature Template

For all Cisco vEdge devices or Cisco SD-WAN Control Components:

Configuration ► Templates ► NTP

Command Hierarchy

```
system
  ntp
    keys
      authentication key-id md5 md5-key
      trusted key-id
    server (dns-server-address | ipv4-address)
      key key-id
      prefer
      source-interface interface-name
      version number
      vpn vpn-id
```

Syntax Description

source-interface *interface-name*	Interface for NTP To Use: Configure outgoing NTP packets to use a specific interface to reach the NTP server. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored. This option establishes the identify of outgoing packets, but has no effect on how the packets are routed to the NTP server. The actual interface used to reach the server is determined solely by a routing decision made in the software kernel.

server (*dns-server-address* | *ipv4-address*)	Location of NTP Server: Configure the location of an NTP server, either by specifying its IPv4 address or the address of a DNS server that knows how to reach the NTP server. You can configure up to four NTP servers. The software uses the server at the highest stratum level.
authentication *key-id* **md5** *md5-key*	Authentication: • Enable MD5 authentication for NTP servers. Each MD5 key is identified by a key-id, which can be a number from 1 through 65535. For md5-key, enter either a cleartext or an AES-encrypted key.
trusted *key-id*	To designate an authentication key as trustworthy, specify the key in the **trusted** command.
key *key-id*	To associate an authentication key with a server, specify the key in the **key** command. For the key to work, you must mark it as trusted.
version *number*	NTP Version: Version of the NTP protocol software. Range: 1 through 4 Default: 4
prefer	Prefer an NTP Server: If you configure multiple NTP servers, the software chooses the one with the highest stratum level. If more than one server is at the same stratum level, you can prefer that server by configuring it as **prefer**.
vpn *vpn-id*	VPN to Reach NTP Server: VPN to use to reach the NTP server, or VPN in which the NTP server is located. *vpn-id* can be from 0 through 65530. If you configure multiple NTP servers, they must all be located or reachable in the same VPN. Range: 0 through 65530 Default: VPN 0

Command History

Release	Modification
14.1	Command introduced.
15.4	Added support for up to four NTP servers, MD5 authentication, and configuring the source interface.

Examples

Configure three NTP servers, including one that uses an NTP server provided by the NTP Pool Project at the Network Time Foundation. The local NTP servers use MD5 authentication.

```
vEdge# show running-config system ntp
system
 ntp
  keys
   authentication 1001 md5 $4$KXLzYT9k6M8zj4BgLEFXKw==
   authentication 1002 md5 $4$KXLzYTxk6M8zj4BgLEFXKw==
   authentication 1003 md5 $4$KXLzYT1k6M8zj4BgLEFXKw==
   trusted 1001 1002
  !
  server 192.168.15.243
   key     1001
   vpn     512
   version 4
  exit
  server 192.168.15.242
   key     1002
   vpn     512
   version 4
  exit
  server us.pool.ntp.org
   vpn     512
   version 4
  exit
 !
!
```

```
vEdge# show ntp peer | table

INDEX  REMOTE           REFID              ST  TYPE  WHEN  POLL  REACH  DELAY   OFFSET
JITTER
------------------------------------------------------------------------------------------
1      +192.168.15.243  17.253.6.253       2   u     57    64    377    0.126   -3.771
0.740
2      192.168.15.242   .INIT.             16  u     -     64    0      0.000   0.000
0.000
3      *69.50.231.130   216.218.254.202    2   u     60    64    377    14.694  0.239
2.174
```

```
vEdge# show ntp associations | table
                                                                  LAST
IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  EVENT     COUNT
-------------------------------------------------------------------------
1    18345    f41a    yes   yes           ok    candidate  sys_peer  1
2    18346    eb5a    yes   no            bad   reject     2         2
3    18347    961a    yes   yes           none  sys.peer   sys_peer  1
```

Operational Commands

clock set date

clock set time

show ntp associations

show ntp peer

Related Topics

allow-service, on page 63

offer-time

Configure how long the IP address offered to a DHCP client is reserved for that client (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      offer-time seconds
```

Syntax Description

seconds	Duration of IP Address Offer: How long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client. Range: 0 through 4294967295 seconds Default: 600 seconds

Command History

Release	Modification
14.3	Command introduced.

Examples

Reserve offered IP address for 2 minutes:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config-interface-ge0/4)# dhcp-server offer-time 120
vEdge(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   offer-time   120
  !
 !
!
```

Operational Commands

show dhcp interfaces

show dhcp server

omp

omp—Modify the OMP configuration (on vEdge routers and vSmart controllers only). By default, OMP is enabled on all vEdge routers and vSmart controllers.

vpn omp—Modify the OMP configuration in a particular VPN (on vEdge routers only). You can configure this command for any service-side VPN, that is, for any VPN except for VPN 0 and VPN 512.

vManage Feature Template

For vEdge routers and vSmart controllers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  advertise (bgp | connected | ospf type | eigrp | static) (on vEdge routers only)
  discard-rejected (on vSmart controllers only)
  ecmp-limit number (on vEdge routers only)
  graceful-restart
  overlay-as as-number (on vEdge routers only)
  send-backup-paths (on vSmart controllers only)
  send-path-limit number
  [no] shutdown
  timers
    advertisement-interval seconds
    eor-timer seconds
    graceful-restart-timer seconds
    holdtime seconds
```

On vEdge routers only:

```
vpn vpn-id
  omp
    advertise (aggregate prefix [aggregate-only] | bgp | connected | network prefix | ospf
 type | eigrp | static)
```

Syntax Description

shutdown	Disable OMP: Disable OMP. Doing so shuts down the Cisco SD-WAN overlay network. Default: OMP is enabled on all vEdge routers and vSmart controllers.

Command History

Release	Modification
14.1	Command introduced.

Release	Modification
16.3	Added **vpn omp** command.

Operational Commands

show omp peers

show omp routes

show omp services

show omp summary

show omp tlocs

on-demand enable

To enable dynamic on-demand tunnels on a spoke device, use the **on-demand enable** command in config-system mode. To disable dynamic on-demand tunnels, use the **no** form of this command.

on-demand enable

no on-demand enable

Command Default Disabled

Command Modes config-system

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines Use **on-demand enable** with **on-demand idle-timeout** to enable on-demand tunnels and configure the timeout in minutes. When there is no traffic in an on-demand tunnel, a timer begins. When the timeout interval is reached, the tunnel is removed and the on-demand link between the two devices is considered to by Inactive. Use **show system on-demand** to show the status of on-demand tunnels.

Example

In this example, the on-demand tunnel timeout is configured to 10 minutes.

```
Device(config-system)#on-demand enable
Device(config-system)#on-demand idle-timeout 10
```

on-demand idle-timeout

To configure the timeout interval for dynamic on-demand tunnels on a spoke device, use the **on-demand idle-timeout** command in config-system mode.

on-demand idle-timeout

Command Default

10 minutes

Command Modes

config-system

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines

Use **on-demand idle-timeout** with **on-demand enable** to enable on-demand tunnels and configure the timeout in minutes. When there is no traffic in an on-demand tunnel, a timer begins. When the timeout interval is reached, the tunnel is removed and the on-demand link between the two devices is considered to be Inactive. Use **show system on-demand** to show the status of on-demand tunnels.

Example

In this example, the on-demand tunnel timeout is configured to 10 minutes.

```
Device(config-system)#on-demand enable
Device(config-system)#on-demand idle-timeout 10
```

options

vpn interface dhcp-server options—Configure the DHCP options to send to the client when the DHCP client request them (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface geslot/port
    dhcp-server
      options
        default-gateway ip-address
        dns-servers ip-address
        domain-name domain-name
        interface-mtu mtu
        tftp-servers ip-address
```

Syntax Description

default-gateway *ip-address*	Default Gateway: IP address of a default gateway in the service-side network.

dns-servers *ip-address*	DNS Servers: One or more of IP addresses for a DNS server in the service-side network. You can specify up to eight addresses.
domain-name *domain-name*	Domain Name: Domain name that the DHCP client uses to resolve hostnames.
interface-mtu *mtu*	Interface MTU: MTU size on the interface to the DHCP client. Range: 68 to 65535 bytes
tftp-servers *ip-address*	TFTP Servers: IP address of a TFTP server in the service-side network. You can specify one or two addresses.
option-code 43 *ascii* | *hex*	Vendor specific information.
option-code 191 *ascii*	Vendor specific information.

Command History

Release	Modification
14.3	Command introduced.

Examples

Configure options to send when requested by a DHCP client:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vm5(config-interface-ge0/4)# dhcp-server options
vEdge(config-options)# default-gateway 10.0.100.100
vEdge(config-options)# dns-servers 10.0.100.8
vEdge(config-options)# tftp-servers 10.0.100.76
vEdge(config-interface-ge0/4)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   options
    default-gateway 10.0.100.100
    dns-servers 10.0.100.8
    tftp-servers 10.0.100.76
  !
 !
!
```

Operational Commands

show dhcp interface

show dhcp server

organization-name

system organization-name—Configure the name of your organization.

vManage Configuration

Administration ► Settings

Command Hierarchy

```
system
  organization-name name
```

Syntax Description

name	Organization Name: Configure 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 SD-WAN network devices.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure an organization name:

```
vEdge(config)# system organization-name "Cisco"
```

Operational Commands

show control local-properties

show orchestrator local-properties

Related Topics

request csr upload, on page 664

orgid

To configure the organization ID for Umbrella registration, on Cisco IOS XE Catalyst SD-WAN devices, use the **orgid** command in config-profile mode.

orgid *organization-id*

Syntax Description

organization-id	Organization ID (decimal).

Command Mode

config-profile

Command History

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

Examples

Use **parameter-map type umbrella global** to enter config-profile mode, then use **orgid**, **api-key**, and **secret** to configure Umbrella registration.

In config-profile mode, use **show full-configuration** to display Umbrella registration details.

Example

This example configures Umbrella registration details.

```
Device(config)# parameter-map type umbrella global
Device(config-profile)# orgid 1234567
Device(config-profile)# api-key aaa12345aaa12345aaa12345aaa12345
Device(config-profile)# secret 0 bbb12345bbb12345bbb12345bbb12345
```

ospf

vpn router ospf—Configure OSPF within a VPN on a vEdge router.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          authentication
            authentication-key key
            message-digest key
            type (message-digest | simple)
          cost number
```

```
      dead-interval seconds
      hello-interval seconds
      network (broadcast | point-to-point)
      passive-interface
      priority number
      retransmit-interval seconds
    ! end area interface
    nssa
      no-summary
      translate (always | candidate | never)
    range prefix/length
      cost number
      no-advertise
    stub
      no-summary
  ! end area
  auto-cost reference-bandwidth mbps
  compatible rfc1583
  default-information
    originate (always | metric metric | metric-type type)
  distance
    external number
    inter-area number
    intra-area number
  max-metric
    router-lsa (administrative | on-startup seconds)
  redistribute (bgp | connected | nat | natpool-outside | omp | static)
  route-policy policy-name in
  router-id ipv4-address
  timers
    spf delay initial-hold-time maximum-hold-time
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Examples

In VPN 1 on a vEdge router, configure OSPF area 0. The interface **ge0/0** participates in the local OSPF network.

```
vEdge# show running-config vpn 1 router ospf
vpn 1
 router
  ospf
   redistribute static
   redistribute omp
   area 0
    interface ge0/0
    exit
   exit
  !
 !
!

vEdge# show interface vpn 1
```

```
                              IF      IF
                              ADMIN   OPER    ENCAP  PORT                                SPEED
            RX       TX
VPN  INTERFACE  IP ADDRESS    STATUS  STATUS  TYPE   TYPE     MTU   HWADDR              MBPS   DUPLEX
UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------------------------------
1    ge0/0      10.2.2.11/24  Up      Up      null   service  1500  00:0c:29:ab:b7:58  10     full
0:01:36:54  725      669
```

Monitoring Commands

show ospf database

show ospf database-summary

show ospf interface

show ospf neighbor

show ospf process

show ospf routes

ospfv3 authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) instance, use the **ospfv3 authentication** command in interface configuration mode. To remove the authentication type for an interface, use the **no** form of this command.

ospfv3 authentication ipsec spi *spi-number* { **md5** | **sha1** } { **0** | **7** } *key-string*
no ospfv3 authentication ipsec

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi-number*	Specifies the Security Policy Index (SPI) value. The *spi-number* value must be a number from 256 to 4294967295.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	One of the following values can be entered: • **0** --The key is not encrypted. • **7** --The key is encrypted.
key-string	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.

Command Default No authentication is specified.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 17.3.2	This command was introduced on Cisco IOS XE SD-WAN devices.

Usage Guidelines Use the **ospfv3 authentication** command to specify the OSPFv3 authentication type on an interface. The **ospfv3 authentication** command cannot be configured per process. If the **ospfv3 authentication** command is used, it affects all OSPFv3 instances.

The **ospfv3 authentication** command applies to all instances of OSPFv3 configured for the interface using the **ospfv3 instance {ipv4 | ipv6} area** *area-id* command.

The following is an example of OSPFv3 IPsec authentication configuration with a MD5 key:

```
Device(config)# interface GigabitEthernet2
Device(config-if)# vrf forwarding 1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 30:1:1::1/64
Device(config-if)# ospfv3 authentication ipsec spi 256 md5 FEEDACEEDEADBEEFFEEDACEEDEADBEEF

Device(config-if)# ospfv3 1 ipv6 area 0
Device(config-if)# ospfv3 1 ipv4 area 0
!
```

The following is an example of OSPFv3 IPsec authentication configuration with a SHA1 key:

```
Device(config)# interface GigabitEthernet4
Device(config)# vrf forwarding 1
Device(config-if)# ip address 10.0.0.0 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 40:1:1::1/64
Device(config-if)# ospfv3 authentication ipsec spi 300 sha1
FEEDACEEDEADBEEFFEEDACEEDEADBEEFFEEDACEE
Device(config-if)# ospfv3 1 ipv4 area 0
```

overlay-as

omp overlay-as—Configure a BGP AS number that OMP advertises to the router's BGP neighbors (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  overlay-as as-number
```

Syntax Description

as-number	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 History

Release	Modification
17.1	Command introduced.

Operational Commands

show bgp routes

show omp routes

Related Topics

propagate-aspath, on page 406

overload

vpn interface nat overload— Control the mapping of addresses on a vEdge router that is acting as a NAT device (on vEdge routers only). By default, the **overload** function is enabled, which enables dynamic NAT.

Addresses are mapped one to one until the address pool is depleted. Then, in Release 16.3.0, the last address is used multiple times, and the port number is changed to a random value between 1024 and 65535. For Releases 16.3.2 and later, when the address pool is depleted, the first address in the pool is used multiple times. This reuse of the last address is called *overloading*. Overloading effectively implements dynamic NAT.

To enable static NAT, which maps a single source IP address to a single translated IP address, include the **no overload** command in the configuration. With this configuration, when the maximum number of available IP addresses is reached, you cannot configure any more mappings between source and translated addresses.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface natpoolnumber
    nat
      [no] overload
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Examples

Dynamic NAT

Configure a vEdge router to perform dynamic NAT:

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
  no shutdown
!
```

Static NAT

Configure a vEdge router to perform static NAT, translating a service-side and a remote IP address:

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
    static source-ip 10.1.17.3 translate-ip 10.15.1.4 inside
    static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
    direction inside
    no overload
  !
  no shutdown
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

Related Topics

encapsulation, on page 202

static, on page 462

parameter-map type umbrella global

To enter config-profile mode, to view or configure Umbrella registration details, on Cisco IOS XE Catalyst SD-WAN devices, use the **parameter-map type umbrella global** command in global configuration mode.

parameter-map type umbrella global

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration (config)

Examples

Use the **parameter-map type umbrella global** command to enter config-profile mode, then use one of the following to display the current Umbrella registration details, or to configure Umbrella registration.

Example

This example displays the Umbrella registration details for a device.

```
Device(config)# parameter-map type umbrella global
Device(config-profile)# show full-configuration
parameter-map type umbrella global
local-domain umbrella_bypass
dnscrypt
orgid        1234567
api-key      aaa12345aaa12345aaa12345aaa12345
secret 0 bbb12345bbb12345bbb12345bbb12345
```

Example

This example configures the Umbrella registration details.

```
Device(config)# parameter-map type umbrella global
Device(config-profile)# orgid 1234567
Device(config-profile)# api-key aaa12345aaa12345aaa12345aaa12345
Device(config-profile)# secret 0 bbb12345bbb12345bbb12345bbb12345
```

parent

To configure a server as an NTP parent, use the **parent enable** command in system configuration mode. To remove the NTP parent configuration, use the **no** form of this command.

parent enable [**source-interface** *inteface-name*] [**stratum** *stratum-value*] [**vpn** *vpn-id*]
no parent enable

Syntax Description

source-interface *interface-name*	Sets the interface that the NTP parent server uses to respond to NTP requests. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is rejected.
stratum *stratum-value*	Sets the stratum, which defines the distance of the router from a reference clock and defines the reliability and accuracy of the NTP source. Valid values are integers 1 through 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 7.
vpn *vpn-id*	Sets the VPN for which this device acts as the NTP parent server. If you configure multiple NTP servers, they must all be located or reachable in the same VPN. Range: 0 through 65530 Default: VPN 0

Command Default

NTP parent is not configured

Command Modes

ntp configuration (config-ntp)

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	This command was introduced.

Usage Guidelines

The following example shows how to configure a server as an NTP parent.

Example

The following example shows how to configure a track list for interfaces.

```
Device# config terminal
Device(config)# system
Device(config-system) ntp
Device(config-ntp)# parent
Device(config-parent)# enable
Device(config-parent)# source-interface loopback511
Device(config-parent)# stratum 6
Device(config-parent)# vpn 511
```

Table 8: Related Commands

Command	Description
peer	Configure an NTP parent to support NTP in symmetric active mode using.

passive-interface

vpn router ospf area interface passive-interface—Set the OSPF interface to be passive (on vEdge routers only). A passive interface advertises its address, but it does not actively run the OSPF protocol.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          passive-interface
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure a passive OSPF interface:

```
vEdge(config)# show config
vpn 1
 router
  ospf
   area 0
    interface ge0/1
     passive-interface
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

password

vpn router bgp neighbor password—Configure message digest5 (MD5) authentication and an MD5 password on the TCP connection with the BGP peer (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        password md5-digest-string
```

Syntax Description

md5-digest-string	Password: Password to use to generate an MD5 message digest. It is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure an MD5 password to a BGP neighbor:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 router bgp 1 neighbor 172.16.255.18
vEdge(config-neighbor-172.16.255.18)# password mypasswordhere
vEdge(config-neighbor-172.16.255.18)# show config
vpn 1
 router
  bgp 1
   neighbor 172.16.255.18
    no shutdown
    password  $4$NGrwc30Xn6BB6+gFXiRXKw==
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

peer

To configure a server to support NTP in symmetric active mode, use the **peer** command in system configuration mode. To remove the configuration, use the **no** form of this command.

peer *ip-address* [**key** *key-id*] [**vpn** *vpn-id*] [**version** *version-number*] [**source-interface** *interface-name*]
no peer *ip-address*

Syntax Description

peer *ip-address*	Configures a Cisco vEdge device to support NTP in symmetric active mode. Enter the IP address of the peer to use for NTP in this mode. When a server is defined with this keyword, NTP routers synchronize with this peer if they cannot reach the parent NTP router. If this keyword is not used, the Cisco vEdge device operates in symmetric passive mode and does not synchronize with the peer.
key *key-id*	Designates the ID of the MD5 authentication key for the peer.
vpn *vpn-id*	Designates the VPN to use to reach the peer, or VPN in which the peer is located. You can configure multiple NTP servers. Each NTP peer, NTP server, and NTP parent server must be located in the same VPN. Range: 0 through 65530 Default: VPN 0
version *version-number*	Designates the version of the NTP protocol software. Range: 1 through 4 Default: 4
source-interface *interface-name*	Configures the specific interface for the local NTP process to use to communicate with the peer. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.

Command Default

Peer is not configured

Command Modes

ntp configuration (config-ntp)

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	This command was introduced.

Usage Guidelines

You can configure up to two devices to support NTP in symmetric active mode.

A device that is configured as an NTP peer should also be configured as an NTP parent.

The source interface must be in the VPN that is configured for the peer.

Example

The following example shows how to configure a server as an NTP peer.

```
Device# config terminal
Device(config)# system
Device(config-system) ntp
Device(config-ntp)# peer 172.16.10.1
Device(config-peer)# key 101
Device(config-peer)# vpn 511
Device(config-peer)# version 4
Device(config-peer)# source-interface ge0/1
```

Table 9: Related Commands

Command	Description
parent	Configures a Cisco vEdge device as an NTP parent.

perfect-forward-secrecy

vpn interface ipsec ipsec perfect-forward-secrecy—Configure the perfect forward secrecy (PFS) settings to use on an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only). PFS ensures that past sessions are not affected if future keys are compromised

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ipsec
      perfect-forward-secrecy pfs-setting
```

Syntax Description

pfs-setting	PFS Setting for IPsec Tunnel: Type of PFS to use on an IPsec tunnel that is being used for IKE key exchange. It can be one of the following: • **group-2**—Use the 1024-bit Diffie-Hellman prime modulus group. • **group-14**—Use the 2048-bit Diffie-Hellman prime modulus group. • **group-15**—Use the 3072-bit Diffie-Hellman prime modulus group. • **group-16**—Use the 4096-bit Diffie-Hellman prime modulus group. • **none**—Disable PFS. Default: **group-16**

Command History

Release	Modification
17.2.3	Command introduced.

Examples

Example 1

Have the IPsec tunnel use the 2048-bit modulus group:

```
vEdge(config)# vpn 1 interface ipsec1 ipsec
vEdge(config-ike)# perfect-forward-secrecy group-14
```

Example 2

For a Microsoft Azure end point that does not support PFS, disable PFS on an IPsec tunnel:

```
vEdge(config)# vpn 1 interface ipsec1 ipsec
vEdge(config-ipsec)# perfect-forward-secrecy none
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

pim

vpn router pim— Configure PIM (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      auto-rp
      interface interface-name
        hello-interval seconds
        join-prune-interval seconds
      replicator-selection
      [no] shutdown
      spt-threshold kbps
```

Syntax Description

None

Command History

Release	Modification
14.2	Command introduced.

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show omp multicast-auto-discover

show omp multicast-routes

show pim interface show pim neighbor

pmtu

vpn interface pmtu—Enable path MTU (PMTU) discovery on the interface, using ICMP. When PMTU is enabled, the device automatically negotiates the largest MTU size that the interface supports in an attempt to minimize or eliminate packet fragmentation.

By default, PMTU discovery using ICMP is disabled.

On vEdge routers, the Cisco SD-WAN BFD software automatically performs PMTU discovery on each transport connection (that is, for each TLOC, or color). BFD PMTU discovery is enabled by default, and it is recommended that you use it and that you not configure ICMP PMTU discovery on router interfaces.

vManage Feature Template

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)Configuration ► Templates ► VPN Interface EthernetConfiguration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    pmtu
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Examples

Enable path MTU discovery on a vSmart interface:

```
vpn 0
  interface eth1
    pmtu
```

Operational Commands

show interface detail

Related Topics

bfd color, on page 106
clear-dont-fragment, on page 128
mtu, on page 339

policer

policy policer—Configure or apply a policer to be used for data traffic. For centralized data policy, you can police unicast traffic. For localized data policy (ACLs), you can police unicast and multicast traffic.

vManage Feature Template

For vEdge routers and vSmart controllers:

Configuration ► Policies

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet (for vEdge routers only)

Configuration ► Templates ► VPN Interface GRE (for vEdge routers only)

Configuration ► Templates ► VPN Interface PPP (for vEdge routers only)

Configuration ► Templates ► VPN Interface PPP Ethernet (for vEdge routers only)

Command Hierarchy

Configure a Policer

```
policy
  policer policer-name
    burst bytes
    exceed action
    rate bps
```

Apply a Policer in Centralized Data Policy

On vSmart controllers only.

```
policy
  data-policy policy-name
    vpn-list list-name
      sequence number
        action accept
          set policer policer-name
```

Apply a Policer via an Access List

On vEdge routers only.

```
policy
  access-list list-name
    sequence number
      action accept
        policer policer-name
```

Apply a Policer Directly to an Interface

On vEdge routers only.

```
vpn vpn-id
  interface interface-name
    policer policer-name (in | out)
```

Syntax Description

policer-name	Policer Name: Name of the policer. It can be a text string from 1 to 32 characters long. When you include a policer in the action portion of an access list or when you apply a policer directly to an interface, the name must match that which you specified when you created the policer with the **policy policer** configuration command. The number of policer-name entries is limited to 2048.
burst *bytes* **exceed** *action* **rate** *bps*	Policer Parameters: Define the policing parameters: • **burst** is the maximum traffic burst size. *bytes* can be a value from 15000 to 10000000. • **exceed** is the action to take when the burst size or traffic rate is exceeded. *action* can be drop (the default) or remark. The drop action is equivalent to setting the packet loss priority (PLP) to low. The remark action sets the PLP to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the match plp option. • **rate** is the maximum traffic rate, in bits per second. *bps* can be value from 0 through 264 – 1.
policy access-list *access-list* **sequence** *number* **action accept policer** *policer-name* **vpn interface access-list** *list-name* (**in** | **out**)	Apply a Policer Conditionally to an Interface, via an Access List: To apply a policer via an access list, first configure the name of the policer in the **action** portion of the access list. Then apply that access list to the interface, specifying the direction in which to apply it. 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. Enabling a policer via an access lists applies the policing parameters conditionally, only to traffic transiting the interface in the specified direction that matches the parameters in the access list.

vpn interface policer *policer-name* (**in** | **out**)	Apply a Policer Unconditionally to an Interface: Apply a policer directly to an interface, specifying the direction in which to apply it. 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. Applying a policer directly to an interface applies the policing parameters unconditionally, to all traffic transiting the interface in the specified direction.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added support for multicast traffic.
26.2.1	The number of policer-name entries limited to 2048.

Examples

Example 1

Create a policer, and apply it conditionally to outbound traffic on an interface in VPN 1:

```
policy
 policer p1
  rate   1000000
  burst  15000
  exceed drop
 !
 access-list acl1
  sequence 1
   match
    source-ip        2.2.0.0/16
    destination-ip   10.1.1.0/24 100.1.1.0/24
    destination-port 20 30
    protocol         6 17 23
   !
   action accept
    policer p1
   !
  !
  default-action drop
 !
!
vpn 1
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
  access-list acl1 out
 !
!
```

Example 2

Apply the same policer unconditionally to outbound traffic on the same interface:

```
policy
 policer p1
  rate   1000000
  burst  15000
  exceed drop
 !
 vpn 1
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
  policer p1
 !
!
```

Operational Commands

clear policer statistics

show interface detail

show policer

show running-config

Related Topics

control-session-pps, on page 149
host-policer-pps, on page 231
icmp-error-pps, on page 232
match, on page 316

policy

policy—Configure IPv4 policy (on vSmart controllers and vEdge routers only).

vManage Feature Template

For vEdge routers and vSmart controllers:

Configuration ► Policies

Configuration ► Security (for zone-based firewall policy)

Command Hierarchy

For Application-Aware Routing Policy

Configure on vSmart controllers only.

```
policy
  lists
    app-list list-name
      (app application-name | app-family family-name)
    data-prefix-list list-name
```

```
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn vpn-id
  sla-class sla-class-name
    jitter milliseconds
    latency milliseconds
    loss percentage

policy
  app-route-policy policy-name
    vpn-list list-name
      default-action sla-class sla-class-name
        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
          protocol number
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port address
        action
          backup-sla-preferred-color color
          count counter-name
          log
          sla-class sla-class-name [strict] [preferred-color colors]
```

For Centralized Control Policy

Configure on vSmart controllers only.

```
policy
  lists
    color-list list-name
      color color
    prefix-list list-name
      ip-prefix prefix/length
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id

policy
  control-policy policy-name
    default-action action
      match
        route
          color color
          color-list list-name
          omp-tag number
          origin protocol
          originator ip-address
          preference number
          prefix-list list-name
          site-id site-id
          site-list list-name
          tloc ip-address color color [encap encapsulation]
          tloc-list list-name
          vpn vpn-id
```

```
        vpn-list list-name
      tloc
        carrier carrier-name
        color color
        color-list list-name
        domain-id domain-id
        group-id group-id
        omp-tag number
        originator ip-address
        preference number
        site-id site-id
        site-list list-name
        tloc address color color [encap encapsulation]
        tloc-list list-name
    action
      reject
      accept
        set
          omp-tag number
          preference value
          service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
          tloc-action action
          tloc-list list-name
```

For Centralized Data Policy

Configure on vSmart controllers only.

```
policy
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
      source-interface interface-name
    flow-active-timeout seconds
    flow-inactive-timeout seconds
    flow-sampling-interval number
    template-refresh seconds
  lists
    app-list list-name
      (app applications | app-family application-families)
    data-prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn-id vpn-id

policy
  data-policy policy-name
    vpn-list list-name
      default-action action
        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
          protocol number
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port number
          tcp flag
```

```
        action
          cflowd (not available for deep packet inspection)
          count counter-name
          drop
          log
          tcp-optimization
          accept
            nat [pool number] [use-vpn 0] (in Releases 16.2 and earlier, not available for
 deep packet inspection)
            redirect-dns (host | ip-address)
            set
              dscp number
              forwarding-class class
              local-tloc color color [encap encapsulation]
              local-tloc-list color color [encap encapsulation] [restrict]
              next-hop ip-address
              policer policer-name
              service service-name local [restrict] [vpn vpn-id]
              service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]
              tloc ip-address color color [encap encapsulation]
              tloc-list list-name
              vpn vpn-id
```

```
policy
  data-policy policy-name
    default-action action
      match
        app-list list-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dscp number
        packet-length number
        protocol number
        source-data-prefix-list list-name
        source-ip prefix/length
        source-port address
        tcp flag
      action
        count counter-name
        drop
        accept
          set local-tloc color
          set next-hop ip-address
          set policer policer-name
          set service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
          set tloc ip-address
          set vpn vpn-id
  vpn-membership policy-name
    default-action action
      match
        vpn vpn-id
        vpn-list list-name
      action
        (accept | reject)
```

For Localized Control Policy

Configure on vEdge routers only.

```
policy
  lists
```

```
    as-path-list list-name
      as-path as-number
    community-list list-name
      community [aa:nn | internet | local-as | no-advertise | no-export]
    ext-community-list list-name
      community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
    prefix-list list-name
      ip-prefix prefix/length
policy
  route-policy policy-name
    default-action action
      match
        address list-name
        as-path list-name
        community list-name
        ext-community list-name
        local-preference number
        metric number
        next-hop list-name
        omp-tag number
        origin (egp | igp | incomplete)
        ospf-tag number
        peer address
      action
        reject
        accept
          set
            aggregator as-number ip-address
            as-path (exclude | prepend) as-number
            atomic-aggregate
            community value
            local-preference number
            metric number
            metric-type (type1 | type2)
            next-hop ip-address
            omp-tag number
            origin (egp | igp | incomplete)
            originator ip-address
            ospf-tag number
            weight number
```

For Localized Data Policy for IPv4

Configure on vEdge routers only.

```
policy
  lists
    prefix-list list-name
      ip-prefix prefix/length
  class-map
    class class-name queue number
  log-frequency number
    remote-dest ip-address source ip-address
  policer policer-name
    burst types
    exceed action
    rate bps
    bandwidth-percent percentage
    buffer-percent percentage
    class class-name
    drops drop-type
  rewrite-rule rule-name
    class class-name priority dscp (high | low) layer-2-cos number
```

```
policy
  access-list acl-name
    default-action action
      match
        class class-name
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        dscp number
        packet-length number
        plp (high | low)
        protocol number
        source-data-prefix-list list-name
        source-ip prefix-length
        source-port number
        tcp flag
      action
        count counter-name
        drop
        log
        accept
          class class-name
          policer policer-name
          set dscp value
          set next-hop ipv4-address
```

For Zone-Based Firewalls

Configure on vEdge routers only.

```
policy
  lists
    prefix-list list-name
      ip-prefix prefix/length
  tcp-syn-flood-limit number
  zone (destination-zone-name | source-zone-name)
    vpn vpn-id
  zone-to-no-zone-internet (allow | deny)
  zone-pair pair-name
    source-zone source-zone-name
    destination-zone destination-zone-name
    zone-policy policy-name
  zone-based-policy policy-name
    default-action action
      match
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        protocol number
        source-data-prefix-list list-name
        source-ip prefix-length
        source-port number
      action
        drop
        inspect
        log
        pass
```

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
14.2	Added application-aware routing policy.
18.2	Added zone-based firewall policy.

Examples

Apply a control policy to the sites defined in the list "west":

```
apply-policy
  site-list west control-policy change-tloc out
```

Operational Commands

show running-config

Related Topics

access-list, on page 30
apply-policy, on page 72
policy ipv6, on page 388
redistribute, on page 416

policy ipv6

policy ipv6—Configure IPv6 policy (on vEdge routers only).

Command Hierarchy

Localized Data Policy for IPv6

Configure on vEdge routers only.

```
policy
  policer policer-name
    burst types
    exceed action
    rate bps
```

```
policy ipv6
  access-list acl-name
    default-action action
    sequence number
      match
        class class-name
        destination-port number
        next-header protocol
        packet-length number
        plp (high | low)
        source-port number
        tcp flag
        traffic-class value
```

```
      action
        drop
          count counter-name
          log
        accept
          class class-name
          count counter-name
          log
          policer policer-name
          set
            traffic-class value
```

Syntax Description

None

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure an IPv6 ACL that changes the traffic class on TCP port 80 data traffic, and apply the ACL to an interface in VPN 0:

```
vEdge# show running-config policy ipv6 access-list
policy
 ipv6 access-list traffic-class-48-to-46
 sequence 10
  match
   destination-port 80
   traffic-class    48
  !
  action accept
   count port_80
   log
   set
    traffic-class 46
   !
  !
 !
 default-action accept
 !
!
vEdge# show running-config vpn 0 interface ge0/7 ipv6
vpn 0
 interface ge0/7
  ipv6 access-list traffic-class-48-to-46 in
 !
!
```

Operational Commands

show running-config

Related Topics

policy, on page 382

port-forward

vpn interface nat port-forward—On a vEdge router operating as a NAT gateway, create port-forwarding rules to allow requests from an external network to reach devices on the internal network (on vEdge routers only). You can create up to 128 rules.

You configure NAT port forwarding on interfaces in the WAN transport VPN (VPN 0).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    nat
      port-forward port-start port-number1 port-end port-number2
        proto (tcp | udp) private-ip-address ip-address private-vpn vpn-id
```

Syntax Description

port-start *port-number1* **port-end** *port-number2*	Port or Range of Ports: Define the port or port range of interest. *port-number1* must be less than or equal to *port-number2*. To apply port forwarding to a single port, specify the same port number for the starting and ending numbers. When applying port forwarding to a range of ports, the range includes the two port numbers that you specify—*port-number1* and *port-number2*. Packets whose destination port matches the configured port or ports are forwarded to the internal device. Range: 0 through 65535
private-ip-address *ip-address*	Private Server: IP address of the internal device to which to direct traffic that matches the port-forwarding rule.
private-vpn *vpn-id*	Private VPN: Private VPN in which the internal device resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65535
(**tcp** | **udp**)	Protocol: Protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.

Command History

Release	Modification
15.1	Command introduced.

Examples

Configure a NAT port filter:

```
vEdge(config-nat)# show full-configuration
vpn 0
 interface ge0/7
  nat
   port-forward port-start 80 port-end 90 proto tcp
    private-vpn        1
    private-ip-address 10.10.1.2
   !
  !
 !
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

port-hop

system port-hop, vpn 0 interface tunnel-interface—For a Cisco vEdge device that is behind a NAT device or for an individual tunnel interface (TLOC) on that Cisco vEdge device, rotate through a pool of preselected OMP port numbers, known as base ports, to establish DTLS connections with other Cisco vEdge devices when a connection attempt is unsuccessful (on vEdge routers, vManage NMSs, and vSmart controllers only). By default, port hopping is enabled on vEdge routers and on all tunnel interfaces on vEdge routers, and it is disabled on vManage NMSs and vSmart 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 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.

vManage Feature Template

For vEdge routers, vManage NMSs, and vSmart controllers only:

Configuration ► Templates ► System

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
system
  port-hop
vpn 0
  interface interface-name
    tunnel-interface
      port-hop
```

Syntax Description

no port-hop	Disable Port Hopping: Disable port hopping on the device, or if global port hopping is enabled, disable port hopping on an individual TLOC. If you disable port hopping on the device, by configuring **no port-hop** at the **system** level, port hopping on all tunnel interfaces is disable, and you cannot enable it on an individual tunnel interface. By default, port hopping is enabled on vEdge routers and on all tunnel interfaces on vEdge routers, and it is and disabled on vManage NMSs and vSmart controllers.

Examples

Enable port hopping:

```
system
  port-hop
```

Command History

Release	Modification
14.3	Command introduced.
15.1	Port hopping enabled by default.
15.3.8	Added support for BFD port hopping.
16.2	Port hopping is disabled by default on vManage NMSs and vSmart controllers.

Operational Commands

request port-hop

show control local-properties

Related Topics

graceful-restart, on page 214
port-offset, on page 393
request port-hop, on page 693

port-offset

system port-offset—Offset the base port numbers to use for the TLOC when multiple Cisco vEdge devices are present behind a single NAT device. Each device must have a unique port number so that overlay network traffic can be correctly delivered.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  port-offset number
```

Syntax Description

number	Offset Value: Offset value from the default base port numbers, which are 12346, 12366, 12386, 12406, and 12426. Range:: 0 through 19

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure a port offset value:

```
vEdge# show control local-properties
organization-name            Cisco
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Not Applicable
certificate-not-valid-before Not Applicable
certificate-not-valid-after  Not Applicable

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     0
system-ip                    172.16.255.11
chassis-num/unique-id        7e7a6da3-ec1c-4d3a-bf74-d14a6afca6eb
serial-num                   NOT-A-HARDWARE
keygen-interval              1:00:00:00
retry-interval               0:00:00:16
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:30:00
port-hopped                  TRUE
time-since-last-port-hop     0:00:06:38
number-vbond-peers           1

INDEX   IP                PORT
------------------------------
0       10.1.14.14        12346

       PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                  ADMIN     OPERATION
INDEX  IP               PORT    IP               PORT     VSMARTS  WEIGHT  COLOR           CARRIER         PREFERENCE  STATE     STATE
-------------------------------------------------------------------------------------------------------------------------------------
0      10.0.5.11        12346   10.0.5.11        12346    2        1       lte             default         0           up        up
```

```
vEdge# config
vEdge(config)# system port-offset 1
vEdge(config-system)# command and-quit
Commit complete.
vEdge# show control local-properties
organization-name            Cisco
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Not Applicable
certificate-not-valid-before Not Applicable
certificate-not-valid-after  Not Applicable

dns-name                     10.1.14.14
site-id                      100
protocol                     dtls
tls-port                     0
system-ip                    172.16.255.11
chassis-num/unique-id        7e7a6da3-ec1c-4d3a-bf74-d14a6afca6eb
serial-num                   NOT-A-HARDWARE
keygen-interval              1:00:00:00
retry-interval               0:00:00:16
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:30:00
port-hopped                  TRUE
time-since-last-port-hop     0:00:06:38
number-vbond-peers           1

INDEX   IP                PORT
-------------------------------
0       10.1.14.14        12346

       PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                    ADMIN     OPERATION
INDEX  IP               PORT    IP               PORT     VSMARTS  WEIGHT  COLOR            CARRIER          PREFERENCE  STATE     STATE
-------------------------------------------------------------------------------------------------------------------------------------
0      10.0.5.11        12347   10.0.5.11        12347    2        1       lte              default          0           up        up
```

Operational Commands

show control local-properties

show orchestrator local-properties

Related Topics

port-hop, on page 391

request port-hop, on page 693

port-scan

To enable port-scanning detection, enable the **port-scan** command in United Threat Defense (UTD) multitenancy threat configuration mode or UTD single-tenancy threat configuration mode. To disable port-scanning detection, use the **no** form of this command.

port-scan

no port-scan

Syntax Description

This command has no arguments or keywords.

Command Default

By default, port-scanning detection is disabled, so you have to enable port-scanning detection.

Command Modes

UTD multitenancy threat configuration mode (utd-mt-threat)

UTD single-tenancy threat configuration mode (utd-eng-std)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This command was introduced.

Usage Guidelines

The **port-scan** command can detect, but not block possible port-scan attacks.

For more information on port-scanning detection, see the Configure Port-Scanning Detection Using a CLI Template section in the Security Configuration Guide, Cisco IOS XE Release 17.x.

For more information on specifying the alert level for port-scanning detection, see the sense level command.

Examples

The following example shows how to enable port-scanning detection:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-mt-threat)# threat protection profile 101
Device(config-utd-mt-threat)# port-scan
Device(config-utd-mt-threat-port-scan)# sense level low
```

The following example shows how to disable port-scanning detection:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-mt-threat)# threat-inspection profile 101
Device(config-utd-mt-threat)# no port-scan
```

The following example shows how to enable port-scanning detection in UTD single-tenancy threat configuration mode:

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# port-scan
Device(config-utd-threat-port-scan)# sense level low
```

The following example shows how to disable port-scanning detection in UTD single-tenancy threat configuration mode:

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# no port-scan
```

ppp

vpn 0 interface ppp—Configure the properties for a PPP virtual interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn 0
  interface pppnumber
    ppp
      ac-name name
      authentication
        chap hostname hostname password password
        pap sent-username username password password
```

Syntax Description

ac-name *name*	Access Concentrator Name: Name of the access concentrator used by PPPoE to route connections to the internet.
chap hostname *hostname* **password** *password*	Authentication Credentials for CHAP: Hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters. You can configure both CHAP and PAP authentication on the same PPP interface. The software tries both methods and uses the first one that succeeds.
pap sent-username *username* **password** *password*	Authentication Credentials for PAP: Username and password provided by your Internet Service Provider (ISP). *sent-username* can be up to 255 characters. You can configure both CHAP and PAP authentication on the same PPP interface. The software tries both methods and uses the first one that succeeds.

Examples

Configure CHAP authentication on a PPP interface:

```
vEdge# show running-config vpn 0 interface ppp10
vpn 0
 interface ppp10
  ppp authentication chap
   hostname branch100@corp.bank.myisp.net
   password $4$OHHjdmsC7M8zj5BgLEFXKw==
  ppp ac-name text

  !
```

Command History

Release	Modification
15.3.3	Command introduced.
17.1	Added ability to configure both CHAP and PAP authentication on a PPP interface.

Operational Commands

clear pppoe statistics

show pppoe session

show pppoe statistics

show ppp interface

Related Topics

pppoe-client, on page 397

pppoe-client

vpn 0 interface pppoe-client—Enable the PPPoE client on the interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn 0
  interface geslot/port
    pppoe-client
      ppp-interface pppnumber
```

Syntax Description

ppp*number*	Interface Name: Name of the PPP interface. Possible values: from **ppp1** through **ppp31**

Command History

Release	Modification
15.3.3	Command introduced.

Examples

Configure an interface to run the PPPoE client:

```
vEdge# show running-config vpn 0
vpn 0
  interface ge0/1
    pppoe-client ppp-interface ppp10
    no shutdown
  !
```

Operational Commands

clear pppoe statistics

show interface detail

show ppp interface

show pppoe session

show pppoe statistics

Related Topics

ppp, on page 395

priority

vpn router ospf area interface priority—Set the priority of the router to be elected as the designated router (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          priority number
```

Syntax Description

number	Designated Router Priority: Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR. Range: 0 through 255 Default: 1

Command History

Release	Modification
14.1	Command introduced.

Examples

Set the router's DR priority to 127

```
vEdge# show running-config vpn 1 router ospf area 0
vpn 1
 router
  ospf
   area 0
    interface ge0/0
      priority 127
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

Related Topics

router-id, on page 437

probe

To configure specific SaaS applications for Cloud onRamp for SaaS, and the frequency for probing the paths to the cloud application servers, in Cisco IOS XE Catalyst SD-WAN devices, use the **probe** command in global configuration mode.

The **no** form of this command cancels probing for specific applications.

probe [**latency** *frequency*] [**saas** *application-name*]

no probe [**saas** *application-name*]

Syntax Description

latency *frequency*	Frequency at which Cloud onRamp for SaaS probes the paths to application servers for specified SaaS applications. Range: 0 to 65535 (seconds) Default: 30 **Note** We recommend that you use the default value.

saas *application-name*	Specifies SaaS applications to probe, from a predefined list: amazon_aws_apps box_net_apps concur_apps dropbox_apps google_apps gotomeeting_apps intuit_apps office365_apps oracle_apps salesforce_apps sugar_crm_apps zendesk_apps zoho_crm_apps Prerequisite: To use this option, probe-path configuration must be enabled either as branch or gateway.

Command Mode

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2	The command was introduced.

Examples

Example

```
Device(config)# probe latency 40
Device(config-probe)# top
Device(config)# probe saas office365_apps
Device(config-probe)# top
Device(config)# probe saas amazon_aws_apps
Device(config-probe)# top
Device(config)# show full probe
probe
latency 40
saas office365_apps
saas amazon_aws_apps
!
```

Example

This example cancels probling for office365_apps.

```
Device(config)# no probe saas office365_apps
```

probe-path branch

To enable Cloud onRamp for SaaS functionality in branch mode, for Cisco IOS XE Catalyst SD-WAN devices, use the **probe-path branch** command in global configuration mode.

The **no** form of this command disables Cloud onRamp for SaaS functionality in branch mode.

probe-path branch [**color-all-dia** | **color-list** *list-of-tloc-colors*]

no probe-path branch

Syntax Description

color-all-dia	Enables Cloud onRamp for SaaS probing in branch mode on all transport locator (TLOC) interfaces that have been assigned a valid color. Use this option when all TLOC interfaces have direct internet access (DIA).
color-list *list-of-tloc-colors*	Enables Cloud onRamp for SaaS probing in branch mode on the interfaces that match the list of colors.

Command Mode

Global configuration (config)

Command History

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

Examples

Example

After enabling Cloud onRamp for SaaS for a branch, confirm that it is enabled with a **show** command.

```
Device(config)# show full probe-path
probe-path branch
```

Enable Cloud onRamp for SaaS for a branch, for a list of colors.

```
Device(config)# probe-path branch color-list public-internet private1
Device(config)# show full probe-path
probe-path branch color-list public-internet private1
```

probe-path gateway

To enable Cloud onRamp for SaaS functionality in gateway mode use the **probe-path gateway** command in global configuration mode. To disable Cloud onRamp for SaaS functionality in gateway mode, use the **no** form of this command.

probe-path gateway { **local-interface-list** *list-of-probe-interface-names* | **color-all-dia** | **color-list** *tloc-color-1* [**. . .** *tloc-color-n*] }

no probe-path gateway [**local-interface-list** *list-of-tloc-interface-names* | **color-all-dia** | **color-list** [**. . .** *tloc-color-n*]]

Syntax Description

local-interface-list *list-of-probe-interface-names*	List of probe interface names in service VPNs.
color-all-dia	Enables Cloud onRamp for SaaS to probe all transport locator (TLOC) interfaces that have been assigned a valid color, when the gateway site connects to the internet using VPN 0. Use this option when all TLOC interfaces have direct internet access (DIA).
color-list *tloc-color-1* [*...tloc-color-n*]	Enables Cloud onRamp for SaaS to probe only the DIA interfaces that match a specific list of TLOC colors, when the gateway site connects to the internet using VPN 0.

Command Mode

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	New keywords added: **color-all-dia** and **color-list**

Usage Guidelines

When using the **no** form of this command, you can include **local-interface-list** to specify interfaces, or omit this option to remove the gateway functionality.

Example

After enabling Cloud onRamp for SaaS for a gateway, with a list of interfaces, display the configuration.

```
Device(config)# show full probe-path
probe-path gateway local-interface-list GigabitEthernet5 GigabitEthernet1
```

profile

cellular profile—Configure a cellular profile (on vEdge routers only).

The firmware installed in the router's cellular module is specific to each service provider and determines which profile properties you can configure. You can modify the attributes for a profile only if allowed by the service provider.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Cellular Profile

Command Hierarchy

```
cellular cellularnumber
  profile profile-id
    apn name
    auth auth-method
    ip-addr ip-address
    name profile-name
    pdn-type type
    primary-dns ip-address
    secondary-dns ip-address
    user-name username
    user-pass password
```

Syntax Description

apn *name*	Access Point Name: Name of the gateway between the service provider network and the public Internet. It can be up to 32 characters long.
auth *auth-method*	Authentication Method: Authentication method used for the connection to the cellular network. Possible values are CHAP, None, PAP, or PAP/CHAP.
primary-dns *ip-address* **secondary-dns** *ip-address*	DNS Servers: IP addresses of the primary and secondary DNS servers in the service provider network, in decimal four-part dotted notation.
ip-addr *ip-address*	IP Address: Static IP address assigned to the cellular interface. This field is used when the service provider requires that a static IP address be pre-configured before attaching to the network.
name *profile-name*	Name: Name used to identify the cellular profile. It can be up to 14 characters long.

pdn-type *type*	Packet Data Network Type: Type of packet data network (PDN) of the cellular network. Possible values are IPv4, IPv6 and IPv46.
profile *profile-id*	Profile Identifier: Identification number of the profile used for the cellular module. Range: 0 to 15
user-name *username*	Username: Username to use in making cellular connections for web services. It can be 1 to 32 characters long. It can contain any alphanumeric characters, including spaces. If the username contains spaces, enclose it in quotation marks (" ").
user-pass *password*	User Password: User password to use in making cellular connections for web services. The password is case sensitive. You can enter it in clear text or an AES-encrypted key.

Command History

Release	Modification
16.1	Command introduced.
16.3	Added support for profile 0; changed profile 16 to reserved, so you cannot modify it.

Examples

Configure a cellular interface with a profile, and the profile with an APN.

```
vEdge# show running-config cellular
cellular cellular0
 profile 1
  apn reg_ims
 !
```

Operational Commands

clear cellular errors

clear cellular session statistics

show cellular modem

show cellular network

show cellular profiles

show cellular radio

show cellular sessions

show cellular status

show interface

profile

vpn 0 interface cellular profile—Assign a cellular profile to a cellular interface (on vEdge routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► VPN Interface Cellular

Command Hierarchy

```
vpn 0
  interface cellularnumber
    profile profile-id
```

Syntax Description

profile *profile-id*	Profile: Number that identifies the profile to use for the cellular interface. This profile is one you configure with the **cellular profile** command. *profile-id* can be a value from 1 through 15.

Command History

Release	Modification
16.1	Command introduced.

Examples

```
vEdge# show running-config vpn 0 interface cellular0
vpn 0
 interface cellular0
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color lte
   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
  !
  mtu      1428
  profile  3
  no shutdown
```

```
 !
!
```

Operational Commands

clear cellular errors

clear cellular session statistics

show cellular modem

show cellular network

show cellular profiles

show cellular radio

show cellular sessions

show cellular status

show interface

Related Topics

profile, on page 403

propagate-aspath

vpn router bgp propagate-aspath—Carry the BGP AS path into OMP (on vEdge routers only). Configuring this option can help to avoid network loops.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      propagate-aspath
```

Syntax Description

None

Command History

Release	Modification
17.1	Command introduced.

Examples

Carry local BGP AS path information into OMP, and receive AS path information from OMP:

```
vpn 1
  router
    bgp 1
      propagate-aspath
```

Operational Commands

show bgp summary

show omp routes detail

Related Topics

overlay-as, on page 368

propagate-community

To propagate the BGP communities between routing protocols during route redestribution, use the **propagate-community** command in the global configuration mode.

propagate-community

This command has no arguments or keywords.

Command Default NA

Command Modes Global Configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced on the Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows the propagation of BGP on Cisco IOS XE Catalyst SD-WAN devices:

```
Device(config)# router bgp 123
Device(config)# address-family ipv4 vrf vrf1
Device(config-af)# propagate-community
Device(config-af)# redistribute omp
```

radius

system radius—Configure the properties of a RADIUS server to use for AAA authorization and authentication, and IEEE 802.1X LAN and IEEE 802.11i WLAN authentication.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  radius
    retransmit number
    server ip-address
      acct-port port-number
      auth-port port-number
      priority number
      secret-key password
      source-interface interface-name
      tag tag
      vpn vpn-id
    timeout seconds
```

Command History

acct-port *port-number*	Accounting Port: UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. The accounting information is sent in accounting attribute–value (AV) pairs, as defined in RFC 2866, RADIUS Accounting. By default, vEdge routers send accounting information on UDP port 1813. To disable accounting, set the accounting port number to 0. Range: 0 through 65535 Default: 1813
server *ip-address*	Address of RADIUS Server: IP address of a RADIUS server host in the local network. You can configure up to eight servers. AAA authentication can be performed by up to eight servers. 802.1X and 802.11i authentication can be performed by a maximum of two servers.
secret-key *password*	Authentication Key: Key to use for authentication and encryption between the Cisco vEdge device and the RADIUS server. You can type the key as a text string from 1 to 128 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
auth-port *port-number*	Destination Port for Authentication Requests: UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. If you do not configure a port number, the default is RADIUS authentication port is 1812. Range: 1 through 65535 Default: 1812

source-interface *interface-name*	Interface To Use To Reach Server: Interface on the local device to use to reach the RADIUS server. The source interface must be the same for all RADIUS servers.
retransmit *number*	Location Attempts: How many times to search through the list of RADIUS servers while attempting to locate an operational server. Range: 1 through 1000 Default: 3
priority *number*	Server Priority: Set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers for AAA authentication or between two servers for 802.1X or 802.11i authentication. A server with lower priority number is given priority over one with a higher number. Range: 0 through 7 Default: 0
tag *tag*	Server Tag Identifier: Text string that identifies the RADIUS server. Range: 4 through 16 characters
timeout *seconds*	Time to Wait for Replies from Server: Configure the interval, in seconds, that the Cisco vEdge device waits to receive a reply from the RADIUS server before retransmitting a request. Range: 1 through 1000 Default: 5 seconds
vpn *vpn-id*	VPN where Server Is Located: VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN. Range: 0 through 65530 Default: VPN 0

Syntax Description

Release	Modification
14.1	Command introduced.
14.3	Added **source-interface** command.
15.3.8	Added **secret-key** command and deprecated **key** command.

Release	Modification
16.1	Changed authentication key from 32 to 128 characters.
16.2.2	Added **priority** command.
16.3	Added **acct-port** and **tag** commands, and added support for IEEE 802.1X LAN and IEEE 802.11i WLAN authentication.

Examples

Configure two RADIUS servers:

```
vEdge# show running-config system radius
system
  radius
     server 10.1.15.150
       tag               freerad1
       source-interface ge0/0
       secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
       priority         1
      exit
    server 10.20.24.150
      auth-port        2000
      acct-port        2001
      tag              freerad2
      source-interface ge0/0
      secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
      priority         2
    exit
  !
!
```

Operational Commands

clear dot1x client

dot1x

show dot1x clients

show dot1x interfaces

show dot1x radius

show running-config system radius

show system statistics

Related Topics

aaa, on page 24
admin-auth-order, on page 54
auth-fallback, on page 82
auth-order, on page 85
dot1x, on page 191
tacacs, on page 474
wlan, on page 547

radius-servers

system aaa radius-servers, **vpn interface dot1x radius-servers**, **wlan interface radius-servers**—Configure which RADIUS servers to use for AAA, IEEE 802.1X, and IEEE 802.11i authentication (for IEEE 802.1X and IEEE 802.11i on vEdge routers only).

vManage Feature Template

For all Cisco SD-WAN devices:

Configuration ► Templates ► AAA

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► WiFi SSID (for vEdge cellular wireless routers only)

Command Hierarchy

```
system
  aaa
    radius-servers tag


vpn 0
  interface interface-name
    dot1x
      radius-servers tag


wlan radio-band
  interface vapnumber
    radius-servers tag
```

Syntax Description

tag	Tag Associated with a RADIUS Server: Tag of RADIUS server to use for AAA, IEEE 802.1X, or IEEE 802.11i authentication. The tag can be from 4 through 16 characters long. You can specify one or two tags. You configure the tags with the **system radius server tag** command. If you specify tags for two RADIUS servers, they must both be reachable in the same VPN. If you do not configure a priority value when you configure the RADIUS server with the **system radius server priority** command, the order in which you list the IP addresses is the order in which the RADIUS servers are tried. If you configure no RADIUS server tags, all RADIUS servers in the configuration are used for authentication.

Command History

Release	Modification
16.3	Command introduced.

Examples

Example 1

Configure two RADIUS servers to use for AAA authentication:

```
vEdge# show running-config system
system
...
 aaa
  auth-order     local radius tacacs
  radius-servers radius-1 radius-2
  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
$6$6fmWvCA6jHuEq/AK$y3gixVkyhtvXLWNTiv3Wy21i9/.6h56IQNWvI3YdjxH9qQmGVWVGQW391dlaqjRRDtUkuxeIy3/m9BqL/0IZG.

  !
 !
...
 radius
  server 1.2.3.4
   tag radius-1
  exit
  server 2.3.4.5
   tag radius-2
  exit
 !
```

Example 2

Configure the RADIUS servers to use for 802.1X authentication:

```
system
 radius
  server 10.1.15.150
   tag              freerad1
   source-interface ge0/0
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         1
  exit
  server 10.20.24.150
   auth-port        2000
   acct-port        2001
   tag              freerad2
   source-interface ge0/4
   secret-key       $4$L3rwZmsIic8zj4BgLEFXKw==
   priority         2
  exit
```

```
 !
!
vpn 0
 interface ge0/5
  dot1x
   auth-reject-vlan 40
   auth-fail-vlan   30
   guest-vlan       20
   default-vlan     10
   radius-servers   freerad1
  !
  no shutdown
 !
!
```

Example 3

Configure the RADIUS servers to use for 802.11i authentication:

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid              tb31_pm6_5ghz_vap2
  data-security     wpa/wpa2-personal
  mgmt-security     optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show running-config

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

radius, on page 407

range

vpn router ospf area range—Summarize OSPF routes at an area boundary so that only a single summary route is advertised to other areas by an ABR (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        range prefix/length
          cost number
          no-advertise
```

Syntax Description

prefix/length	Address Range: IP address and subnet mask of the IP addresses to be consolidated and advertised.
cost *number*	Cost for the Summary Routes: Metric for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777215
no-advertise	Do Not Advertise Type 3 Summary LSAs: Do not advertise the Type 3 Summary LSAs.

Command History

Release	Modification
14.1	Command introduced.

Operational Commands

show ospf process

reauthentication

vpn interface dot1x reauthentication—Enable periodic reauthentication of 802.1X clients (on vEdge routers only). By default, clients are authenticated only once, when they first request access to the LAN.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      reauthentication minutes
```

Syntax Description

minutes	Time between Reauthentication Attempts: Set the time between reauthentication attempts. Range: 0 through 1440 minutes Default: 0 (no reauthentication attempts are made after the initial LAN access request)

Command History

Release	Modification
16.3	Command introduced.

Examples

Require a client to reauthenticate once an hour:

```
vpn 0
  interface ge0/8
    dot1x
      requthentication 3600
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

radius, on page 407

redistribute

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the address family configuration mode.

redistribute *protocol* [**metric** { *metric-value* | **transparent** }] [**match** { **internal** | **external 1** | **external 2** }] [**route-map** *map-tag*]
nssa-only

no redistribute *protocol* [**metric** { *metric-value* }] [**route-map** *map-tag*]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **application**, **bgp**, **connected**, **eigrp**, **iso-igrpisis**, **mobile**, **ospf**, **rip**, **ospfv3**, **omp**, **static**, **nat**, **natpool-outside** [**nat-route**]. The **static** [**ip**] keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0.
match {**internal** | **external**}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system. • **nssa-external** —Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes. The default is **internal**.
route-map	(Optional) Specifies the route map that should be interrogated to filter the routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

Command History

Release	Modification
14.1	This command was introduced.
14.2	Added **nat** option.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Added route-map.

Usage Guidelines

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
Device(config)# router bgp 109
Device(config-router)# redistribute ospf
```

The following example shows how to redistribute EIGRP routes into an OSPF domain:

```
Device(config)# router ospf 110
Device(config-router)#  redistribute eigrp
```

The following example shows how to redistribute the specified EIGRP process routes into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Device(config)# router ospf 109
Device(config-router)# redistribute eigrp 108 metric 100 subnets
Device(config-router)# redistribute rip metric 200 subnets
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4
Device(config-router-af)# redistribute bgp 100 metric 100 metric-type 1 subnets route-map
BGP-To_OSPF
```

Related Topics

route-policy, on page 433

redistribute leaked routes

To redistribute routes between the local service VPNs at the same edge site, use the **redistribute** command in the address-family configuration mode or router configuration mode. To stop the redistribution, use the **no** form of this command.

redistribute *protocol* [**route-policy** *policy-name*]

no redistribute *protocol* [**route-policy** *policy-name*]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **omp**, **static**. Due to the fact that leaked routes lose their original attributes and appear as **static**, the redistribution protocol will always be **static**.
route-policy	(Optional) Specifies a route policy to apply to a BGP neighbor or to OSPF.
policy-name	(Optional) Specifies the route policy name. Name of the route policy to configure or apply to a BGP neighbor or to OSPF. Range: 1 to 127 characters.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

The following example shows how routes from service underlay A to service underlay B are redistributed via OSPF:

```
Device(config)# vpn 102
Device(config-vpn-102)# router ospf
Device(config-router)# redistribute static route-policy VPN101_TO_VPN102
```

refresh

vpn interface nat refresh— Configure how NAT mappings are refreshed (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn
  interface interface-name
    nat
      refresh (bi-directional | outbound)
```

Syntax Description

bi-directional	Refresh NAT Mappings for Inbound and Outbound Packets: On the interface, keep the NAT mappings for both outbound and inbound traffic active.
outbound	Refresh NAT Mappings for Outbound Packets Only: On the interface, keep the NAT mappings for outbound traffic active. This is the default behavior.

Command History

Release	Modification
14.2	Command introduced.

Examples

Refresh NAT mappings for outbound and inbound data traffic:

```
vm5# config
vm5(config)# vpn 1 interface ge0/4 nat refresh bi-directional
vm5(config-nat)# show full-configuration
vpn 1
 interface ge0/4
  nat
    bi-directional
  !
 !
!
```

Operational Commands

show ip nat interface

show ip nat interface-statistics

rekey

security ipsec rekey—Modify the IPsec rekeying timer (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Security

Command Hierarchy

```
security
  ipsec
    rekey seconds
```

Syntax Description

seconds	Rekeying Time: How often a vEdge router changes the AES key used on its secure IPsec connection to other vEdge routers. If OMP graceful restart is enabled, the rekeying time must be at least twice the value of the OMP graceful restart timer. This value is equivalent to the security association (SA) lifetime. Range: 10 through 1209600 seconds (14 days) Default: 86400 seconds (24 hours)

Command History

Release	Modification
14.1	Command introduced.
15.3.5	Rekeying time default changed from 7200 seconds (2 hours) and maximum time increased from 2 days to 7 days.

Examples

Change the IPsec rekeying time to 1 week:

```
security
  ipsec
    rekey 604800
```

Operational Commands

show ipsec local-sa

show security-info

Related Topics

graceful-restart, on page 214
request security ipsec-rekey, on page 700
show bfd sessions, on page 748
timers, on page 492

rekey

vpn interface ipsec ike rekey—Modify the IPsec rekeying timer to use during IKE key exchanges (on vEdge routers only).

vpn interface ipsec ipsec rekey—Modify the IPsec rekeying timer to use on an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ike
      rekey seconds
    ipsec
      rekey seconds
```

Syntax Description

seconds	Rekeying Time: How often IKE changes the AES key that is being used during IKE key exchanges. Range: 30 through 1209600 seconds (up to 14 days) Default: 3600 seconds (1 hour) (for **ipsec rekey**); 14400 seconds (4 hours) (for **ike rekey**)

Command History

Release	Modification
17.2	Command introduced.

Examples

Change the rekeying interval for IKE key exchanges to 7 days:

```
vEdge(config)# vpn 1 interface ipsec1 ike rekey-interval 604800
```

Operational Commands

clear ipsec ike sessions

request ipsec ike-rekey request ipsec ipsec-rekey

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

remote-as

vpn router bgp neighbor remote-as—Configure AS number of the remote BGP peer (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
 router
    bgp local-as-number
      neighbor ip-address
        remote-as remote-as-number
```

Syntax Description

remote-as *as-number*	Remote AS Number: AS number of the remote BGP peer.

Release Information

Release	Modification
14.1	Command introduced.

Examples

Set the remote AS number to 456:

```
vpn 1
 router bgp 123
   neighbor 18.72.0.3
     remote-as 456
```

Operational Commands

show bgp neighbor

replay-window

vpn interface ipsec ipsec replay-window—Modify the size of the IPsec replay window on an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsecnumber
    ipsec
      replay-window number
```

Syntax Description

number	Replay Window Size: Size of the sliding replay window. Values: 64,128, 256, 512, 1024, 2048, 4096 packets Default: 512 packets

Command History

Release	Modification
17.2	Command introduced.

Examples

Change the size of the IPsec replay window to 1024 packets:

```
vEdge(config)# vpn 1 interface ipsec1 ipsec
vEdge(ipsec)# replay-window 1024
```

Operational Commands

show ipsec local-sa

show security-info

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

ike, on page 236

replay-window

security ipsec replay-window—Modify the size of the IPsec replay window (on vEdge routers only).

Command Hierarchy

```
security
  ipsec
    replay-window number
```

Syntax Description

number	Replay Window Size: Size of the sliding replay window. Values: 64, 128, 256, 512, 1024, 2048, 4096 packets Default: 512 packets

Release Information

Release	Modification
14.1	Command introduced.

Examples

Change the replay window size to 1024:

```
security
  ipsec
    replay-window 1024
```

Operational Commands

show ipsec local-sa

show security-info

replicator-selection

vpn router pim replicator-selection— Allow vEdge routers to use different replicators for the same multicast group (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      replicator-selection (random | sticky)
```

Syntax Description

(**random** | **sticky**)	How Replicator Is Chosen: Determine how the replicator for a multicast group is chosen: • **random**—Choose the replicatorat random. • **sticky**—Always use the same replicator. This is the default.

Command History

Release	Modification
14.3	Command introduced.

Operational Commands

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show pim interface

show pim neighbor

respond-to-ping

vpn interface nat respond-to-ping—Have a vEdge router that is acting as a NAT device respond to ping requests to the NAT interface's IP address that are received from the public side of the connection (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    nat
      respond-to-ping
```

Syntax Description

None

Command History

Release	Modification
15.4	Command introduced.

Examples

Configure a vEdge router acting as a NAT so that it responds to ping requests from the WAN:

```
vEdge# config
vEdge(config)# vpn 1 interface ge0/4 nat respond-to-ping
vEdge(config-nat)# show full-configuration
vpn 1
 interface ge0/4
  nat
    respond-to-ping
  !
 !
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

retransmit-interval

vpn router ospf area interface retransmit-interval—Set the interval at which the router retransmits OSPF link-state advertisements (LSAs) to its adjacencies (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        interface interface-name
          retransmit-interval seconds
```

Syntax Description

seconds	Retransmit Interval: Time interval at which the OSPF retransmits LSAs to its neighbors. Range: 1 through 65535 seconds Default: 5 seconds

Command History

Release	Modification
14.1	Command introduced.

Examples

Set the LSA retransmission interval to 10 seconds:

```
vEdge# show running-config vpn 1 router ospf area 0
vpn 1
 router
  ospf
   area 0
    interface ge0/0
      retransmit-interval 10
    exit
   exit
  !
 !
!
```

Operational Commands

show ospf interface

rewrite-rule

rewrite-rule—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 (on vEdge routers only). A rewrite rule is applied to packets being transmitted out the interface.

You can apply rewrite rules to both unicast and multicast traffic.

vManage Feature Template

For vEdge routers only:

Configuration ► Policies ► Localized Policy

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

Create a Rewrite Rule

```
policy
  rewrite-rule rule-name
    class class-name loss-priority dscp dscp-value layer-2-cos number
```

Apply a Rewrite Rule on an Interface

```
vpn vpn-id
  interface interface-name
    rewrite-rule rule-name
```

Syntax Description

layer-2-cos *number*	Class-of-Service Value: Number of an 802.1p CoS value to use to mark transit traffic. Range: 0 through 7
dscp *dscp-value*	DSCP Value: Assign a DSCP value to transit traffic. Range: 0 through 63
class *class-name*	Forwarding Class Name: Name of the forwarding class.
loss-prioritye	Loss Priority: Packet loss priority (PLP) for the forwarding class. Values: **high**, **low**
rule-name	Rewrite Rule Name: Name of the QoS map. 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 maximum of 64 entries only per rewrite rule.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added support for multicast traffic.

Release	Modification
18.3	Added support for Layer 2 class of service (CoS).

Examples

Create a rewrite rule, and apply it to an interface:

```
vEdge(config)# show config
rewrite-rule transport
 class af1 low dscp 3
 class af1 high dscp 4
 class af2 low dscp 5
 class af2 high dscp 6
 class af3 low dscp 7
 class af3 high dscp 8
 class be low dscp 1
 class be high dscp 2
 !
!
vpn 0
interface ge0/0
  ip-address 10.1.15.15/24
  tunnel-interface
  no shutdown
  rewrite-rule transport
 !
!
```

Operational Commands

show running-config policy

show running-config vpn

route-consistency-check

system route-consistency-check—Check whether the IPv4 routes in the router's route and forwarding tables are consistent (on vEdge routers only). Performing route consistency checks is useful when you are troubleshooting routing and forwarding problems. However, the checking requires a large amount of device CPU, so it is recommended that you enable it only when you trouble shooting an issue and that you disable it at other times.

By default, route consistency checking is disabled.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  route-consistency-check
```

Syntax Description

None

Command History

Release	Modification
17.1	Command introduced.

Examples

Enable route-consistency checking:

```
vEdge(config)# system route-consistency-check
```

Operational Commands

show ip fib

show ip routes

Related Topics

ip route, on page 267
ipv6 route, on page 275

route-export

To export routes from the transport VPN to service VPNs and vice-versa use the **route-export** command in VPN configuration mode.

route-export { **bgp** | **connected** | **ospf** | **static** } [**route-policy** *policy-name*]

Syntax Description

bgp	Leaks BGP routes into the selected VPN
connected	Leaks connected routes into the selected VPN
ospf	Leaks OSPF routes into the selected VPN
static	Leaks static routes into the selected VPN
route-policy *policy-name*	Filters the leaked routes based on the policy selected

Command History

Release	Modification
Cisco SD-WAN Release 20.3.1	Command introduced.

```
Device# config
Device(config)# vpn 1
Device(config-vpn-1)# route-export bgp route-policy policy-name
```

route-import

To configure route leaking between the transport VPN and service VPNs use the **route-import** command in SD-WAN configuration mode.

route-import { **bgp** | **connected** | **ospf** | **static** } [**route-policy** *policy-name*]

Syntax Description

bgp	Leaks BGP routes into the selected VPN
connected	Leaks connected routes into the selected VPN
ospf	Leaks OSPF routes into the selected VPN
static	Leaks static routes into the selected VPN
route-policy *policy-name*	Filters the leaked routes based on the policy selected

Command History

Release	Modification
Cisco SD-WAN Release 20.3.1	Command introduced.

```
Device# config
Device(config)# vpn 1
Device(config-vpn-1)# route-import bgp route-policy policy-name
```

route-import-service (for route leak)

To enable route leaking between the service VPNs, use the **route-import-service** command in VPN configuration mode. To disable the configurations, use the **no** form of this command.

route-import-service from vpn *vpn-id* { **bgp** | **connected** | **ospf** | **static** } **route-policy** *policy-name*
no route-import-service from vpn *vpn-id* { **bgp** | **connected** | **ospf** | **static** } **route-policy** *policy-name*

Syntax Description

from	The source from which the routes are leaked.
vpn *vpn-id*	Specify the VPN ID from which the routes are imported.
bgp	Leaks BGP routes into the selected VPN.
connected	Leaks connected routes into the selected VPN.

ospf	Leaks OSPF routes into the selected VPN.
static	Leaks static routes into the selected VPN.
route-policy *policy-name*	Filters the leaked routes based on the policy selected.

Command Default

Access for the services shared from the source VPN is disabled.

Command Modes

VPN configuration (config-vpn-vpn-id)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

Usage Guidelines

Route replication creates a link to a route in a routing information base (RIB) that is in a different VPN.

Examples

The following command shows how to enable route leaking on Cisco vEdge devices using the **route-import-service** command:

```
Device(config)# vpn 102
Device(config-vpn-102)# route-import-service from vpn 101 static route-policy VPN101_TO_VPN102
```

route-map

To define the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing, use the **route-map** command in global configuration mode and the **match** and **set** commands in route-map configuration modes.

route-map name *name* [**deny** | **description** | **match** | **ordering-seq** *sequence-number* | **permit** | **set**]

no route-map name *name*

Syntax Description

name	Specifies the name of the route map.
deny	(Optional) Blocks routes matching the route map from being forwarded or redistributed.
description	(Optional) Describes the route-maps that are redistributed.
match	Redistributes routes in the routing table that matches the specified tags.
ordering-seq	(Optional) Orders the route maps based on the string provided.
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.
permit	(Optional) Permits only routes matching the route map to be forwarded or redistributed.
set	(Optional) Sets routes to match the route map from being forwarded or redistributed.

Command Default

Route-map is not enabled and conditions for redistributing routes from one routing protocol into another routing protocol are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was added.

Usage Guidelines

The route maps are used when distributing the routes into the RIP, EIGRP or OSPF routing process. The route map defines which of the routes from a specified routing protocol that are allowed to be redistributed into a target routing process. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** and **set** route-map configuration commands define the conditions for redistributing routes from one routing protocol into another. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map**command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Example

This example shows how to set the autonomous system path to match BGP autonomous system path access list 20:

```
Device(config)# router bgp 10
Device(config)# route-map bgp1
Device(config-route-map)# match as-path 20
```

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into 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.

```
Device(config)# router ospf 109
Device(config-router)# redistribute rip route-map rip-to-ospf
Device(config-router)# exit
Device(config)# route-map rip-to-ospf permit
Device(config-route-map)# match metric 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type1
Device(config-route-map)# set tag 1
```

route-policy

policy route-policy—Configure or apply a localized control policy (on vEdge routers only). For BGP, you apply the policy to an address family running on a specific BGP neighbor. For OSPF, you can apply the policy either to specific types of routes being redistributed into OSPF or to all inbound traffic.

vManage Feature Template

For vEdge routers only:

Configuration ► Policies ► Localized Policy

Configuration ► Templates ► OSPF

Command Hierarchy

Create a Localized Control Policy

```
policy
  route-policy policy-name
    default-action action
    sequence number
      match
        address list-name
        as-path list-name
        community list-name
        ext-community list-name
        local-preference number
        metric number
        next-hop list-name
        omp-tag number
        origin (egp | igp | incomplete)
        ospf-tag number
        peer address
      action
        reject
        accept
          set
            aggregator number
            as-path (exclude | prepend) as-number
            atomic-aggregate
            community value
            local-preference number
            metric number
            metric-type (type1 | type2)
            next-hop ip-address
            omp-tag number
            origin (egp | igp | incomplete)
            originator ip-address
            ospf-tag number
            weight number
```

Apply a Localized Control Policy To BGP

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor address
        address-family ipv4-upcast
          route-policy policy-name (in | out)
```

Apply a Localized Control Policy To OSPF

```
vpn vpn-id
  router
    ospf
      redistribute route-type route-policy policy-name
      route-policy policy-name in
```

Syntax Description

policy-name	Control Policy Name: Name of the localized control policy to configure or apply to a BGP neighbor or to OSPF. *policy-name* can be up to 32 characters long.
in, **out**	Direction To Apply Policy: Apply the policy to routes coming in to the router or being sent out of the router. For BGP, the policy can be applied to incoming or outgoing routes. For OSPF, the policy is apply to routes coming from OSPF neighbors. Use the OSPF redistribute command to apply policy to outgoing routes.

Command History

Release	Modification
14.1	Command introduced.
15.4	Added support for configuring route policy on all OSPF inbound routes (route-policy in).

Operational Commands

show ip routes detail

show running-config

Related Topics

policy, on page 382
redistribute, on page 416

router

Configure the BGP, OSPF, and PIM routing protocol to run in a VPN (on vEdge routers only). You can configure BGP and OSPF routing protocols in all VPNs except for VPN 512, which is the management VPN. You can configure PIM in all VPNs except for VPN 0, which is the transport VPN reserved for the control plane, and VPN 512.

Command Hierarchy

```
vpn vpn-id
  router
    bgp ...
    igmp ...
    multicast-replicator local [threshold number]
    ospf ...
    pim ...
    ...
```

Command History

Release	Modification
14.1	Command introduced.
14.2	PIM and multicast added.
14.3	IGMP added.

Examples

Enable OSPF in VPN 1

```
Device# show running-config vpn 1 router ospf
vpn 1
 router
  ospf
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
    exit
   exit
  !
 !
```

The following example shows the OSPFv3 configuration

```
router ospfv3 1
  !
 address-family ipv4 unicast vrf vrf1
   passive-interface int1
```

Operational Commands

show bgp neighbor

show bgp routes

show bgp summary

show igmp groups

show igmp interface

show igmp statistics

show igmp summary

show ip fib

show ip routes

show multicast replicator

show multicast rpf

show multicast topology

show multicast tunnel

show omp multicast-auto-discover

show omp multicast-routes

show ospf database

show ospf database-summary

show ospf interface

show ospf neighbor

show ospf process

show ospf routes

show pim interface

show pim neighbor

router-id

Configure the OSPF router ID, which is the IP address associated with the router for OSPF adjacencies (on vEdge routers only).

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      router-id ipv4-address
```

Syntax Description

pv4-address	OSPF Router ID: Configure the OSPF router ID as an IPv4 address, in decimal four-part dotted notation. The router ID can be used when electing the OSPF designated router (DR). if there is a tie in the router priority values, the node with the highest router ID becomes the DR or the backup DR. If you have configured a system IP address, that address is used for the OSPF router ID. If you configure a OSPF router ID that differs from the system IP address, the router ID takes precedence.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the router ID for OSPF adjacencies in VPN 1

```
vpn 1
  router
    ospf
      router-id 172.16.255.11
```

Operational Commands

show ospf process

Related Topics

priority, on page 398
system-ip, on page 470

router-id

Configure the BGP router ID, which is the IP address associated with the router for BGP sessions (on vEdge routers only).

vManage Feature Template

For all vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      router-id ip-address
```

Syntax Description

router-id *ip-address*	BGP Router ID: Configure the BGP router ID as an IPv4 address, in decimal four-part dotted notation. If you have configured a system IP address, that address is used for the BGP router ID. If you configure a BGP router ID that differs from the system IP address, the router ID takes precedence.).

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the router ID for BGP sessions in VPN 1

```
vpn 1
  router
    bgp 123
      router-id 75.0.0.1
```

Operational Commands

show bgp summary

Related Topics

system-ip, on page 470

secret

To configure the secret key for Umbrella registration, on Cisco IOS XE Catalyst SD-WAN devices, use the **secret** command.

secret 0 *secret*

Syntax Description

secret	Secret key (hexadecimal).

Command Mode

config-profile

Command History

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

Examples

Use **parameter-map type umbrella global** to enter config-profile mode, then use **orgid**, **api-key**, and **secret** to configure Umbrella registration.

In config-profile mode, you can use **show full-configuration** to display Umbrella registration details.

Example

This example configures Umbrella registration details.

```
Device(config)# parameter-map type umbrella global
Device(config-profile)# orgid 1234567
Device(config-profile)# api-key aaa12345aaa12345aaa12345aaa12345
Device(config-profile)# secret 0 bbb12345bbb12345bbb12345bbb12345
```

security

To configure security parameters on routers, Cisco vManage, and Cisco vSmart Controllers, use the use the **security** command in global configuration mode.

security

Syntax Description

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.

Examples

The following example shows how to configure the security for a router.

```
Router(config)# security
```

send-community

Send the local router's BGP community attribute to the BGP neighbor (on vEdge routers only).

This feature is disabled by default. If you have configured it, use the **no send-community** command to return to the default.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        send-community
```

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the local vEdge router to send the BGP community attribute to its BGP neighbor

```
vEdge# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
  bgp 123
   neighbor 1.10.10.10
    no shutdown
    remote-as 456
    send-community
    !
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

send-ext-community

Send the local router's BGP extended community attribute to the BGP neighbor (on vEdge routers only). This feature is disabled by default. If you enable it, use the **no send-ext-community** configuration command to disable it.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        send-ext-community
```

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the local vEdge router to send the BGP extended community attribute to its BGP neighbor

```
vm1# show running-config vpn 1 router bgp neighbor 1.10.10.10
vpn 1
 router
bgp 123
   neighbor 1.10.10.10
    no shutdown
    remote-as 456
    send-ext-community
    !
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

send-path-limit

Configure the maximum number of equal-cost routes that are advertised per prefix (on vSmart controllers and vEdge routers only).

Command Hierarchy

```
omp
  send-path-limit number
```

Syntax Description

send-path-limit *number*	Number of Routes: Maximum number of equal-cost routes that a Cisco vEdge device advertises to a Cisco SD-WAN Controller or that a Cisco SD-WAN Controller redistributes to Cisco vEdge devices. More exactly, a route is a route–TLOC tuple. (Each TLOC consists of an IP address, color, and encap type.) Each Cisco vEdge device can have up to four WAN interfaces and hence can advertise up four route–TLOC tuples for each route. 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. Default: 4

Command History

Release	Modification
14.2	Command introduced.
15.2	Maximum number of routes increased to 16.
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.

Operational Commands

show omp routes

sense level

To specify the alert level for port-scanning detection, use the **sense level** command in United Threat Defense (UTD) multitenancy threat configuration mode or UTD single-tenancy threat configuration mode.

sense level { **low** | **medium** | **high** }

no sense level

Syntax Description

low	Generates alerts only on error packets sent from the target host. Because of the nature of error responses, the **low** alert level should see very few false positives. When the sense level is **low**, the metadata is valid for a short span after which it is reset. Network Mapper (Nmap) has an option for running slow port scans that can take longer to execute. If the sense level is **low**, slower Nmap scans may not be detected.
medium	Tracks connection counts and generates filtered scan alerts. The **medium** alert level may generate false positives on active hosts (Network Address Translation [NATs], proxies, and Domain Name System [DNS] caches).
high	Tracks hosts on a network using a time window to evaluate port-scanning statistics for that host. A **high** setting can identify some of the slow scans because of continuous monitoring, but is sensitive to active hosts. **Note** When the sense level is set to **high**, false positives may be generated.

Command Default

If you do not configure the **sense level** command, or you use the **no** form of the command, sense level is configured as **low** by default.

Command Modes

UTD multitenancy threat configuration mode (utd-mt-threat)

UTD single-tenancy threat configuration mode (utd-eng-std)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This command was introduced.

Usage Guidelines

Port-scanning detection must be enabled prior to specifying the alert level.

For more information on enabling port-scanning detection, see the port-scan command.

Examples

The following examples show how to set the different port-scanning alert levels in UTD multi-tenancy threat configuration mode:

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-mt-threat)# port-scan
Device(config-utd-threat-port-scan)# sense level low
```

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-mt-threat)# port-scan
Device(config-utd-threat-port-scan)# sense level medium
```

```
Device(config)# utd engine standard multi-tenancy
Device(config-utd-mt-threat)# port-scan
Device(config-utd-threat-port-scan)# sense level high
```

The following examples show how to set the different port-scanning alert levels in UTD single-tenancy threat configuration mode:

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# port-scan
Device(config-utd-threat-port-scan)# sense level low
```

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# port-scan
Device(config-utd-threat-port-scan)# sense level medium
```

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# port-scan
Device(config-utd-threat-port-scan)# sense level high
```

The following is sample alert output:

```
2019/10/21-16:22:36.299733 UTC [**] [Hostname: 192.0.2.1] [**]
[Instance_ID: 2] [**] Alert [**] [116:401:1] snort_decoder:
WARNING: Nmap XMAS Attack Detected [**] [Classification: Attempted
Information Leak] [Priority: 2] [VRF: 3]
{TCP} 198.51.100.9:33108 -> 203.0.113:2008
```

```
2019/10/07-18:04:15.926169 UTC [**] [Hostname: 192.0.2.5] [**]
[Instance_ID: 1] [**] Alert [**] [116:423:2] snort_decoder:
WARNING: TCP has no SYN, ACK, or RST [**] [Classification: Misc activity]
[Priority: 3] [VRF: global] {TCP} 192.0.2.5:47519 -> 192.0.2.240:35533
```

service

Configure a service, such as a firewall or IDS, that is present on the local network in which the router is located. Configuring a service allows it to be used in a service chaining policy. You can configure services in all VPNs except for VPN 0, which is the transport VPN reserved for the control plane.

vManage Feature Template

Configuration ► Templates ► VPN

Command Hierarchy

For Cisco vEdge devices:

```
vpn vpn-id
  service service-name address ip-address
vpn vpn-id
  service service-name interface gre number1 [gre number2]
```

For Cisco IOS XE Catalyst SD-WAN devices:

```
sdwan
  service service-name vrf vrf-id
  [[no] track-enable]
  ipv4 address ip-address [ip-address]...
```

Syntax Description

service-name	Type of Service Type of service available at the local site and in the VPN. Standard services are firewall, IDS, and IDP. Four custom services are available. *Values:*FW, IDP, IDS, netsvc1, netsvc2, netsvc3, netsvc4, TE
address *ip-address* interfacegre **number1** [gre **number2**]	Location of Service IP address of the the service device, or GRE interface through which the service is reachable. You can specify up to four IP address. The service is advertised to the vSmart controller only if the address (or one of the addresses) can be resolved locally, at the local site, and not via routes learned through OMP. When configuring a GRE tunnel, specify the names of one or two GRE interfaces. If you configure two, the first interface is the primary GRE tunnel, and the second is the backup tunnel. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary GRE tunnel.

[**no**] **track-enable**	(optional) Cisco Catalyst SD-WAN tests each service device periodically to check whether it is operational. Tracking saves the results of the periodic tests in a service log. On a Cisco IOS XE Catalyst SD-WAN device, this can be viewed using **debug platform software sdwan tracker**. On a Cisco vEdge device, **debug transport event level high** enables tracking the debug logs and copies the logs to the debug file. You can view this file using the **show log** *filename* command. Tracking is enabled by default. Including **no track-enable** disables tracking. After disabling tracking, you can use **track-enable** to re-enable tracking.
ipv4 address *ip-address*	Specify one or more IPv4 addresses of the service device, separated by spaces. Minimum: 1 address per service Maximum: 4 addresses per service

Command History

Release	Modification
14.1	Command introduced.
14.2	Configured IP address of the service resolved locally.
15.4.1	Support for GRE interfaces added.
17.2.0	Support for traffic engineering (TE) service added.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco SD-WAN Release 20.3.1	Added support for Cisco IOS XE Catalyst SD-WAN devices. Added **track-enable** keyword to enable tracking the status of a devices that provide services used in a service chaining policy.

Usage Guidelines

Configuration using the service command makes a service device available to a device managed by Cisco Catalyst SD-WAN. A control policy is required to send traffic to the service device. For information about configuring control policies to direct traffic to service devices, see the Policies configuration guide.

The workflow is:

1. Configure a service device to provide a network service, such as a firewall. The service device can be a Cisco or non-Cisco device, and does not have to be managed by Cisco Catalyst SD-WAN.
2. On a device managed by Cisco Catalyst SD-WAN, configure access to the service device.
3. On the device managed by Cisco Catalyst SD-WAN, apply a traffic policy that routes specific traffic to the service device.

Examples

Configure a firewall service that is available in VPN 1

```
vpn 1
  service FW address 10.0.2.11
```

Configuring Firewall Service Insertion for a Cisco vEdge Device

The following example configures a Cisco vEdge device to use a firewall service on a device in VPN 10. The device operating the firewall service has the address 10.0.2.1. In this example, tracking the service device status is enabled by default. The example shows the configuration, followed by the **show running-config vpn** output.

```
vEdge(config)# vpn 10
vEdge(config-vpn-1)# service FW address 10.0.2.1
vEdge(config-service-FW)#commit

vEdge# show running-config vpn 10
vpn 10
  service FW
     address 10.0.2.1
```

Use **no track-enable** to disable tracking.

```
vEdge(config)# vpn 10
vEdge(config-vpn-1)# service FW
vEdge(config-service-FW)# no track-enable

vEdge# show running-config vpn 10
vpn 10
  service FW
     no track-enable
     address 10.0.2.1
```

Configuring Firewall Service Insertion for a Cisco IOS XE Catalyst SD-WAN Device

The following example configures a Cisco IOS XE Catalyst SD-WAN device to use a firewall service on a device in VRF 10. The device operating the firewall service has two addresses: 10.0.2.1 and 10.0.2.2. Tracking is enabled by default. The example shows the configuration, followed by the **show sdwan running-config sdwan** output.

```
ISR4451(config)# sdwan
ISR4451(config-sdwan)# service firewall vrf 10
ISR4451(config-vrf-10)# ipv4 address 10.0.2.1 10.0.2.2
ISR4451(config-vrf-10)# commit

ISR4451# show sdwan running-config sdwan
sdwan
 service firewall vrf 10
  ipv4 address 10.0.2.1 10.0.2.2
```

Use **no track-enable** to disable tracking.

```
ISR4451(config-sdwan)# no track-enable

ISR4451# show sdwan running-config sdwan
sdwan
```

```
service firewall vrf 10
 no track-enable
 ipv4 address 10.0.2.1 10.0.2.2
```

Related Commands

show omp services

show tunnel gre-keepalives

Related Topics

allow-service, on page 63
tunnel-destination, on page 511
tunnel-source, on page 515

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
  !
```

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
```

shaping-rate

Configure the aggregate traffic rate on an interface to be less than line rate so that the interface transmits less traffic than it is capable of transmitting (on vEdge routers only). The interface cannot be a VLAN interface (subinterface).

Shaping rate below 2M is not supported on the following Cisco vEdge devices: Cisco vEdge100b, Cisco vEdge100m, Cisco vEdge 1000, and Cisco vEdge 2000.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    shaping-rate kbps
```

Syntax Description

kbps	Traffic Shaping Rate: Rate at which to transmit traffic, in kilobits per second (kbps). *Range:* 0 through the maximum interface speed

Command History

Release	Modification
14.1	Command introduced.
17.1	Starting with this release, you can no longer configure **shaping-rate** on a VLAN interface

Examples

Limit the maximum amount of traffic that an interface can transmit

```
vEdge# show running-config vpn 0 interface ge0/0
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
   color lte
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
  !
  no shutdown
  shaping-rate 100000
 !
!
```

Operational Commands

show running-config vpn

shutdown

Disable a parameter or property. The **no** form of the command enables a parameter or property.

vManage Feature Template

For all vEdge devices:

Instances of the **shutdown** and **no shutdown**command appear in multiple configuration templates.

Command Hierarchy

Instances of the **shutdown** and **no shutdown** command appear throughout the configuration command hierarchy on vEdge devices.

Command History

Release	Modification
14.1	Command introduced.

Examples

This example enables four interfaces and VPN 0 by including the no shutdown command in the configuration

```
vEdge# show running-config vpn 0
vpn 0
 interface ge0/0
  ip address 10.1.16.16/24
  tunnel-interface
   color lte
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
  !
  no shutdown
 !
 interface ge0/1
  ip address 10.1.18.16/24
  no shutdown
 !
 interface ge0/2
  shutdown
 !
 interface ge0/3
  ip address 10.0.21.16/24
  no shutdown
 !
 interface ge0/7
  ip address 10.0.100.16/24
  no shutdown
 !
 ip route 0.0.0.0/0 10.1.16.13
!
```

The IF OPER STATUS column in the show interface command output reports that **ge0/0**, **ge0/1**, **ge0/3**, and **ge0/7** are operational, as per our configuration, and **ge0/2** is down:

```
vEdge# show interface vpn 0
                                    IF      IF

                                    ADMIN   OPER    ENCAP
   SPEED                         RX       TX
VPN  INTERFACE  IP ADDRESS        STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
   MBPS   DUPLEX  UPTIME      PACKETS  PACKETS
```

```
0    ge0/0      10.1.16.16/24     Up      Up      null   transport  1500  00:0c:29:d7:63:18
  10     full    0:00:20:03  7506     7646
0    ge0/1      10.1.18.16/24     Up      Up      null   service    1500  00:0c:29:d7:63:22
  10     full    0:00:20:03  2        4
0    ge0/2      -                 Down    Down    null   service    1500  00:0c:29:d7:63:2c
  -      -       -           2        2
0    ge0/3      10.0.21.16/24     Up      Up      null   service    1500  00:0c:29:d7:63:36
  10     full    0:00:20:03  24       28
0    ge0/7      10.0.100.16/24    Up      Up      null   service    1500  00:0c:29:d7:63:5e
  10     full    0:00:27:46  1117     857
0    system     172.16.255.16/32  Up      Up      null   loopback   1500  00:00:00:00:00:00
  10     full    0:00:19:40  0        0
```

Operational Commands

The **show** commands for the various device functionalities indicate whether that functionality is operationally up (that is, enabled) or operationally down (that is, disabled).

site-id

Configure the identifier of the site in the Cisco SD-WAN overlay network, such as a branch, campus, or data center, in which the device resides (for vEdge routers, vManage NMSs, and vSmart controllers).

vManage Feature Template

For all vEdge device:

Configuration ► Templates ► System

Command Hierarchy

```
system
  site-id site-id
```

Syntax Description

site-id	Site Identifier: Numeric identifier of the site in the Cisco SD-WAN overlay network. The site ID must be the same for all Cisco vEdge devices that reside in the same site. *Range:* 0 through 4294967295 ($2^{32} – 1$)

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the site ID to be 50

```
Cisco SD-WAN# show running-config system
system
  system-ip 1.1.1.9
  domain-id 1
  site-id   50
  vbond 10.0.4.12
!
```

Operational Commands

show control local-properties

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 Catalyst SD-WAN devices and four SLA classes for Cisco vEdge devices.

sla-class *sla-class-name* **jitter** *jitter* **latency** *latency* **loss** *percentage* **app-probe-class** *app-probe-class-name*

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:* 0 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 percent
app-probe-class *app-probe-class-name*	Specifies the app-probe-class configured on the SLA class.

Command Default

There are no default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
14.2	Command introduced.
16.2	**jitter** option added.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Support for upto eight SLA classes added. In previous releases, you can only configure upto four SLA classes. However, only four unique SLA classes can be defined in an App-Route policy or attached to a site.
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	A app-probe-class keyword is added.

The following example shows the SLA configuration for a latency of 50 milliseconds and app-probe-class:

```
Device(config)# policy
Device(config)# sla-class 50ms-sla
Device(config)# latency 50
Device(config)# app-probe-class real-time-video
Device(config)# fallback-best-tunnel
Device(config)# criteria loss jitter
```

snmp

Configure the Simple Network Management Protocol. The Cisco SD-WAN software supports SNMPv2 and SNMPv3 simultaneously. By default, SNMP is disabled.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  community name
    authorization (read-only | read-write)
    view string
  contact string
  group group-name authentication
    view string
  location string
  name string
  [no] shutdown
  trap
    group group-name
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name group-name
```

```
    source-interface interface-name
user username
  auth authentication
  auth-password password
  group group-name
  priv privacy
  priv-password password
view string
  oid oid-subtree [exclude]
```

Command History

Release	Modification
14.1	Command introduced.
15.2	Support for SNMP traps added.
16.2	Support for SNMPv3 traps added.

Operational Commands

show running-config snmp

sp-organization-name

Configure the name of your service provider for a vBond orchestrator or vSmart controller that is part of a software multitenant architecture (on vBond orchestrators and vSmart controllers).

Command Hierarchy

```
system
  sp-organization-name name
```

Syntax Description

name	Service Provider Organization Name: Configure 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 vEdge network devices.

Command History

Release	Modification
17.1	Command introduced.

Examples

Configure an service provider organization name

```
vSmart(config)# system sp-organization-name "My Phone Company Inc"
```

Operational Commands

show control local-properties

show orchestrator local-properties

Related Topics

request csr upload, on page 664

speed

Set the speed of the interface. Configure the interface speed, for use when the remote end of the connection does not support autonegotiation.

On all vEdge router models, all interfaces support 1-Gigabit Ethernet SFPs. These SFPs can either be copper or fiber. For fiber 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, you must disable autonegotiation and then use the **speed** and **duplex** commands to set the appropriate interface link characteristics.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    speed speed
```

Syntax Description

speed	Interface Speed: Interface speed, in Mbps. Values: 10, 100 Default: Autonegotiate (10/100/1000 Mbps) on vEdge 1000 routers

Command History

Release	Modification
14.1	Command introduced.
15.3	Support for autonegotiation added

Examples

Set the interface speed to 100 Mbps

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 0 interface ge0/0
vEdge(config-interface-ge0/0)# no autonegotiate
vEdge(config-interface-ge0/0)# speed 100
```

Operational Commands

show interface

Related Topics

autonegotiate, on page 96
duplex, on page 195

spt-threshold

Configure when a PIM router should join the shortest-path source tree (SPT) (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► PIM

Command Hierarchy

```
vpn vpn-id
  router
    pim
      spt-threshold kbps
```

Syntax Description

kbps	Traffic Rate: Traffic rate at which the router should join the shortest-path source tree. Until that rate occurs, traffic remains on the shared tree, and travels through the RP. By default, a vEdge router joins the SPT immediately after the first packet arrives from a new source. Range: 0 to 100 kbps Default: 0

Command History

Release	Modification
14.3	Command introduced.

Operational Commands

show multicastreplicator

show multicast rpf

show multicast topology

show multicast tunnel

show omp multicast-auto-discover

show omp multicast-routes

show pim interface

show pim neighbor

show pim rp-mapping

ssid

Configure the service set identifier (SSID) for a WLAN (on vEdge cellular wireless routers only). You can configure up to four SSIDs.

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.

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  interface vapnumber
    ssid ssid
```

Syntax Description

ssid	WLAN SSID: SSID for the WLAN. Range: A string from 4 through 32 characters. The SSID for each virtual access point within a single radio frequency must be unique.

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure four SSIDs

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

static

Configure static NAT address mappings (on vEdge routers only).

In service VPNs (VPNs except VPN 0 and VPN 512, configure static NAT address mappings on a vEdge router that is acting as a NAT device. Across all NAT pools, a vEdge router can NAT a maximum of 254 source IP addresses. This is the number of addresses in a /24 prefix, less the .0 and .255 addresses. You cannot configure translation for .0 and .255 addresses.

In the transport VPN (VPN 0), configure static NAT address mappings to a pool of NAT addresses. You can configure as many static address mappings as there are IP address in the configured NAT pool. If you configure no static mappings, NAT address mapping is performed dynamically.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

In service VPNs:

```
vpn vpn-id
  interface natpool number
    nat
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
```

In the transport VPN:

```
vpn 0
  interface ge slot | port
    nat
      static source-ip ip-address1 translate-ip ip-address2 source-vpn vpn-id protocol (tcp
 | udp) source-port number translate
```

Syntax Description

Table 10: In Service VPNs

(**inside** | **outside**)	Direction To Perform Network Address Translation: Direction in which to perform network address translation. It can be one of the following: **inside**: Translate the IP address of packets that are coming from the service side of the vEdge router and that are destined to transport side of the router. For translation of inside source IP addresses to occur, the translation direction, configured with the **direction** command, must be **inside**. **direction inside** is the default, so you can omit this command from the configuration. **outside**: Translate the IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined to a service-side device. For translation of outside source IP addresses to occur, the translation direction, configured with the **direction** command, must be **outside**.
source-ip *ip-address1*	Source IP Address: Private source IP address to be NATed. This is the IP address of a device or branch router on the service side of the vEdge router.
translate-ip *ip-address2*	Translate IP Address: Public IP address to map the private source address to. This is the IP address that the vEdge router places in the source field of the packet's IP header when transmitting the packet over a transport network.

Table 11: In the Transport VPN

(**tcp** | **udp**)	Protocol: Protocol being used to transmit the traffic flow.
source-ip *ip-address1*	Source IP Address: Private source IP address to be NATed. This is the IP address of a device or branch router on the service side of the vEdge router.
source-port *number*	Source Port Number: Number of the source port. *Range:* 1 through 65535
source-vpn vpn-id	Source VPN: Service VPN from which the traffic flow is being sent.
translate-ip *ip-address2*	Translated IP Address: Public IP address to map the private source address to. This IP address must be contained in the pool of NAT addresses that you configure with the **natpool** command.

translate-port *number*	Translated Port Number: Number to translate the port number to. *Range:* 1 through 65535

Command History

Release	Modification
16.3	Command introduced.
18.3	Support for static NAT address mappings in VPN 0 added.

Examples

Configure a vEdge router to NAT a service-side and a remote IP address

```
vEdge# show running-config vpn 1
interface natpool1
  ip address 10.15.1.4/30
  nat
    static source-ip 10.1.17.3 translate-ip 10.15.1.4 inside
    static source-ip 10.20.25.18 translate-ip 10.25.1.1 outside
    direction inside
    no overload
  !
  no shutdown
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

Related Topics

encapsulation, on page 202
direction, on page 183
natpool, on page 349
overload, on page 369

static-ingress-qos

Allocate ingress traffic on an interface to a specific queue (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    static-ingress-qos number
```

Syntax Description

number	Queue Number: Queue number to use for incoming traffic. Range: 0 through 7

Command History

Release	Modification
15.3	Command introduced.

Examples

Have incoming traffic on interface ge0/0 use queue 1

```
vEdge(config-interface-ge0/1)# static-ingress-qos 1
```

Operational Commands

show running-config vpn

static-lease

Assign a static IP address to a client device on the service-side network (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► DHCP Server

Command Hierarchy

```
vpn vpn-id
  interface ge number | subinterface
    dhcp-server
      static-lease mac-address ip ip-address host-name hostname
```

Syntax Description

host-name *hostname*	Hostname of Client: Hostname of client device.
mac-address	Network Client: MAC address of client to which static IP address is being assigned.
ip *ip-address*	Static IP Address: Static IP address to assign to the client.

Command History

Release	Modification
14.3	Command introduced.

Examples

Assign a static IP address to a device in the service-side network

```
vm5# config
Entering configuration mode terminal
vm5(config)# vpn 1 interface ge0/4
vm5(config-interface-ge0/4)# dhcp-server address-pool 10.0.100.0/24
vm5(config-dhcp-server)# static-lease b8:e8:56:38:5e:89 ip 10.0.100.23
vm5(config-dhcp-server)# show full-configuration
vpn 1
 interface ge0/4
  dhcp-server
   address-pool 10.0.100.0/24
   static-lease b8:e8:56:38:5e:89 ip 10.0.100.23
  !
 !
!
```

Operational Commands

show dhcp interfaces

show dhcp server

stub

Configure an OSPF stub area (on vEdge routers only). A stub area is an area that OSPF does not flood AS external link-state advertisements (Type 5 LSAs).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      area number
        stub
          no-summary
```

Syntax Description

no-summary	Summary Routes: Do not inject OSPF summary routes into the stub area.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure area 2 as a stub area

```
vedge(config)# vpn 1 router ospf area 2 stub
```

Operational Commands

show ospf neighbor detail

system

Configure system-wide parameters.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  aaa
    admin-auth-order (local | radius | tacacs)
    auth-fallback
    auth-order (local | radius | tacacs)
    logs
      audit-disable
      netconf-disable
```

```
  radius-servers tag
  user username
    group group-name
    password password
  usergroup group-name
    task (interface | policy | routing | security | system) (read | write)
admin-tech-on-failure
allow-same-site-tunnels
archive
  interval minutes
  path file-path/filename
  ssh-id-file file-path/filename
  vpn vpn-id
clock
  timezone timezone
console-baud-rate rate
control-session-pps rate
description text
device-groups group-name
domain-id domain-id
eco-friendly-mode (on vEdge Cloud routers only)
gps-location (latitude decimal-degrees | longitude decimal-degrees)
host-name string
host-policer-pps rate
icmp-error-pps rate
idle-timeout minutes
iptables-enable
location string
logging
  disk
    enable
    file
      name filename
      rotate number
      size megabytes
    priority priority
  host
    name (name | ip-address)
    port udp-port-number
    priority priority
    rate-limit number interval seconds
multicast-buffer-percent percentage
ntp
  keys
    authentication key-id md5 md5-key
    trusted key-id
  server (dns-server-address | ip-address)
    key key-id
    prefer
    source-interface interface-name
    version number
    vpn vpn-id
on-demand [enable | disable]
on-demand idle-timeout minutes
organization-name string
port-hop
port-offset number
radius
  retransmit number
  server ip-address
    auth-port port-number
    priority number
    secret-key key
    source-interface interface-name
```

```
    tag tag
    vpn vpn-id
  timeout seconds
route-consistency-check (on vEdge routers only)
site-id site-id
sp-organization-name name (on vBond orchestrators and vSmart controllers only)
system-ip ip-address
system-tunnel-mtu bytes
tacacs
  authentication authentication-type
  server ip-address
    auth-port port-number
    priority number
    secret-key key
    source-interface interface-name
    vpn vpn-id
  timeout seconds
tcp-optimization-enabled (on vEdge routers only)
timer
  dns-cache-timeout minutes
track-default-gateway
track-interface-tag number
track-transport
tracker tracker-name
  endpoint-dns-name dns-name
  endpoint-ip ip-address
  interval seconds
  multiplier number
  threshold milliseconds
upgrade-confirm minutes
[no] usb-controller (on vEdge 1000 and vEdge 2000 routers only)
vbond (dns-name | ip-address [local] [port number] [ztp-server]
```

Command History

Release	Modification
14.1	Command introduced.
Cisco SD-WAN Release 20.3.1	Added **on-demand** and **on-demand idle-timeout** to enable and configure dynamic on-demand tunnels.
Cisco SD-WAN Release 20.4.1	Added **vrrp-advt-with-phymac** to enable the interface to send a duplicate VRRP multicast advertisement with an L2 source, as a physical MAC adddress.

Examples

Configure basic system parameters on a vEdge router

```
vEdge# show running-config system
system
 host-name         vEdge
 system-ip         172.16.255.14
 domain-id         1
 site-id           400
 port-offset       4
 organization-name "Cisco Inc"
 clock timezone America/Los_Angeles
 vbond 10.1.14.14 local
```

```
 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 $1$ZDmsKZbc$oVs.oZxEZPDAVLrBLJCR9.
  !
 !
 logging
  disk
   enable
  !
 !
 vrrp-advt-with-phymac
!
```

Operational Commands

show aaa usergroup

show control local-properties

show logging

show ntp associations

show ntp peer

show orchestrator local-properties

show running-config system

show system status

show uptime

show users

system-ip

Configure a system IP address for a vEdge device.

The system IP address is a persistent IP address that identifies the Cisco vEdge device. It is 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 device's loopback address in the transport VPN (VPN 0). (Note that this is not the same as a loopback address that you configure for an interface.)

On a vEdge 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 is different from the system IP address, the router ID takes precedence.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  system-ip ipv4-address
```

Syntax Description

ipv4-address	System IP Address: System IP address. Specify it as an IPv4 address in decimal four-part dotted notation. Specify just the address; 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, and 224.0.0.0/4, and 240.0.0.0/4 and later. Each device in the overlay network must have a unique system IP address. You cannot use this same address for another interface in VPN 0.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the system IP address and verify its configuration

```
vEdge# show running-config system
system
 host-name          vm1
 system-ip          172.16.255.11
 domain-id          1
 site-id            100
...
!
vEdge# show interface vpn 0 | tab
                                      IF      IF

                                      ADMIN   OPER    ENCAP
   SPEED                         RX       TX
VPN  INTERFACE  IP ADDRESS          STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
   MBPS   DUPLEX  UPTIME       PACKETS  PACKETS
-------------------------------------------------------------------------------------------
0    ge0/1      10.0.26.11/24     Up      Up      null   service    1500  00:0c:29:ab:b7:62
  10     full    0:00:46:41  82       28
0    ge0/2      10.0.5.11/24      Up      Up      null   transport  1500  00:0c:29:ab:b7:6c
  10     full    0:00:46:41  19399    19368
0    ge0/3      -                 Down    Down    null   service    1500  00:0c:29:ab:b7:76
  -      -       -           0        2
0    ge0/4      -                 Down    Down    null   service    1500  00:0c:29:ab:b7:80
  -      -       -           0        2
0    ge0/5      -                 Down    Down    null   service    1500  00:0c:29:ab:b7:8a
  -      -       -           0        2
```

```
0    ge0/6      -                Down    Down    null   service    1500  00:0c:29:ab:b7:94
  -      -        -           0        2
0    ge0/7      10.0.100.11/24   Up      Up      null   service    1500  00:0c:29:ab:b7:9e
  10     full     0:00:54:34  1198     871
0    system     172.16.255.11/32 Up      Up      null   loopback   1500  00:00:00:00:00:00
  10     full     0:00:46:17  0        0
```

Operational Commands

show control local-properties

show interface vpn 0

Related Topics

ip address, on page 259
router-id, on page 438
router-id, on page 437

system-tunnel-mtu

Configure the MTU to use on the tunnels that send OMP control traffic between Cisco vEdge devices. These tunnels are internal tunnels used by the devices to exchange control traffic. This MTU value is not related to, and has no effect on, interface MTUs.

Generally, you never need to modify the system tunnel MTU. The only case when you might consider configuring this parameter is when you are adjusting the TCP MSS value.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  system-tunnel-mtu mtu
```

Syntax Description

mtu	MTU: MTU size to use on tunnels that carry OMP control traffic. *Range:* 500 through 2000 bytes *Default:* 1024 bytes

Command History

Release	Modification
14.1	Command introduced.

Examples

Explicitly configure the system tunnel MTU to the default value of 1000 bytes

```
vEdge(config-system)# system-tunnel-mtu 1000
```

Operational Commands

show running-config system

Related Topics

tcp-mss-adjust, on page 477

system patch-confirm

To configure a time limit to verify that a software patch was successful, use the **system patch-confirm** command in configuration mode.

system patch-confirm *minutes*

patch-confirm *minutes*	Time To Wait for Confirmation: If a software patch fails, this command specifies the amount of time the device waits for you to run `request support software patch-confirm` command. If you do not run this command, the device reverrts to the previous software image . Range: 5 through 60 minutes

Command Default

No default.

Command Modes

configuration (config)

Release	Modification
17.4	This command was introduced.

Usage Guidelines

When this option is enabled, after you patch a device, you must run this command to confirm the patch. If you do not run this command, the device automatically reverts to the previous softwarer image. For example, after you patch the device using the `request support software patch` command, you must log in to the device after it reboots. Then you must run the `request support software patch-confirm` within the time limit that you specfied.

If the control connections fail to come up when this option is enabled, the devices can still revert to the previous image. By default, this option is disabled.

Examples

The following example sets the time limit to 7 minutes:

```
Device(config)# system patch-confirm 7
```

table-map

To configure the policy for filtering and modifying the Open Shortest Path First version3 (OSPFv3) routes before installing them in to the Routing Information Base (RIB), use the **table-map** command in the router configuration mode. To disable this function, use the **no** form of this command.

table-map *route-map-name* [**filter**]

Syntax Description

route-map-name	Name of the table map. The *route-map-name* is 1 to 63 alphanumeric characters. For OSPFv3, the *route-map-name* argument specifies the name of a route map to be used for route attribute modification and filtering.
filter	(Optional) Filters routes based on the configuration of the specified route map. An OSPFv3 route is not installed in the RIB if it is denied in the route-map configuration.

Command Default

No route-map is configured as a table-map and all OSPFv3 routes are installed without modification or filtering.

Command Modes

Router configuration mode

Command History

Release	Modification
Cisco IOS XE Release 17.3.2	This command was introduced on Cisco IOS XE SD-WAN devices.

Usage Guidelines

A **table-map** can be used to modify and filter routes that are installed in the RIB. To filter routes that are explicitly or implicitly denied by the route-map, use the filter keyword. Before using this command, you must configure the required route-map in global configuration mode. A route-map can be used to modify the metric, tag, and omp-tag of OSPFv3 routes installed into the RIB.

The following example shows a route-map configuration for blocking the next hops that are learned through VRF:

```
Device(config)# router ospfv3 1
Device(config)# address-family ipv4 vrf vrf1
Device(config-af)# redistribute omp route-map match-omp-tag
Device(config-af)# table-map set-omp-tag
Device(config-af)# exit-address-family
```

tacacs

Configure the properties of a TACACS+ server that is used in conjunction with AAA to authorize and authenticate users who attempt to access Cisco vEdge devices.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  tacacs
    authentication password-authentication
    server ip-address
      auth-port port-number
      priority number
      secret-key password
      source-interface interface-name
      vpn vpn-id
    timeout seconds
```

Syntax Description

server *ip-address*	Address of TACACS+ Server: Address of TACACS+ Server IP address of a TACACS+ server host in the local network. You can configure up to 8 TACACS+ servers.
secret-key *password*	Authentication Key: **secret-key** *password* Key to use for authentication and encryption between the Cisco vEdge device and the TACACS+ server. You type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the encryption key used on the TACACS+ server.
auth-port *port-number*	Destination Port for Authentication Requests: UDP destination port to use for authentication requests to the TACACS server. If the server is not used for authentication, configure the port number to be 0. If you do not configure a port number, the default is TACACS+ authentication port is 49.
source-interface *interface-name*	Interface To Use To Reach Server: Interface on the local device to use to reach the TACACS+ server.
authentication *authentication-type*	Password Authentication: Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII.
priority *number*	Server Priority: Set the priority of a TACACS+ server, as a means of choosing or load balancing among multiple TACACS+ servers. A server with lower priority number is given priority over one with a higher number. *Range:* 0 through 7 *Default:* 0

timeout *seconds*	Time to Wait for Replies from Server: Configure the interval, in seconds, that the Cisco vEdge device waits to receive a reply from the TACACS+ server before retransmitting a request. *Range:* 1 through 1000 *Default:* 5 seconds
vpn *vpn-id*	VPN where Server Is Located: VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN. *Range:* 0 through 65530 *Default:* VPN 0

Command History

Release	Modification
14.2	Command introduced.
14.3	**source-interface** command added.
15.3.8	**secret-key** and deprecate **key** commands added.
16.2.2	**authentication** and **priority** commands added.

Examples

Configure TACACS+

```
vEdge(config)# system tacacs
vEdge(config-tacacs)# server 1.2.3.4 secret-key $4$aCGzJg5k6M8zj4BgLEFXKw==
vEdge(config-server-1.2.3.4)# exit
vEdge(config-tacacs)# exit
vEdge(config-system)# aaa auth-order local tacacs
vEdge(config-aaa)# exit
vm5(config-system)# show configuration
system
 aaa
  auth-order local tacacs
 !
 tacacs
  server 1.2.3.4
   secret-key $4$aCGzJg5k6M8zj4BgLEFXKw==
   vpn 1
  exit
 !
!
```

Operational Commands

show running-config system tacacs

Related Topics

aaa, on page 24
admin-auth-order, on page 54
auth-fallback, on page 82
auth-order, on page 85
radius, on page 407

tcp-mss-adjust

Configure the maximum segment size (MSS) of TCP SYN packets passing through a device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. For data sent over an interface, the MSS is calculated by adding the interface maximum transmission unit (MTU), the IP header length, and the maximum TCP header length. For data sent over a tunnel, the MSS is the sum of the tunnel MTU, the IP header length, and the maximum TCP header length.

The resulting TCP MSS ADJUST will be always a value 84 bytes lower than the MTU, or less. The reason for this is that the MSS value is derived as:

MSS = MTU – (TCP header with maximum options) – (IP header) – (MPLS header)

MSS = MTU – (60) – (20) – (4)

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    tcp-mss-adjust bytes
```

Syntax Description

bytes	Change the Packet Size: TCP maximum segment size (MSS), which is the largest amount of data that the interface can receive in a single IP datagram, excluding the TCP and IP headers. Range: 552 to 1960 bytes; for PPP interface, 552 to 1452 bytes Default: None

Command History

Release	Modification
14.1	Command introduced.
15.3	TCP SYN MSS dynamically adjusted based on the interface or tunnel MTU.
16.3	Maximum TCP MSS changed from 1460 bytes to 1960 bytes.

Examples

Set the TCP MSS

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 0 interface ge0/1
vEdge(config-interface-ge0/1)# tcp-mss-adjust 1400
vm5(config-interface-ge0/1)# commit and-quit
Commit complete.
vEdge# show interface

                                  IF      IF
                  TCP
                                  ADMIN   OPER    ENCAP
   SPEED          MSS                RX       TX
VPN  INTERFACE  IP ADDRESS        STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
   MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------
0    ge0/0      10.1.15.15/24     Up      Up      null   transport  1500  00:0c:29:7d:1e:fe
  10     full    1420    0:04:12:25  202419   218746
0    ge0/1      10.1.17.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:08
  10     full    1400    0:04:04:10  448      5
0    ge0/2      -                 Down    Up      null   service    1500  00:0c:29:7d:1e:12
  10     full    1420    0:04:12:33  448      0
0    ge0/3      10.0.20.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:1c
  10     full    1420    0:04:04:10  453      5
0    ge0/6      57.0.1.15/24      Up      Up      null   service    1500  00:0c:29:7d:1e:3a
  10     full    1420    0:04:04:10  448      4
0    ge0/7      10.0.100.15/24    Up      Up      null   service    1500  00:0c:29:7d:1e:44
  10     full    1420    0:04:10:19  1044     594
0    system     172.16.255.15/32  Up      Up      null   loopback   1500  00:00:00:00:00:00
  10     full    1420    0:04:03:49  0        0
1    ge0/4      10.20.24.15/24    Up      Up      null   service    1500  00:0c:29:7d:1e:26
  10     full    1420    0:04:04:07  2009     1603
1    ge0/5      56.0.1.15/24      Up      Up      null   service    1500  00:0c:29:7d:1e:30
  10     full    1420    0:04:04:07  448      4
512  eth0       10.0.1.15/24      Up      Up      null   service    1500  00:50:56:00:01:0f
  1000   full    0       0:04:12:18  7581     4581
```

Operational Commands

show interface

Related Topics

system-tunnel-mtu, on page 472

tcp-optimization

Fine-tune TCP to decrease round-trip latency and improve throughput for TCP traffic (on vEdge routers only). You can configure TCP optimization in service-side VPNs only (VPNs other than VPN 0 and VPN 512).

Optimizing TCP traffic can be useful for improving the performance of SaaS applications, transcontinental links, and high-latency transport devices such as VSAT satellite communications systems.

By default, TCP optimization is disabled.

To configure TCP optimization for individual traffic flows rather than across a VPN, create a centralized data policy that includes the **tcp-opt** action.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  tcp-optimization
```

Command History

Release	Modification
17.2	Command introduced.

Examples

Optimize TCP traffic in VPN 1

```
vEdge# show running-config vpn 1
vpn 1
  tcp-optimization
```

Operational Commands

show app tcp-opt

Related Topics

tcp-optimization-enabled, on page 479

tcp-optimization-enabled

Enabled TCP optimization (on vEdge routers only).

On vEdge 1000 and vEdge 2000 routers, enabling TCP optimization carves out a separate CPU core to use for the optimization, because TCP optimization is CPU intensive.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  tcp-optimization-enabled
```

Command History

Release	Modification
17.2	Command introduced.

Examples

Enable TCP optimization on a vEdge router

```
vEdge# show running-config system
...
tcp-optimization-enabled
...
```

Operational Commands

show app tcp-opt

Related Topics

tcp-optimization, on page 479

tcp-syn-flood-limit

Configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection (on vEdge routers only).

Command Hierarchy

```
policy
tcp-syn-flood-limit number
```

Syntax Description

number	Number of TCP SYN Packets: Number of TCP SYN packets to allow before terminating an attempt to establish a TCP connection. *Range:* 1 through 2147483647 *Default:* 2000

Command History

Release	Modification
18.3	Command introduced.

Examples

For a zone-based firewall, change the number of TCP SYN packets that the router can receive from the default of 2000 to 2200

```
vEdge# show running-config policy
policy
  tcp-syn-flood-limit 2200
  zone A
    vpn 1
  !
  zone B
    vpn 2
    vpn 3
    vpn 4
  !
  zone-to-nozone-internet allow
  zone-pair zbfw-pair-1
    source-zone A
    destination-zone B
    zone-policy zbfw-policy-1
  !
  zone-based-policy zbfw-policy-1
    sequence 1
      match
        protocol 6
      !
      action inspect
      !
    !
    default-action drop
  !
!
```

Operational Commands

show policy zbfw global-statistics

Related Topics

vpn-membership, on page 541
zone, on page 550

tcp-timeout

Configure when NAT translations over a TCP session time out (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    nat
     tcp-timeout minutes
```

Syntax Description

minutes	Time: Time after which NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

Command History

Release	Modification
14.2	Command introduced.

Examples

Change the NAT translation timeout value for TCP sessions to 2 hours

```
vEdge# config
vEdge(config)# vpn 1 interface ge0/4 nat tcp-timeout 120
vEdge(config-nat)# show full-configuration
vpn 1
 interface ge0/4
  nat
    tcp-timeout 120
  !
 !
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

technology

Associate a radio access technology (RAT) with a cellular interface (on vEdge routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► VPN Interface Cellular

Command Hierarchy

```
vpn 0
  interface cellular number
    technology technology
```

Syntax Description

technology	Cellular Technology: Define the RAT for a cellular interface on vEdge routers that support 4G LTE and CDMA-based 2G/3G networks (such as Sprint and Verizon networks). It can be one of the following: **auto**: Automatically select the RAT. Use this value for a **cellular0** interface when you are using this interface for ZTP. **cdma**: Use 2G/3G CDMA cellular technology. **lte**: Use 4G LTE cellular technology. This is the default.

Command History

Release	Modification
16.2.10 and 16.3.2	Command introduced.

Examples

Configure a cellular interface to automatically choose its radio access technology

```
vEdge# show running-config vpn 0 interface cellular0
vpn 0
 interface cellular0
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color lte
   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
  !
  mtu      1428
  profile  0
  technology auto
  no shutdown
 !
!
```

Operational Commands

clear cellular errors

clear cellular session statistics

show cellular modem

show cellular network

show cellular profiles

show cellular radio

show cellular sessions

show cellular status

show interface

Related Topics

profile, on page 403

template-refresh

How often to send the cflowd template record fields to the collector (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  cflowd-template template-name
    template-refresh seconds
```

Syntax Description

seconds	Refresh Time: How often to send the cflowd template record fields to the collector. If you configure this time and later modify it, the changes take effect only on flows that are created after the configuration change has been propagated to the vEdge router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the **clear app cflowd flows** command. Range: 60 through 86400 seconds (1 minute through 1 day) Default: 90 seconds

Command History

Release	Modification
14.3	Command introduced.

Examples

Configure a cflowd template

```
vSmart# show running-config policy
cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.14 port 11233
 flow-active-timeout 60
 flow-inactive-timeout 90
 template-refresh 86400
!
```

Operational Commands

clear app cflowd flows (on vEdge routers only)

clear app cflowd statistics (on vEdge routers only)

show policy from-vsmart (on vEdge routers only)

show running-config policy (on vSmart controllers only)

show app cflowd collector (on vEdge routers only)

show app cflowd template (on vEdge routers only)

timeout inactivity

Set how long to wait before revoking the authentication of an client that is using 802.1X to access a network (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      timeout
        inactivity minutes
```

Syntax Description

seconds	Client Inactivity Timeout: Time to wait before revoking the authentication of an inactive 802.1X client. Range: 0 through 1440 minutes (24 hours) Default: 60 minutes (1 hour)

Command History

Release	Modification
16.3	Command introduced.

Examples

Revoke a client's authentication after 2 hours

```
vpn 0
  interface ge0/7
    dot1x
      timeout
        activity 7200
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

radius, on page 407

timer

Configure the DNS cache timeout value.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  timer
    dns-cache-timeout minutes
```

Syntax Description

dns-cache-timeout *minutes*	Timeout for vBond DNS Cache: When to time out the vBond orchestrator addresses that have been cached by the local device. Range: 1 through 30 minutes Default: 2 minutes

Command History

Release	Modification
15.2	Command introduced.
15.4.4	Default timeout changed from 30 minutes to 2 minutes.

Examples

Change the DNS cache timeout to 15 minutes

```
vEdge(config)# system timer dns-cache-timeout 15
vEdge(config)# commit and-quit
vEdge# show local control-properties
vm1# show control local-properties
organization-name            Cisco Inc
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Not Applicable
certificate-not-valid-before Not Applicable
certificate-not-valid-after  Not Applicable

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     0
system-ip                    172.16.255.11
chassis-num/unique-id        b9a28025-5954-456b-9028-9d74d3ed4e2a
serial-num                   NOT-A-HARDWARE
keygen-interval              1:00:00:00
register-interval            0:00:00:30
retry-interval               0:00:00:17
```

```
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:15:00
port-hopped                  TRUE
time-since-last-port-hop     0:02:44:55
number-vbond-peers           0
number-active-wan-interfaces 1
...
```

Operational Commands

clear dns cache

show control local-properties

Related Topics

vbond, on page 529

tracker-dns-cache-timeout

To configure the the duration for which Cisco vEdge devices cache SIG endpoint IP addresses obtained through DNS query resolution of SIG endpoint FQDNs, use the **timer tracker-dns-cache-timeout** command on Cisco vManage in the system configuration mode. To remove the configuration and revert to default behavior, use the **no** form of the command.

timer tracker-dns-cache-timeout *duration*

Syntax Description

duration	Specifies the the duration (in minutes) for which WAN edge devices cache resolved SIG endpoint IP addresses. Range: 5 to 1440 minutes Default: 120 minutes

Command Default

120 minutes (2 hours)

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco vManage Release 20.9.1	This command is introduced.

Examples

The following example shows a sample configuration which defines the cache timeout as 15 minutes:

```
config
 system
  timer tracker-dns-cache-timeout 15
```

timers

Configure OSPF timers (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► OSPF

Command Hierarchy

```
vpn vpn-id
  router
    ospf
      timers
        spf delay initial-hold-time maximum-hold-time
```

Syntax Description

spf *delay initial-hold-time maximum-hold-time*	SPF Algorithm Timer: Configure the amount of time between when OSPF detects a topology and when it runs its SPF algorithm. This timer consists of three parts: Delay: Delay from first change received until performing the SPF calculation. Range: 0 through 600000 milliseconds (60 seconds). Default: 200 milliseconds. Initial hold time: Initial hold time between consecutive SPF calculations. Range: 0 through 600000 milliseconds (60 seconds). Default: 1000 milliseconds. Maximum hold time: Longest time between consecutive SPF calculations. Range: 0 through 600000 milliseconds (60 seconds). Default: 10000 milliseconds.

Command History

Release	Modification
14.1	Command introduced.

Examples

Set the OSPF SPF timers

```
vEdge# show running-config vpn 1 router ospf
vpn 1
 router
  ospf
   timers spf 300 1200 15000
   redistribute static
   redistribute omp
   max-metric router-lsa administrative
   area 0
    interface ge0/0
```

```
    exit
   exit
  !
 !
!
vEdge# show ospf process | include time
 spf-holdtime          1200
 spf-max-holdtime      15000
 spf-last-exec-time    2607
```

Operational Commands

show ospf process

timers

Configure global and per-neighbor BGP timers (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      timers
        holdtime seconds
        keepalive seconds
        vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        timers
          advertisement-interval seconds
          connect-retry seconds
          holdtime seconds
          keepalive seconds
```

Syntax Description

advertisement-interval *seconds*	Advertisement Interval: For a BGP neighbor, set the minimum route advertisement interval (MRAI) between when BGP routing update packets are sent to that neighbor. Range: 0 through 600 seconds Default: 5 seconds for IBGP route advertisements; 30 seconds for EBGP route advertisements

connect-retry *seconds*	Connection Retry Time: For a BGP neighbor, set the amount of time between retries to establish a connection to a configured peer that has gone down. Range: 0 through 65535 seconds Default: 30 seconds
holdtime *seconds*	Hold Time: Set the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Provisioning the hold time for a specific neighbor overrides the global default or the hold time configured at the global level. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive timer)
keepalive *seconds*	Keepalive Time: Frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Provisioning the keepalive time for a specific neighbor overrides the global default or the keepalive configured at the global level. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)

Command History

Release	Modification
14.1	Command introduced.

Examples

Modify the connection retry time and the advertisement interval for a BGP neighbor

```
vEdge# show running-config vpn 1 router bgp neighbor 10.20.25.18
vpn 1
 router
bgp 1
  neighbor 10.20.25.18
     no shutdown
     remote-as 2
     timers
       connect-retry          60
      !
     password  $4$L3rwZmsIiZB6wtBgLEFXKw==
   !
  !
```

```
 !
!
```

Operational Commands

show bgp neighbor detail

timers

Configure OMP timers on vEdge routers and vSmart controllers.

When you change an OMP timer on a device, the BFD sessions on that device go down and then come back up.

vManage Feature Template

For vEdge routers and vSmart controllers only:

Configuration ► Templates ► OMP

Command Hierarchy

```
omp
  timers
    advertisement-interval seconds
    eor-timer seconds
    graceful-restart-timer seconds
    holdtime seconds
```

Syntax Description

eor-timer *seconds*	End-of-RIB Timer: 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 were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1 through 3600 seconds (1 hour) Default: 300 seconds (5 minutes)
graceful-restart-timer *seconds*	Graceful Restart Timer: 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 will wait for the timer configured on Cisco vSmart to expire before removing the stale routes from the OMP table and Cisco vSmart will wait for the timer configured on WAN Edge. Range: 1 through 604800 seconds (168 hours, or 7 days) Default: 43200 seconds (12 hours)

holdtime *seconds*	Holdtime Interval: How long to wait before closing the OMP connection to a peer. If the peer does not 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 is not 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 through 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: Configure the amount of time between OMP Update packets. Range: 0 through 65535 seconds Default: 1 second We recommended you to configure 5 seconds on edge devices and 20 seconds on vSmart.

Command History

Release	Modification
14.1	Command introduced.
14.2	Removed keepalive option; changed default hold-time interval from 15 to 60 seconds; added **graceful-restart-timer** command.
15.3	Changed maximum graceful restart timer value to 12 hours.
15.3.5	Change default graceful restart timer value to 12 hours, and changed maximum graceful restart timer value to 7 days.
16.2	Added **eor-timer** command

Examples

Modify the default OMP timers

```
vEdge(config-timers)# show config
omp
 timers
  holdtime               20
  advertisement-interval 2
 !
!
```

Operational Commands

show omp summary

Related Topics

graceful-restart, on page 214

rekey, on page 419

tloc-extension

Bind this interface, which connects to another vEdge router at the same physical site, to the local router's WAN transport interface (on vEdge routers only). Note that you can configure the two routers themselves with different site identifiers.

You cannot configure TLOC extensions on cellular (LTE) interfaces.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn 0
  interface interface-name
    tloc-extension interface-name
```

Syntax Description

interface-name	Local Router's WAN Transport Interface: 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 History

Release	Modification
15.4	Command introduced.

Examples

In this example, vEdge2 has two circuits, one to the Internet and the second to an MPLS network. vEdge1 is also located at the same site, but has no circuits. This configuration binds two subinterfaces from vEdge1 to the two circuit interfaces on vEdge2 so that vEdge1 can establish TLOCs on the overlay network.

```
vEdge1# show running-config vpn 0
interface ge0/2.101
  ip address 101.1.19.15/24
  mtu 1496
  tunnel-interface
    color red
  !
  no shutdown
!
interface ge0/2.102
  ip address 102.1.19.15/24
  mtu 1496
  tunnel-interface
    color blue
  !
  no shutdown
!

vEdge2# show running-config vpn 0
interface ge0/0
  ip address 172.16.255.2
  tunnel-interface
    color red
  !
  no shutdown
!
interface ge0/3
  ip address 172.16.255.16
  tunnel-interface
    color blue
  !
  no shutdown
!
interface ge0/2.101
  ip address 101.1.19.16/24
  mtu 1496
  tloc-extension ge0/0
  no shutdown
!
interface ge0/2.102
  ip address 102.1.19.16/24
  mtu 1496
  tloc-extension ge0/3
  no shutdown
!
```

Operational Commands

show bfd sessions

show control connections

show interface

show omp tlocs

Related Topics

allow-same-site-tunnels, on page 61

tloc-extension-gre-from

Configure an interface as an extended interface, to channel TLOC traffic from a source branch router to the local WAN interface (on IOS XE routers only).

vManage Feature Template

For Cisco IOS XE routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
sdwan
  interface interface-name
    tloc-extension-gre-from extended-wan-interface-ip-address xconnect wan-interface-name
```

Syntax Description

wan-interface-name	Interface Name: Name of WAN interface that you are using for sending traffic over the extended TLOC.
extended-wan-interface-ip-address	IP Address of GRE Tunnel Destination: IP address of the destination of the GRE tunnel that is being used as the TLOC interface. GRE tunnel destination IP address of the TLOC interface. This is the interface in the branch router that you are using to extend the TLOC.

Command History

Release	Modification
16.9.1	Command introduced.

Examples

Bind two subinterfaces from Router 1 to two circuit interfaces on Router 2 so that Router 1 can establish TLOC connections in the overlay network. Router 2 has two circuits, one to the Internet and the second to an MPLS network. Router 1 is also located at the same site, but has no circuits and is on a different L3 network.

```
ISRK2# show sdwan running-config
sdwan
 interface GigabitEthernet0/2.101
  encapsulation dot1q 101
  ip address 30.1.19.16/24
   mtu 1496
!
interface GigabitEthernet0/2.102
  encapsulation dot1q 102
  ip address 40.1.19.16/24
   mtu 1496
!
sdwan
 interface GigabitEthernet0/0
  ip address 172.16.255.2
  tunnel-interface
    color lte
  !
 interface GigabitEthernet0/2.101
  tloc-extension-gre-from 10.1.19.15 xconnect GigabitEthernet0/0
 !
 interface GigabitEthernet0/2.102
  tloc-extension-gre-from 20.1.19.15 xconnect GigabitEthernet0/3
 !
 interface GigabitEthernet0/3
  ip address 172.16.255.16
  tunnel-interface
    color mpls
  !
 !
!
```

Operational Commands

show sdwan bfd sessions

show sdwan control connections

show sdwan control local-properties

show sdwan interface

show sdwan omp tlocs

Related Topics

tloc-extension-gre-to, on page 497

tloc-extension-gre-to

Configure a tunnel interface over which to run TLOC extensions (on IOS XE routers only). TLOC extensions allow you to extend a TLOC, over a GRE tunnel, to another router in the branch.

vManage Feature Template

For Cisco IOS XE routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
sdwan
  interface interface-name
    tunnel-interface
      tloc-extension-gre-to extended-interface-ip-address
```

Syntax Description

extended-interface-ip-address	IP Address of GRE Tunnel Destination: GRE tunnel destination IP address of the interface that you are extended to another router in the branch.

Command History

Release	Modification
16.9.1	Command introduced.

Examples

Create a GRE tunnel from Router 1 to Router 2 over an L3 network. Router 2 has two circuits, one to the Internet and the second to an MPLS network. Router 1 is located at the same site, but has no circuits and is on a different L3 network.

```
Device# show sdwan running-config
sdwan
 interface GigabitEthernet0/2.101
  no shutdown
  encapsulation dot1 101
  ip address 10.1.19.15/24
  mtu 1496
 !
 interface GigabitEthernet0/2.102
  no shutdown
  encapsulation dot1 102
  ip address 20.1.19.15/24
  mtu 1496
 !
 interface Tunnel1
  no shutdown
  ip unnumbered GigabitEthernet0/2.101
  tunnel source GigabitEthernet0/2.101
  tunnel mode sdwan
 !
 interface Tunnel2
  no shutdown
  ip unnumbered GigabitEthernet0/2.102
  tunnel source GigabitEthernet0/2.102
  tunnel mode sdwan
 !
sdwan
```

```
 interface GigabitEthernet0/2.101
  tunnel-interface
   color lte
   tloc-extension-gre-to 30.1.19.16
 !
 interface GigabitEthernet0/2.102
  tunnel-interface
   color mpls
   tloc-extension-gre-to 40.1.19.16
 !
!
```

Operational Commands

show sdwan bfd sessions

show sdwan control connections

show sdwan control local-properties

show sdwan interface

show sdwan omp tlocs

Related Topics

tloc-extension-gre-from, on page 496

track

To configure interface or SIG container list tracking <as a single entity>, use the **track** command in vrrp configuration mode. To remove the tracking for this list, use the **no** form of this command.

track *track-list-name* [**decrement** *priority*]

Syntax Description

track-list-name	Interface or container list name
decrement	Decrement value for list priority

Command Default

?

Command Modes

vrrp configuration (config-vrrp)

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure a track list for interfaces.

```
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 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
```

Table 12: Related Commands

Command	Description
vrrp	Configures the VRRP to allow multiple routers to share a common virtual IP address for default gateway redundancy.
track	To configure object tracking on a VRRP object list
show vrrp	Displays information about the configured VRRP interfaces and groups.

track-default-gateway

For a static route, determine whether the next hop is reachable before adding that route to the device's route table. By default, this function is enabled.

With gateway tracking enabled, the software sends ARP messages every 10 seconds to the next hop of a static route. If the software receives an ARP response, it places the static route into the local route table. After 10 consecutive ARP responses are missed, the 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 response, the static route is added back to the route table.

Note The internal threshold timeout value for receiving an ARP response is 1000 milliseconds. If an ARP response is not received by the internal threshold value, the tracker is marked as down.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  track-default-gateway
```

Command History

Release	Modification
15.3.5	Command introduced.
15.4	Number of retries changed from 3 to 10.

Examples

Have the device determine whether the next hop for a static route is reachable before placing the static route in the local route table:

```
system
  track-default-gateway
```

Operational Commands

show ip routes

Related Topics

ip route, on page 267

track-interface-tag

Configure a tag to apply to routes associated with a network that is connected to a non-operational interface (on vEdge routers only). Specifically, the tagging occurs only when a vEdge router has been unable to reset a port that has stopped transmitting packets but whose status remains Up. This error is reported by the "PCS issue detected" alarm.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  track-interface-tag number
```

Syntax Description

number	Tag: Set the tag string to include in routes associated with a network that is connected to a non-operational interface. Range: 1 through 4294967295

Command History

Release	Modification
15.3.8 and 15.4.3	Command introduced.

Examples

On a vEdge router, set a tag for tracking a non-operational interface, and on a vSmart controller create a policy to send data traffic on an alternate path around the interface

```
vEdge# show running-config system
system
  track-interface-tag 555
  ...
vSmart# show running-config policy
policy
 control-policy pcs-policy
  sequence 10
   match route
    omp-tag 555
   !
   action accept
    set
     preference 5
    !
   !
  !
  default-action accept
 !
!
```

Operational Commands

show running-config system

Related Topics

track-interface-tag, on page 501

track-list

To configure object tracking on a VRRP object list, use the **track-list** command in system configuration mode. To remove the object tracking for this object list, use the **no** form of this command.

track-list *list-name* [**interface** *interface-type-number* [*...interface-type-number*] | **sig-container global**]
no track-list *list-name*

Syntax Description

interface *interface-type-number*	Sets a list of one or more interfaces that should be tracked for up/down events
sig-container global	Sets a list of SIG containers that should be tracked for up/down events

Command Default

No VRRP tracking is enabled

Command Modes

System configuration (config-system)

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure a track list for interfaces.

```
Device# config terminal
Device(config)# system
Device(config-system)# track-list zs1 interface ge0/1 gre1 ipsec1

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 SIG container.

```
Device# config terminal
Device(config)# system
Device(config-system)# track-list SIG-1 sig-container global

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
```

Table 13: Related Commands

Command	Description
vrrp	Configures the VRRP to allow multiple routers to share a common virtual IP address for default gateway redundancy.
track	Tracks interface or container lists
show vrrp	Displays information about the configured VRRP interfaces and groups.

track-transport

Checks whether the routed path between the local device and a vBond orchestrator is up using ICMP probes at regular interval of 3s. By default, transport checking is enabled.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

```
system
  [no] track-transport
```

Command History

Release	Modification
14.1	Command introduced.

Examples

Explicitly configure regular monitoring of the DTLS connection to the vBond orchestrator.

```
vEdge(config-system)# track-transport
vedge(config-system)# commit and-quit
Commit complete.
vEdge# show transport connection
TRACK
TYPE    SOURCE  DESTINATION     HOST            INDEX  TIME                      STATE
-------------------------------------------------------------------------------------
system     -    2001:cdba::1:2  system12.vbond  0      Wed May 10 10:27:29 2017  up
system     -    2001:cdba::1:3  system12.vbond  0      Wed May 10 10:29:01 2017  up
                                                1      Wed May 10 10:27:30 2017  down
```

Operational Commands

show transport connection

tracker

Track the status of transport interfaces that connect to the internet.

Tracker uses HTTP. If you are using an endpoint that does not respond to HTTP, then the tracker will remain in a down state. You need the response to be 200 OK for an up state.

Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet.

When you enable transport tunnel tracking, the software periodically probes the path to the internet to determine whether it is up. If the software detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When the software detects that the path to the internet is again functioning, the route to the internet is reinstalled.

The Enable Layer 7 Health Check feature helps in maintaining tunnel health by providing tunnels the ability to failover. Tracker module with **endpoint-api-url** is used for L7 Health check in the routers. The Direct Internet Access (DIA) traffic ingressing on SD-WAN service VPNs is tunnelled to the Secure Internet Gateways (SIG) for securing enterprise traffic. All LAN/WIFI enabled enterprise client's traffic, based on routing, is forwarded to the SIG.

vManage Feature Template

Configuration ► Templates ► System

Configuration ► Templates ► VPN Interface Cellular (for cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
system
  tracker tracker-name
    endpoint-dns-name dns-name
    endpoint-ip ip-address
    endpoint-api-url api-url
    interval seconds
    multiplier number
    threshold milliseconds

vpn 0
  interface interface-name
    tracker tracker-name
```

Syntax Description

endpoint-dns-name *dns-name*	DNS Name of Interface End Point: DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address or URL.
endpoint-ip *ip-address*	IP Address of Interface End Point: IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address or URL.
endpoint-api-url *api-url*	DNS API URL of tunnel interface Internet security endpoint. This is the destination in the internet to which the router sends probes to determine the status of the transport tunnel interface. For each tracker, you must configure either one DNS name or one IP address or URL.
interval *seconds*	Interval between Status Probes. The frequency to determine the status of the transport interface. **Note** The tracker takes additional time (0 - interval) to go down than the configured time (interval multiplies with the multiplier) as probe can happen after the network issue. For example, when the interval is 30 seconds, multiplier is 3, tracker goes down after [30*3 + (0-30)] seconds loss in the network. Range: 10 through 600 seconds Default: 60 seconds (1 minute)
multiplier *number*	Number of Retries Number of times to probes are resent before declaring that the transport interface is down. Range: 1 through 10 Default: 3
threshold *milliseconds*	Time To Wait for Response The elapse time for the probe to return a response before declaring that the transport interface is down. Range: 100 through 1000 milliseconds Default: 300 milliseconds
tracker-name	Tracker Name Name of the tracker. tracker-name can be up to 128 lowercase letters. You can configure up to eight trackers. You can apply only one tracker to an interface.

Command History

Release	Modification
17.2.2	Command introduced.
19.3	Command modified. **endpoint-api-url** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Support added for Cisco IOS XE Catalyst SD-WAN devices.

Usage Guidelines

The **endpoint-api-url** keyword is supported on IPSec and GRE interfaces. However, **endpoint-ip** and **endpoint-dns** are not supported on IPSec/GRE interfaces.

The **endpoint-api-url** is used directly on tunnel interface. NAT is not required for tunnels in the Transport side.

Examples

Enable transport tracking on a NAT interface.

```
system
  tracker nat-tracker
    endpoint-ip 10.2.3.4
  vpn 0
  interface ge0/1
    nat
    tracker nat-tracker
```

Enable transport tracking on GRE interface.

```
system
 tracker gre-tracker
  endpoint-api-url http://gateway.zscalerbeta.net/vpntest
 !
 interface gre1
   tracker gre-tracker

!
```

Related Topics

nat, on page 346

trap group

Configure SNMP trap groups.

For each trap generated by a vEdge device, the device also generates a notification message. Use the show notification stream command to display these messages.

For SNMPv3, the PDU type for notifications ie either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  trap
    group group-name
      trap-type
        level severity
```

Syntax Description

group *group-name*	Group Name: Name of the trap group. It can be from 1 to 32 characters.
level *severity*	Severity Level: Severity level of the trap. Severity can be **critical**, **major**, or **minor**. You can specify one, two, or three severity levels for each trap type.
trap-type	Trap Type: Type of traps to include in the trap group. **trap-group** can be one of the following: all—All trap types. app-route—Traps generated by application-aware routing. bfd—Traps generated by BFD and BFD sessions. bridge—Traps generated by bridging sessions. control—Traps generated by DTLS and TLS sessions. dhcp—Traps generated by DHCP. hardware—Traps generated by Cisco vEdge hardware. omp—Traps generated by OMP. policy—Traps generated by control and data policy. routing—Traps generated by BGP, OSPF, and PIM. security—Trap generated by certificates, vSmart and vEdge serial number files, and IPSec. system—Traps generated by functions configured under the system vpn—Traps generated by VPN-specific functions, including interfaces and VRRP. wwan—Traps generated by WLAN interfaces.

Command History

Release	Modification
15.2	Command introduced.

Examples

Configure trap groups and associate them with SNMP trap servers.

```
vEdge(config-snmp)# show full-configuration
snmp
 view snmp-view
 !
 community public
  view          snmp-view
  authorization read-only
 !
 trap target 0 10.0.0.1 162
  group-name     all-traps
  community-name public
 !
 trap target 0 10.0.0.2 162
  group-name     critical-traps
  community-name public
 !
 trap group all-traps
  all
   level minor major critical
  !
 !
 trap group critical-traps
  control
   level critical
 !
!
```

Operational Commands

show running-config snmp

Related Topics

show notification stream, on page 903
trap target, on page 509

trap target

Configure the target SNMP server to receive the SNMP traps generated by this device.

For each trap generated by a vEdge device, the device also generates a notification message. Use the **show notification stream viptela** command to display these messages.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  trap
    target vpn vpn-id ipv4-address udp-port
```

```
community-name community-name
group-name name
source-interface interface-name
```

Syntax Description

community-name *community-name*	Community Name: Name of an SNMP community configured with the **community** command.
group *group-name*	Group Name: Name of a trap group configured with the **trap group** command.
source-interface *interface-name*	Interface To Reach Target: Interface to use to send traps to the SNMP server that is receiving the trap information. This interface cannot be a subinterface.
vpn *vpn-id ipv4-address udp-port*	Trap Target: Location of the SNMP server to receive the trap information. You must specify the following: **vpn** *vpn-id*—Number of the VPN to use to reach to the SNMP server. It can be a value from 0 through 65530. *ipv4-address*—IPv4 address of the SNMP server. *udp-port*—UDP port number to connect to on the SNMP server. The number can be a value from 1 through 65535.

Command History

Release	Modification
15.2	Command introduced.
16.2	**source-interface** option added.

Examples

Configure trap groups and associate them with SNMP trap servers

```
vEdge# show running-config snmp
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 community private
  view          v2
  authorization read-only
 !
 trap target vpn 0 10.0.100.1 162
  group-name     test
  community-name private
  source-interface eth0
```

```
 !
 trap target vpn 0 10.0.100.1 16662
  group-name     test
  community-name private
  source-interface eht0
 !
 trap group test
  all
   level critical major minor
  !
 !
!
```

Operational Commands

show running-config snmp

Related Topics

show notification stream, on page 903
trap group, on page 507

tunnel-destination

Configure the destination IP address of a GRE tunnel interface (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface GRE

Command Hierarchy

```
vpn vpn-id
  interface gre number
    tunnel-destination ip-address
```

Syntax Description

ip-address	IP Address: IP address of the destination of a GRE tunnel interface.

Command History

Release	Modification
15.4.1	Command introduced.

Examples

Configure the destination IP address for a GRE tunnel

```
vEdge(config-vpn-0)# interface gre1
vEdge(config-interface-gre1)# tunnel-destination 172.168.1.1
vEdge(config-interface-gre1)# show full configuration
vpn 0
 interface gre1
  ip address 10.0.111.11/24
  keepalive 60 10
  tunnel-source      10.0.5.11
  tunnel-destination 172.168.1.1
  no shutdown
 !
!
```

Operational Commands

show interface

show tunnel gre-keepalives

show tunnel statistics

Related Topics

keepalive, on page 279
tunnel-source, on page 515

tunnel-destination

Configure the destination IP address of an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsec number
    tunnel-destination (dns-name | ipv4-address)
```

Syntax Description

dns-name	DNS Name: DNS name that points to the destination of the IPsec tunnel.
ipv4-address	IPv4 Address: IPv4 address of the tunnel's destination.

Command History

Release	Modification
17.2	Command introduced.

Examples

Configure a destination of an IPsec tunnel being used for IKE key exchange

```
vEdge(config)# vpn 1 interface ipsec1 tunnel-destination dns.viptela.com
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

ike, on page 236
tunnel-source, on page 514
tunnel-source-interface, on page 517

tunnel-interface

Configure the interface to be a secure DTLS or TLS WAN transport connection (on vEdge routers, vManage NMSs, and vSmart controllers only). Configuring an interface to be a transport tunnel enables the flow of control and data traffic on the interface. On vEdge routers, it configures the interface's TLOC attributes, which are carried in the TLOC OMP routes that the vEdge router sends to the vSmart controllers in its domain. For the TLOC attributes on vEdge routers, 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.

Because tunnel interfaces connect to the WAN transport, they can be present only in VPN 0, so you can include the **tunnel-interface** command only when configuring VPN 0.

On vEdge routers, you can configure up to six tunnel interfaces (a combination of tunnel interfaces on both physical and loopback interfaces). On vSmart controllers, you can configure only one tunnel interface.

vManage Feature Template

For vEdge routers, vManage NMSs, and vSmart controllers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      allow-service service-name
      bind interface-name (on vEdge routers only)
      carrier carrier-name
      color color [restrict]
      encapsulation (gre | ipsec) (on vEdge routers only)
        preference number
        weight number
      exclude-controller-group-list number (on vEdge routers only)
      group group-id
      hello-interval milliseconds
      hello-tolerance seconds
      hold-time milliseconds (on vEdge routers only)
      last-resort-circuit (on vEdge routers only)
      low-bandwidth-link (on vEdge routers only)
      max-control-connections number (on vEdge routers only)
      nat-refresh-interval seconds
      port-hop
      vbond-as-stun-server (on vEdge routers only)
      vmanage-connection-preference number (on vEdge routers only)
```

Command History

Release	Modification
14.1	Command introduced.
19.1	Added **group** option.

Examples

Create a tunnel for LTE traffic

```
vEdge(config)# vpn 0 interface ge0/0 tunnel-interface color lte
vEdge(config-tunnel-interface)# preference 10
vEdge(config-tunnel-interface)# weight 10
```

Operational Commands

show control connections

show interface

show omp tlocs and show omp tlocs detail (to display configured preference and weight values)

tunnel-source

Configure the source IP address of an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only). To configure the physical interface that is the source of an IPsec tunnel, use the **tunnel-source-interface** command.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsec number
    (tunnel-source ipv4-address | tunnel-source-interface interface-name)
```

Syntax Description

ipv4-address	Source Address: Source IPv4 address of the IPsec tunnel. This is an address in VPN 0 on the local vEdge router.

Command History

Release	Modification
17.2	Command introduced.

Examples

Configure the source IPv4 address of the IPsec tunnel used for IKE key exchange

```
vEdge(config)# vpn 1 interface ipsec1 tunnel-source 10.0.5.11
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

ike, on page 236
tunnel-destination, on page 512
tunnel-source-interface, on page 517

tunnel-source

Configure the source IP address of a GRE tunnel (on vEdge routers only).

To configure the physical interface that is the source of a GRE tunnel, use the **tunnel-source-interface** command.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface GRE

Command Hierarchy

```
vpn vpn-id
  interface gre number
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

Syntax Description

ip-address	Source Address: Source IP address of a GRE tunnel. This is an address on the local vEdge router.

Command History

Release	Modification
15.4.1	Command introduced.

Examples

Configure the source IP address for a GRE tunnel

```
vEdge(config-vpn-0)# interface gre1
vEdge(config-interface-gre1)# tunnel-source 10.0.5.11
vEdge(config-interface-gre1)# show full configuration
vpn 0
 interface gre1
  ip address 10.0.111.11/24
  keepalive 60 10
  tunnel-source      10.0.5.11
  tunnel-destination 172.168.1.1
  no shutdown
 !
!
```

Operational Commands

show interface

show tunnel gre-keepalive

show tunnel statistics

Related Topics

keepalive, on page 279
tunnel-destination, on page 511
tunnel-source-interface, on page 518

tunnel-source-interface

Configure the physical interface that is the source of an IPsec tunnel that is being used for IKE key exchange (on vEdge routers only). To configure the IPv4 address that is the source of an IPsec tunnel, use the **tunnel-source** command.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
vpn vpn-id
  interface ipsec number
    (tunnel-source ipv4-address | tunnel-source-interface interface-name)
```

Syntax Description

interface name	Source Address: Name of the physical interface that is the source IPv4 address of the IPsec tunnel. This is an interface that is configured in VPN 0 on the local vEdge router.

Command History

Release	Modification
17.1	Command introduced.

Examples

Configure the source physical interface of the IPsec tunnel being used for IKE key exchange

```
vEdge(config)# vpn 1 interface ipsec1 tunnel-source-interface ge0/2
```

Operational Commands

clear ipsec ike sessions

show ipsec ike inbound-connections

show ipsec ike outbound-connections

show ipsec ike sessions

Related Topics

ike, on page 236
tunnel-destination, on page 512
tunnel-source, on page 514

tunnel-source-interface

Configure the physical interface that is the source of a GRE tunnel (on vEdge routers only). To configure the source IP address of a GRE tunnel, use the **tunnel-source** command.

Command Hierarchy

```
vpn vpn-id
  interface gre number
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

Syntax Description

interface-name	Source Address: Name of the physical interface that is the source of a GRE tunnel. This interface must be configured in the same VPN as the GRE tunnel.

Command History

Release	Modification
16.1	Command introduced.

Examples

Configure the source interface for a GRE tunnel

```
vEdge(config-vpn-0)# interface gre1
vEdge(config-interface-gre1)# tunnel-source-interface ge1/2
vEdge(config-interface-gre1)# show full configuration
vpn 0
 interface gre1
  ip address 10.0.111.11/24
  keepalive 60 10
  tunnel-source-interface  ge1/2
  tunnel-destination 172.168.1.1
  no shutdown
 !
!
```

Operational Commands

show interface

show tunnel gre-keepalive

show tunnel statistics

Related Topics

keepalive, on page 279
tunnel-destination, on page 511
tunnel-source, on page 515

tunnel vrf multiplexing

To enable tunnel multiplexing, use the **tunnel vrf multiplexing** command in interface configuration mode. To remove the multiplexing, use the **no** form of this command.

tunnel vrf multiplexing
no tunnel vrf multiplexing

Command Default

Tunnel multiplexing is enabled.

Command Modes

Interface configuration (config-if)

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 configuring Secure Internet Gateway (SIG) tunnels, add this command to your tunnel configuration. 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 this command. This command enables VPN multiplexing and demultiplexing. This allows the hosts of multiple service VPNs to use the tunnel.

The following example shows how to set a Gigabit Ethernet interface as the tunnel source:

```
interface Tunnel10001
 no shutdown
 ip address 192.168.0.5 255.255.255.252
 ip mtu 1500
 tunnel source GigabitEthernet0/0/0
 tunnel destination 10.1.1.1
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
```

udp-timeout

Configure when NAT translations over a UDP session time out (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PP

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    nat
     udp-timeout minutes
```

Syntax Description

minutes	Time: Time after which NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minute

Command History

Release	Modification
14.2	Command introduced.

Examples

Change the NAT translation timeout value for UDP sessions to 1 hour

```
vEdge# config
vEdge(config)# vpn 1 interface ge0/4 nat udp-timeout 60
vEdge(config-nat)# show full-configuration
vpn 1
 interface ge0/4
  nat
    udp-timeout 60
  !
 !
!
```

Operational Commands

show ip nat filter

show ip nat interface

show ip nat interface-statistics

update-source

Have BGP use a specific IP address or interface for the TCP connection to the neighbor(on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp local-as-number
      neighbor ip-address
        update-source (ip-address | interface-name)
```

Syntax Description

ip-address	IP Address: IP address to use for the TCP connection to the neighbor, in decimal four-part dotted notation.
interface-name	Interface Name: Interface name to use for the TCP connection to the neighbor.

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure the IP address to use for the TCP connection to the BGP neighbor

```
vm6# show running-config vpn 1 router bgp 1 neighbor 10.20.25.18
vpn 1
 router
  bgp 1
   neighbor 10.20.25.18
    no shutdown
    remote-as 2
    !
    password  $4$L3rwZmsIiZB6wtBgLEFXKw==
    update-source 75.0.0.1
   !
  !
 !
!
```

Operational Commands

show bgp neighbor

upgrade-confirm

Configure the time limit for confirming that a software upgrade is successful. It is recommended that you configure this on all vEdge devices.

By default, software upgrade confirmation is not enabled. When you enable the confirmation, the device waits for the amount of time you configure. If the device does not come 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 come up.

After you issue the **request software install reboot** command to upgrade the software and then log in to the device after the reboot completes, enter the **request software 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.

Command Hierarchy

```
system
  upgrade-confirm minutes
```

Syntax Description

minutes	Time To Wait for Confirmation: How long to wait for a **request software upgrade-confirm** command to be issued before reverting to the previous software image if a software upgrade fails. Range: 5 through 60 minutes Default: None

Command History

Release	Modification
15.1	Command introduced.
15.2	Support for vBond orchestrator, vManage NMS, and vSmart controller added.

Examples

Set the upgrade confirmation time to 5 minutes. After a software upgrade, when the system reboots and restarts, if you do not issue a request software upgrade-confirm command within 5 minutes (either from the CLI or from the vManage NMS), the system automatically reverts to the software image that was running before the upgrade.

```
system
  upgrade-confirm
!
```

Operational Commands

request software activate

request software install

request software upgrade-confirm

Related Topics

request software activate, on page 701

usb-controller

Enable or disable the USB controller, which drives the external USB ports (on vEdge 1000 and vEdge 2000 series routers only). By default, the USB controller is disabled.

When you change the setting of this command in the configuration, the router reboots immediately, when you press the Enter key. You are prompted before the reboot occurs.

Enabling the USB controller allows you to copy configurations or files from or to a USB stick installed in the router.

Note that for vEdge 100 and vEdge 5000 series routers, the USB controller is enabled by default.

vManage Feature Template

For vEdge 1000 and vEdge 2000 series routers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  [no] usb-controller
```

Command History

Release	Modification
15.3.2	Command introduced.

Examples

Enable the USB controller on a vEdge route

```
vEdge(config)# system
vEdge(config-system)# usb-controller
The following warnings were generated:
  'system usb-controller': For this configuration to take effect, this command
  will cause an immediate device reboot
Proceed? [yes, no] yes
Starting cleanup
Stopping viptela daemon: sysmgr.
Rebooting now

Broadcast message from root@vEdge (pts/1) (Fri Apr 15 09:53:07 2016):

The system is going down for reboot NOW!
```

Operational Commands

show hardware environment

user

Configure an SNMPv3 user.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  user username
    auth authentication
    auth-password password
    group group-name
    priv privacy
    priv-password password
```

Syntax Description

auth *authentication* **auth-password** *password*	Authentication Type and Password: Authentication mechanism to use for the user. *authentication* can be either message digest5 (md5) or SHA-2 message digest (sha). Enter the password either in cleartext or as an AES-encrypted key.
group *group-name*	Group Name: Name of an SNMPv3 group configured with the **snmp group** command. *group-name* can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (" ").
priv *privacy* **priv-password** *password*	Privacy Type and Password: Privacy mechanism to use for the user. *privacy* can be the Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key (aes-cfb-128). In Releases 17.1 and earlier, *privacy* can also be the data encryption standard algorithm (des). Enter the password either in cleartext or as an AES-encrypted key.
user *username*	Username: Name of an SNMP user. It can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (" ").

Command History

Release	Modification
16.2	Command introduced.
17.2	Support for DES privacy removed.

Operational Commands

show running-config snmp

Related Topics

group, on page 217

user

system aaa user: Configure a login account for each user who can access the local Cisco vEdge device, assigning the user a login name and a password and placing them into an authorization group.

Only a user who is logged in as the **admin** user has permission to create login accounts for users.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
    user username
      group group-name
      password password
```

Syntax Description

group *group-name*	Authorization Group: Name of an authorization group configured with the **usergroup** command. You must assign the user to one or more groups.

user-name	Username: Name for the user. In Releases 17.1 and later, *username* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. In Releases 16.3 and earlier, *username* can be 1 to 32 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, and the hyphen (-) and underscore (_) characters. The name cannot contain any uppercase letters. The Cisco SD-WAN software provides one standard username, **admin**, which is a superuser who has read and write permissions to all commands and operations on the device. The following usernames are reserved, so you cannot configure them: **backup**, **basic**, **bin**, **daemon**, **games**, **gnats**, **irc**, **list**, **lp**, **mail**, **man**, **news**, **nobody**, **proxy**, **quagga**, **root**, **sshd**, **sync**, **sys**, **uucp**, and **www-data**. Also, names that start with **viptela-reserved** are reserved. If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user "basic", with a home directory of /home/basic. If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of */home/username* (so, /home/eve).
password *password*	User Password: Password for the user. *password* is an MD5 digest string, and it can contain any Unicode and ISO/IEC 10646 characters, including tabs, carriage returns, and linefeeds. To include an exclamation point (!) in a password, enclose the entire password in quotation marks (for example, "Pass01!"). For more information about allowed password characters, see Section 9.4 in RFC 7950, *The YANG 1.1 Data Modeling Language*. Each username is required to have a password, and each user is allowed to change their own password. After you type the password during the CLI configuration process, the string is immediately encrypted and a readable version of the password is never displayed. When you type the password in the vManage AAA feature template, a readable version is never displayed. When a user is logging in to a vEdge device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and they must wait 15 minutes before attempting to log in again.

Command History

Release	Modification
14.1	Command introduced.
17.1	Increased maximum group name to 128 characters and support periods (.) in group name.

Examples

Configure a user whose role is to be a system operator

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# system aaa
vedge-1(config-aaa)# user eve
vEdge(config-user-eve)# password 123456
vEdge(config-user-eve)# group operator
vEdge(config-user-eve)# exit
vEdge(config-aaa)# show configuration
system
 aaa
  user eve
   password encrypted-password
   group    operator
  !
 !
!
```

Operational Commands

show aaa usergroup

show users

Related Topics

auth-fallback, on page 82
auth-order, on page 85
radius, on page 407
tacacs, on page 474
usergroup, on page 527

usergroup

Configure groupings of users and assign authorization privileges to the group. Groups define what tasks the group members are authorized to perform on the vEdge device.

If an *admin* user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

```
system
  aaa
     usergroup group-name
       task (interface | policy | routing | security | system) (read | write)
```

Syntax Description

group-name	Group Name: Name of an authentication group. In Releases 17.1 and later, *group-name* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. In Releases 16.3 and earlier, *group-name* can be 1 to 32 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, and the hyphen (-) and underscore (_) characters. The name cannot contain any uppercase letters. The vEdge software provides three standard user groups, *basic*, *netadmin*, and *operator*. The user *admin* is automatically placed in the group *netadmin* and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group *basic*. All users in the basic group have the same permissions to perform tasks, as do all users in the *operator* group. The following groups names are reserved, so you cannot configure them: *adm*, *audio*, *backup*, *bin*, *cdrom*, *dialout*, *dip*, *disk*, *fax*, *floppy*, *games*, *gnats*, *input*, *irc*, *kmem*, *list*, *lp*, *mail*, *man*, *news*, *nogroup*, *plugdev*, *proxy*, *quagga*, *quaggavty*, *root*, *sasl*, *shadow*, *src*, *sshd*, *staff*, *sudo*, *sync*, *sys*, *tape*, *tty*, *uucp*, *users*, *utmp*, *video*, *voice*, and *www-data*. Also, group names that start with the string *viptela-reserved* are reserved. If a remote server validates authentication but does not specify a user group, the user is placed into the user group *basic*. If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).
task (interface | policy | routing | security | system) (read | write)	Tasks Allowed: Privilege roles that the user group has. Each role allows the group to read or write specific portions of the device's configuration and to execute specific types of operational commands. For details, see the *Role-Based Access with AAA* article for your software release.

Command History

Release	Modification
14.1	Command introduced.
15.3	Force a user to log out when their permissions are changed.
17.1	Increase maximum group name to 128 characters and support periods (.) in group name.

Examples

Display the default user groups and their privileges

```
vEdge# show running-config system aaa usergroup
system
 aaa
  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
  !
 !
!
```

Operational Commands

show aaa usergroup

show users

Related Topics

radius, on page 407
tacacs, on page 474
user, on page 525

vbond

Configure the IP address and other information related to the vBond orchestrator.

vManage Feature Template

For vEdge routers acting as vBond controllers only:

Configuration ► Templates ► System

Command Hierarchy

```
system
  vbond (dns-name | ip-address) [local] [port number] [ztp-server]
```

In Releases 16.3 and later, the following command hierarchy is also available:

```
system
  vbond [dns-name | host-name | ip-address] [local] [port number] [ztp-server]
```

Syntax Description

vbond-only (Deprecated starting with Release 16.1)	Configure Device To Be only a vBond Orchestrator: Configure a hardware vEdge router or a software vEdge Cloud router to act only as a vBond orchestrator. Starting with Release 16.1, you must include this option to configure a vBond orchestrator. Starting with Release 16.1, a vBond orchestrator and a vEdge router cannot coexist in the same virtual machine or on the same hardware router, so do not configure any edge router functionality on a vBond orchestrator.
dns-name	DNS Name of the vBond Orchestrator: DNS name that points to one vBond orchestrator. The address can resolve to a vBond orchestrator configured with an IPv4 address or an IPv6 address.
ip-address	IP Address of the vBond Orchestrator: IPv4 or IPv6 address of the vBond orchestrator, in decimal four-part dotted notation. You can configure one address, and it must be a public IP address.
local	Local vBond System: (On vBond orchestrator only. Designate the local vEdge router to be a vBond orchestrator in the vEdge overlay network domain. Starting in Release 16.3, if you configure the *local* option, you can omit the DNS name, hostname, or IP address of the vBond orchestrator as long as one of the interfaces in VPN 0 has a routable public IP address.
ztp-server	Local Zero-Touch-Provisioning Server: Designate the local vEdge router to be the zero-touch-provisioning (ZTP) server in the overlay network domain. Such a vBond orchestrator acts as an enterprise ZTP server, and provides the vEdge routers in your domain with the IP address of your enterprise vBond orchestrator and with the enterprise root CA chain. You must load two files onto your enterprise ZTP server: the vEdge authorized serial number file that you received from vEdge and your enterprise root CA chain, which must be signed by Symantec. You must also configure your enterprise DNS server with an A record that redirects the URL ztp.viptela.com to your enterprise ZTP server. The recommended URL for this enterprise server is *ztp.your-company-name.com*. A vEdge router acting as an enterprise ZTP server should be dedicated to that function. It cannot be used as a regular vBond orchestrator in the overlay network domain. Also, it is recommended that you not use it in an edge router capacity.
host-name	Host name of the vBond Orchestrator: Fully-Qualified Domain Name (FQDN) of the vBond orchestrator. **Note** If you want to configure addresses of multiple vBond orchestrators, but are not using a DNS name resolution server, you can configure the hostname of an orchestrator. Then, in VPN 0, use the **host** command to configure the IP addresses of the vBond orchestrators. For example, if you configure **system vbond vbond1**, you could configure **vpn 0 host vbond1 10.0.12.26 2001::10.0.12.26** to configure two vBond orchestrator addresses, one an IPv4 address and the second an IPv6 address.

port *number*	Port Number to Connect to vBond Orchestrator: Port number to use to connect to the vBond orchestrator. If you omit this option, the local system first tries port 12346 on the vBond orchestrator. 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 use to connect to the vBond orchestrator. Default: 12346 Range: 1 through 65535
no system vbond	Remove a vBond Orchestrator from the Configuration: Remove the vBond configuration from the device. If you have configured an IP address for the vBond orchestrator, to change the address, you must delete the address and then configure the new address. Doing this causes all of the devices existing connections to the vEdge devices in the network to go down; they come back up after you commit the configuration with the new IP address. To avoid this problem, it is highly recommended that you always use a DNS name for your vBond orchestrators, and then make changes to the DNS devices instead of on the vEdge routers and vSmart controllers directly.

Command History

Release	Modification
14.1	Command introduced.
14.3	**ztp-server** option added.
16.1	**vbond-only** option deprecated.

Examples

Configure the DNS name of a vBond orchestrator on a vEdge router:

```
system
  vbond vbond.east.acme.com
!
```

Designate the local vEdge router to be a vBond orchestrator in its vEdge overlay network domain:

```
system
  vbond 10.0.4.12 local
!
```

Designate the local vEdge router to be an enterprise ZTP server:

```
system
  vbond 75.1.16.4 local ztp-server
!
```

Operational Commands

nslookup

show control connections

Related Topics

port-hop, on page 391

vbond-as-stun-server

Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT (on vEdge routers only). When you configure this command, vEdge routers can exchange their public IP addresses and port numbers over private TLOCs.

With this configuration, the vEdge router uses the vBond orchestrator as a STUN server, so the router can determine its public IP address and public port number. (With this configuration, the router 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 the the vBond orchestrator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it.

Because no control traffic is sent over a tunnel interface that is configured to use the vBond orchestrator as a STUN server, you must configure at least one other tunnel interface on the vEdge router so that it can exchange control traffic with the vSmart controller and the vManage NMS.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      vbond-as-stun-server
```

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure two tunnel interfaces, one to use for the exchange of control traffic (ge0/2) and the other to allow the device to discover its public IP address and port number from the vBond orchestrator (ge0/1). Note that the no allow-service stun command, which is configured by default on tunnel interfaces, pertains to allowing or disallowing the vEdge router 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.

```
vEdge(config-interface-ge0/1)# show full-configuration
vpn 0
 interface ge0/1
  ip address 10.0.26.11/24
  tunnel-interface
   encapsulation ipsec
   vbond-as-stun-server
   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
  !
  no shutdown
 !
!
vEdge(config-interface-ge0/1)# exit
vEdge(config-vpn-0)# interface ge0/2
vEdge(config-tunnel-interface)# show full-configuration
vpn 0
 interface ge0/2
  tunnel-interface
   encapsulation ipsec
   color lte
   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
  !
 !
!
```

Operational Commands

show running-config

Related Topics

allow-service, on page 63

view

Define an SNMP MIB view.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► SNMP

Command Hierarchy

```
snmp
  view string
    oid oid-subtree [exclude]
```

Syntax Description

exclude	Include or Exclude a Subtree of MIB Objects: If you omit the **exclude** option in the **oid** command, the subtree of MIB objects is included, or viewable, in the MIB view. If you specify the **exclude** option, the subtree of MIB objects is excluded and hence is not viewable in the MIB view. For example, you might want to exclude MIB objects which could potentially reveal information about configure SNMP credentials (such as snmpUsmMIB, snmpVacmMIB, and snmpCommunityMIB).
oid *oid-subtree*	Object Identifier: Object identifier of a subtree of MIB objects. Specify the OID in Abstract Syntax Notation One (ASN.1) notation, as a sequence of dotted integers that identify the node of an SNMP tree. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name.
view *string*	View Name: Name of the view record you are creating. It can be a maximum of 32 characters. If the name includes spaces, enclose it in quotation marks (" ").

Command History

Release	Modification
14.1	Command introduced.
16.2	Wildcard for configuring OID subtree added.

Examples

Create a view of the Internet portion of the SNMP MIB:

```
vEdge# show running-config snmp
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 community private
  view          v2
  authorization read-only
 !
!
```

Create a view of the private portion of the Cisco SD-WAN MIB:

```
vEdge(config-snmp)# view viptela-private oid 1.3.6.1.4.1.41916
```

Configure a MIB view for system status:

```
vEdge(config)# show config
snmp
 view status
  oid 1.3.6.1.2.1.2.2.2.1.8
 !
!
```

Operational Commands

show running-config snmp

vlan

Associate a VLAN tag (identifier) with the bridging domain (on vEdge routers only).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► Bridge

Command Hierarchy

```
bridge bridge-id
  vlan vlan-id
```

Syntax Description

vlan-id	VLAN Tag: VLAN identifier to associate with the bridging domain. Range: 0 through 4095

Command History

Release	Modification
15.3	Command introduced.

Examples

Associate a VLAN ID with a bridging domain

```
vEdge(config)# bridge 1
vEdge(config-bridge-1)# vlan 27
```

Operational Commands

show bridge interface

show bridge mac

show bridge table

vmanage-connection-preference

Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS (on vEdge routers only). Configuring this option is useful for LTE and other links on which you want to minimize traffic.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface PPP

Command Hierarchy

```
vpn 0
  interface interface-name
    tunnel-interface
      vmanage-connection-preference number
```

Syntax Description

number	Preference Value: Preference for using the tunnel interface to exchange control traffic with the vManage NMS. The tunnel with the higher value has a greater preference to be used for connections to the vManage NMS. To have a tunnel interface never connect to the vManage NMS, set the preference value to 0. At least one tunnel interface on the vEdge router must have a non-0 preference value. Range: 0 through 8 Default: 5

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure a tunnel interface for an LTE interface to be the TLOC that carries control traffic between the vEdge router and the vManage NMS

```
vpn 0
 interface ge0/0
  ip address 10.1.15.15/24
  tunnel-interface
   color lte
   vmanage-connection-preference 8
  !
  no shutdown
 !
```

Operational Commands

show control local-properties | display xml | include vmanage-connection

Related Topics

low-bandwidth-link, on page 309

vpn

Configure VPNs to use for segmentation of the vEdge overlay network.

vManage Feature Template

Configuration ► Templates ► VPN Interface Bridge

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)

Configuration ► Templates ► VPN Interface Ethernet

Configuration ► Templates ► VPN Interface GRE

Configuration ► Templates ► VPN Interface IPsec

Configuration ► Templates ► VPN Interface NAT Pool

Configuration ► Templates ► VPN Interface PPP

Configuration ► Templates ► VPN Interface PPP Ethernet

Command Hierarchy

```
vpn vpn-id
  bandwidth-downstream kbps (on vEdge routers and vManage NMSs only)
  bandwidth-upstream kbps (on vEdge routers and vManage NMSs only)
  dns ip-address [primary | secondary]
  ecmp-hash-key layer4 (on vEdge routers only)
  host hostname ip ip-address
  interface interface-name
    access-list acl-list (on vEdge routers only)
    arp
      ip ip-address mac mac-address
    arp-timeout seconds (on vEdge routers only)
    autonegotiate (on vEdge routers only)
```

```
block-non-source-ip (on vEdge routers only)
clear-dont-fragment
dead-peer-detection interval seconds retries number
description text
dhcp-helper ip-address (on vEdge routers only)
dhcp-server (on vEdge routers only)
  address-pool prefix/length
  exclude ip-address
  lease-time seconds
  max-leases number
  offer-time minutes
  options
    default-gateway ip-address
    dns-servers ip-address
    domain-name domain-name
    interface-mtu mtu
    tftp-servers ip-address
  static-lease mac-address ip ip-address host-name hostname
dot1x
  accounting-interval seconds
  acct-req-attr attribute-number (integer integer | octet octet | string string)
  auth-fail-vlan vlan-id
  auth-order (mab | radius)
  auth-reject-vlan vlan-id
  auth-req-attr attribute-number (integer integer | octet octet | string string)
  control-direction direction
  das
    client ip-address
    port port-number
    require-timestamp
    secret-key password
    time-window seconds
    vpn vpn-id
  default-vlan vlan-id
  guest-vlan vlan-id
  host-mode (multi-auth | multi-host | single-host)
  mac-authentication-bypass
    allow mac-addresses
    server
  nas-identifier string
  nas-ip-address ip-address
  radius-servers tag
  reauthentication minutes
  timeout
    inactivity minutes
  wake-on-lan
duplex (full | half)
flow-control (bidirectional | egress | ingress)
ike (on vEdge routers only)
  authentication-type type
    local-id id
    pre-shared-secret password
    remote-id id
  cipher-suite suite
  group number
  mode mode
  rekey seconds
  version number
(ip address prefix/length | ip dhcp-client [dhcp-distance number])
(ipv6 address prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-commit])

ip address-list prefix/length (on vSmart controller containers only)
ip secondary-address ipv4-address (on vEdge routers only)
ipsec (on vEdge routers only)
```

```
      cipher-suite suite
      perfect-forward-secrecy pfs-setting
      rekey seconds
      replay-window number
    keepalive seconds retries (on vEdge routers only)
    mac-address mac-address
    mtu bytes
    nat (on vEdge routers only)
      block-icmp-error
      direction (inside | outside)
      log-translations
      [no] overload
      port-forward port-start port-number1 port-end port-number2
        proto (tcp | udp) private-ip-address ip address private-vpn vpn-id
      refresh (bi-directional | outbound)
      respond-to-ping
      static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
     static source-ip ip-address1 translate-ip ip-address2 source-vpn vpn-id protocol (tcp
 | udp) source-port number translate-port number
      tcp-timeout minutes
      udp-timeout minutes
    pmtu (on vEdge routers only)
    policer policer-name (on vEdge routers only)
    ppp (on vEdge routers only)
      ac-name name
      authentication (chap | pap) hostname name password password
    pppoe-client (on vEdge routers only)
      ppp-interface name
    profile profile-id (on vEdge routers only)
    qos-map name (on vEdge routers only)
    rewrite-rule name (on vEdge routers only)
    shaping-rate name (on vEdge routers only)
    [no] shutdown
    speed speed
    static-ingress-qos number (on vEdge routers only)
    tcp-mss-adjust bytes
    technology technology (on vEdge routers only)
    tloc-extension interface-name (on vEdge routers only)
    tracker tracker-name (on vEdge routers only)
    tunnel-interface
      allow-service service-name
      bind geslot/port (on vEdge routers only)
      carrier carrier-name
      color color [restrict]
      connections-limit number (on vManage NMSs only)
      encapsulation (gre | ipsec) (on vEdge routers only)
        preference number
        weight number
      exclude-controller-group-list number (on vEdge routers only)
      hello-interval milliseconds
      hello-tolerance seconds
      last-resort-circuit (on vEdge routers only)
      low-bandwidth-link (on vEdge routers only)
      max-control-connections number (on vEdge routers only)
      nat-refresh-interval seconds
      vbond-as-stun-server (on vEdge routers only)
      vmanage-connection-preference number (on vEdge routers only)
    tunnel-destination ip-address (GRE interfaces; on vEdge routers only)
    tunnel-destination (dns-name | ipv4-address) (IPsec interfaces; on vEdge routers only)
    (tunnel-source ip-address | tunnel-source-interface interface-name) (GRE interfaces;
on vEdge routers only)
    (tunnel-source ip-address | tunnel-source-interface interface-name) (IPsec interfaces;
 on vEdge routers only)
    upgrade-confirm minutes
```

```
    vrrp group-name (on vEdge routers only)
      priority number
      timer seconds
      track-omp
  ! end vpn interface
  ip route ip-address/subnet next-hop-address
  name text
  omp
    advertise (aggregate prefix [aggregate-only] | bgp | connected | network prefix | ospf
 type | static) (on vEdge routers only)
  router (on vEdge routers only)
    bgp ...
    igmp ...
    multicast-replicator local
      threshold number
    ospf ...
    pim ...
  service service-name address ip-address (on vEdge routers only)
```

Syntax Description

vpn-id	VPN Identifier: Numeric identifier of the VPN. VPN 0 is the transport VPN and is reserved for control plane traffic. VPN 512 is reserved for out-of-band management traffic. Values: On vEdge routers: 0 through 65530 On Cisco SD-WAN controller devices: 0, 512

Command History

Release	Modification
14.1	Command introduced.

Examples

Configure VPN 0, which is the transport VPN used to reach the WAN. Here, the vEdge router connects to the WAN over interface ge0/1

```
vpn 0
 interface ge0/1
   ip address 10.2.6.11/24
     color default
     preference 10
     weight 10
   !
   no shutdown
   !
 ip route 0.0.0.0/0 10.2.6.12
!
```

Operational Commands

show bgp commands (on vEdge routers only)

show interface commands

show multicast commands (on vEdge routers only)

show ospf commands (on vEdge routers only)

show pim commands (on vEdge routers only)

vpn-membership

Configure or apply a centralized data policy based on VPN membership (on vSmart controllers only).

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

Create a Centralized Data Policy

```
policy
  vpn-membership policy-name
    default-action (accept | reject)
    sequence number
      match
        vpn vpn-id
        vpn-list list-name
      action (accept | reject)
```

Apply a Centralized Data Policy

```
apply-policy
  site-list list-name vpn-membership policy-name
```

Syntax Description

policy-name	VPN Membership Policy Name: Name of the VPN membership 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 History

Release	Modification
14.1	Command introduced.

Examples

Create and apply a VPN membership policy for a group of VPNs

```
vSmart# show running-config
...
```

```
policy
 lists
  vpn-list east-vpns
   vpn 1-10
  !
  site-list east-sites
   site-id 100-110
  !
 !
 vpn-membership vpn-policy
  sequence 1
   match vpn-list east-vpns
   action accept
   !
  !
  default-action reject
 !
!
...
apply-policy
 site-list east-sites
  vpn-membership vpn-policy
 !
!
...
```

Operational Commands

show policy commands

Related Topics

data-policy, on page 165

vrrp

Configure the Virtual Router Redundancy Protocol (VRRP) to allow multiple routers to share a common virtual IP address for default gateway redundancy (on vEdge routers only).

Hosts are assigned a single default gateway (also called default router) IP address, either through DHCP or statically for the first-hop router. This situation creates a single point of failure in the network. VRRP provides default gateway (first-hop router) redundancy through configuration of a virtual IP address shared by multiple routers on a single LAN or subnet.

One router on the LAN or subnet becomes primary, thus assuming the role of the default gateway, and the other routers take the role of subordinate. When the primary router fails, one of the subordinates is elected as the new primary and assumes the role of default gateway.

You cannot configure VRRP on an interface that is in the transport VPN (VPN 0).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface geslot/port[.subinterface]
    vrrp group-number
      ipv4 ip-address
      priority number
      timer seconds
      (track-omp | track-prefix-list list-name )
```

Syntax Description

timer *seconds*	Advertisement Time: How often the VRRP primary sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary. **For Cisco vEdge Devices** Range: 1 through 3600 seconds Default: 1 second **For Cisco XE SD-WAN Routers** Range: 100 through 3600 milliseconds Default: 100 milliseconds
priority *number*	Priority To Be Elected Primary: Priority level of the router. The router with the highest priority is elected as primary. If two vEdge routers have the same priority, the one with the higher IP address is elected as primary. Range: 1 through 254 Default: 100

(**track-omp | track-prefix-list list-name** *list-name*)	Track Interface State: By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which vEdge router is the primary virtual router. When the interface for the primary goes down, a new VRRP primary virtual router is elected based on the VRRP priority value. Because VRRP runs on a LAN interface, if a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following: **track-omp**: Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the VRRP primary virtual router. If all OMP sessions are lost on the primary VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current primary. With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. (The default OMP hold timer interval is 300 seconds.) Until the hold timer expires and a new VRRP primary is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as primary even before it learns and installs OMP routes from the vSmart controllers. Until the routes are learned, traffic is also dropped. **track-prefix-list**: Tracks only the selected OMP remote prefixes on routing table (RIB). *list-name* is the name of a prefix list configured with the **policy lists prefix-list** command on the vEdge router. If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp** option. OMP session lost does not immediately mean that failover occurs. Default: VRRP tracks only the interface on which it is configured.
vrrp *group-number*	Virtual Router ID: Virtual router ID, which is a numeric identifier of the virtual router. For each interface or subinterface, you can configure only a single VRRP group. On a router, you can configure a maximum of 512 groups. Range: 1 through 512
ip address *ip-address*	Virtual Router IP Address: IP address of the virtual router. The virtual IP address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP. For each interface or subinterface, you can configure only a single virtual IP address.

Command History

Release	Modification
14.1	Command introduced.
15.2	Tracking by prefix list added.
18.3	You can configure a maximum of 24 VRRP groups on a router.

Release	Modification
Cisco SD-WAN Release 20.3.1	Added support for up to 5 VRRP groups per interface, and up to 512 groups on a router. The VRRP group number range increased to: 1 to 512

Example: Configure VRRP in VPN 1, on the subinterface ge0/1.3 on vEdge Devices

```
vpn 1
 interface ge0/1.3
  ip address 10.2.3.11/24
  mtu 1490
  no shutdown
  vrrp 3
   priority 200
   timer    1
   ipv4 10.2.3.201
   track-prefix-list vrrp-prefix-list
  !
 !
```

Example: Configure VRRP on Cisco XE SD-WAN Routers

```
interface GigabitEthernet0/0/2
description to-LAN
no shutdown
arp timeout 1200
vrf forwarding 1
ip address 10.180.4.3 255.255.255.0
ip redirects
ip mtu    1500
mtu         1500
negotiation auto
vrrp 1 address-family ipv4
  vrrpv2
  address 10.180.4.1
  priority 90
  timers advertise 1000
exit
exit
```

Example: Multiple VRRP Groups on One Interface

The following is an example of configuring 5 VRRP groups on 1 interface.

```
vpn 2
 interface ge0/4.2
  ip address 10.0.1.10/24
  ip secondary-address 10.0.2.10/24
  ip secondary-address 10.0.3.10/24
  ip secondary-address 10.0.4.10/24
  mtu 1496
  no shutdown
  vrrp 1
   priority 101
    ipv4 10.0.1.1
!
```

```
  vrrp 2
   ipv4 10.0.1.2
!
  vrrp 3
   priority 101
    ipv4 10.0.2.1
!
  vrrp 4
   ipv4 10.0.3.1
!
  vrrp 5
   ipv4 10.0.4.1
  !
 !
!
```

Note For Cisco IOS XE Catalyst SD-WAN devices, the VRRP timer range is 100 to 3600 milliseconds.

Related Topics

timers, on page 492

wake-on-lan

Allow a client to be powered up when the vEdge router receives an Ethernet magic packet frame (on vEdge routers only). This feature allows you to connect to clients that have been powered down.

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface Ethernet

Command Hierarchy

```
vpn vpn-id
  interface interface-name
    dot1x
      wake-on-lan
```

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure wake on LAN on an 802.1X interface

```
vEdge# show running-config vpn 0 interface ge0/7
vpn 0
```

```
interface ge0/7
  dot1x
    control-direction in-and-out
    wake-on-lan
```

Operational Commands

clear dot1x client

show dot1x clients

show dot1x interfaces

show dot1x radius

show system statistics

Related Topics

control-direction, on page 147
radius, on page 407

wlan

Configure a wireless WAN (WLAN) (on vEdge cellular wireless routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi Radio

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  channel channel
  channel-bandwidth megahertz
  country country
  guard-interval nanoseconds
  interface vapnumber
    data-security security
    description text
    max-clients number
    mgmt-security security
    radius-servers tag
    [no] shutdown
    ssid ssid
    wpa-personal-key password
```

Syntax Description

radio-band	WLAN Frequency: Select the radio band for the WLAN channel to use: 2.4GHz—Supports 13 channels that are spaced 5 MHz apart; channel 14 is not supported. This radio band supports IEEE 802.11b, 802.11g, and 802.11n clients. 5GHz—For this channel, allowable channels, allowed users, and maximum power level with the frequency ranges are country-specific. This radio band supports IEEE 802.11a, 802.11n, and 802.11ac clients. The allowable channels and the maximum transmission power for these channels are country specific.

Command History

Release	Modification
16.3	Command introduced.

Examples

Configure a 5-GHz WLAN channel

```
vEdge# show running-config wlan
wlan 5GHz
 channel 36
 interface vap0
  ssid     tb31_pm6_5ghz_vap0
  no shutdown
 !
 interface vap1
  ssid           tb31_pm6_5ghz_vap1
  data-security  wpa/wpa2-enterprise
  radius-servers tag1
  no shutdown
 !
 interface vap2
  ssid             tb31_pm6_5ghz_vap2
  data-security    wpa/wpa2-personal
  mgmt-security    optional
  wpa-personal-key $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
  no shutdown
 !
 interface vap3
  ssid           tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers tag1
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

radius, on page 407

wpa-personal-key

Configure the password to access a wireless LAN that uses wpa-personal or wpa2-personal security (on vEdge cellular wireless routers only).

vManage Feature Template

For vEdge cellular wireless routers only:

Configuration ► Templates ► WiFi SSID

Command Hierarchy

```
wlan radio-band
  interface vapnumber
    wpa-personal-key password
```

Syntax Description

password	Password: Password that users must enter to access the wireless LAN. The password is case sensitive. You can enter it in clear text or an AES-encrypted key.

Command History

Release	Modification
16.3	Command introduced.

Examples

Set a WPA password for a VAP interface (that is, for an SSID)

```
vEdge# show running-config wlan 5GH1 interface vap1
wlan 5GHz
 interface vap1
  ssid             GuestNetwork
  data-security    wpa/wpa2-personal
```

```
  wpa-personal-key GuestPassword
  max-clients      10
  no shutdown
 !
!
```

Operational Commands

clear wlan radius-stats

show interface

show wlan clients

show wlan interfaces

show wlan radios

show wlan radius

Related Topics

data-security, on page 168

zone

Create a group of one or more VPNs in the overlay network that form a zone (on vEdge routers only).

Command Hierarchy

```
policy
  zone zone-name
    vpn vpn-id
```

Syntax Description

vpn *vpn-id*	VPN: Numeric identifier of the VPN. Range: 0 through 65530
zone-name	Zone Name: Name of the zone.

Command History

Release	Modification
18.2	Command introduced.

Examples

Configure and apply a zone-based firewall policy

```
vEdge# show running-config policy
policy
  zone A
    vpn 1
  !
  zone B
    vpn 2
    vpn 3
    vpn 4
  !
  zone-to-nozone-internet allow
  zone-pair zbfw-pair-1
    source-zone A
    destination-zone B
    zone-policy zbfw-policy-1
  !
  zone-based-policy zbfw-policy-1
    sequence 1
      match
        protocol 6
      !
      action inspect
      !
    !
    default-action drop
  !
!
```

Operational Commands

show running-config policy

show policy zbfw filter-statistics

Related Topics

zone-based-policy, on page 551
zone-pair, on page 553
zone-to-nozone-internet, on page 555

zone-based-policy

Create a zone-based firewall policy for stateful inspection of ICMP, TCP, and UDP flows between one VPN, or zone, and another (on vEdge routers only).

Command Hierarchy

Create a Zone-Based Firewall Policy

```
policy
  zone-based-policy zone-policy-name
    default-action (drop | inspect | pass)
    sequence number
      match
```

```
        destination-data-prefix-list list-name
        destination-ip prefix/length
        destination-port number
        protocol number
        source-data-prefix-list list-name
        source-ip prefix-length
        source-port number
      action
        drop
        inspect
        log
        pass
```

Apply a Zone-Based Firewall Policy

```
policy
  zone zone-name
    vpn vpn-id
  zone-pair zone-pair-name
    destination-zone zone-name
    source-zone zone-name
    zone-policy zone-policy-name
```

Syntax Description

zone-policy-name	Zone Policy Name: Name of the zone-based firewall policy to configure or to apply to a zone pair in the overlay network. The zone name can be from 1 to 32 characters longs.

Command History

Release	Modification
18.2	Command introduced.

Examples

Configure and apply a zone-based firewall policy

```
vEdge# show running-config policy
policy
  zone A
    vpn 1
  !
  zone B
    vpn 2
    vpn 3
    vpn 4
  !
  zone-to-nozone-internet allow
  zone-pair zbfw-pair-1
    source-zone A
    destination-zone B
    zone-policy zbfw-policy-1
  !
  zone-based-policy zbfw-policy-1
    sequence 1
      match
```

```
        protocol 6
      !
      action inspect
      !
    !
    default-action drop
  !
!
```

Operational Commands

clear policy zbfw filter-statistics

clear policy zbfw global-statistics

clear policy zbfw sessions

show policy zbfw filter-statistics

show policy zbfw global-statistics

show policy zbfw sessions

Related Topics

zone, on page 550
zone-pair, on page 553
zone-to-nozone-internet, on page 555

zone-pair

Configure a zone pair to apply a zone-based firewall policy to traffic flows between a source zone and a destination zone (on vEdge routers only).

Command Hierarchy

```
policy
  zone-pair pair-name
    destination-zone zone-name
    source-zone zone-name
    zone-policy zone-policy-name
```

Syntax Description

destination-zone *zone-name*	Destination Zone: Name of the destination zone. This is the zone to which traffic flows are destined, and that you configured with the **policy zone** command.
source-zone *zone-name*	Source Zone: Name of the source zone. This is the zone from which traffic flows are sent, and that you configured with the **policy zone** command.
zone-policy *zone-policy-name*	Zone-Based Firewall Policy: Name of the zone-based firewall policy to apply to the zone pair. This is a policy you configured with the **policy zone-based-policy** command.

pair-name	Zone Pair Name: Name of the zone pairing.

Command History

Release	Modification
18.2	Command introduced.

Examples

Configure and apply a simple zone-based firewall policy

```
vEdge# show running-config policy
policy
  zone A
    vpn 1
  !
  zone B
    vpn 2
    vpn 3
    vpn 4
  !
  zone-to-nozone-internet allow
  zone-pair zbfw-pair-1
    source-zone A
    destination-zone B
    zone-policy zbfw-policy-1
  !
  zone-based-policy zbfw-policy-1
    sequence 1
      match
        protocol 6
      !
      action inspect
      !
    !
    default-action drop
  !
!
```

Operational Commands

clear policy zbfw sessions

show policy zbfw sessions

show running-config policy

Related Topics

zone, on page 550
zone-based-policy, on page 551

zone-to-nozone-internet

For a zone-based firewall, control whether packets can reach destination zones that are accessible only over the public internet if none of the zones in the zone-based firewall policy include VPN 0 (on vEdge routers only). By default, if you do not include VPN 0 in any of the configured zones, packets can reach their destination zone over the public internet.

You can add this command to the configuration only after you have configured at least one zone. If you remove all zones from a configuration, the value of this command returns to the default of **allow** . If you want to block internet access, you must configure the **deny** option again.

Command Hierarchy

```
policy
  zone-to-nozone-internet (allow | deny)
```

Syntax Description

allow	Allow Traffic To Use the Public Internet: If you do not include VPN 0 in any of the configured zones, packets can travel over the public internet to reach their destination zone. This is the default.
deny	Do Not Allow Traffic To Use the Public Internet: If you do not include VPN 0 in any of the configured zones, packets cannot travel over the public internet to reach their destination zone.

Command History

Release	Modification
18.2	Command introduced.

Examples

Configure and apply a simple zone-based firewall

```
vEdge# show running-config policy
policy
  zone A
    vpn 1
  !
  zone B
    vpn 2
    vpn 3
    vpn 4
  !
  zone-to-nozone-internet allow
  zone-pair zbfw-pair-1
    source-zone A
    destination-zone B
    zone-policy zbfw-policy-1
  !
```

```
  zone-based-policy zbfw-policy-1
    sequence 1
      match
        protocol 6
      !
      action inspect
      !
    !
    default-action drop
  !
!
```

Operational Commands

clear policy zbfw filter-statistics

clear policy zbfw global-statistics

clear policy zbfw sessions

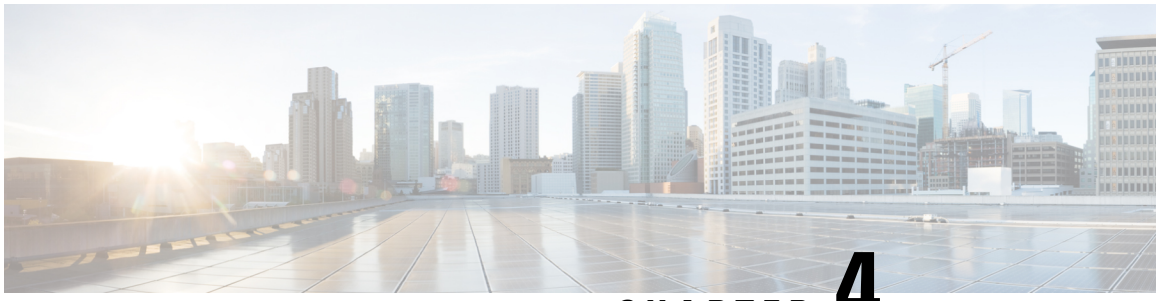
show policy zbfw filter-statistics

show policy zbfw global-statistics

show policy zbfw sessions

Related Topics

zone, on page 550
zone-based-policy, on page 551
zone-pair, on page 553



CHAPTER 4

Operational Commands

Note For a list of Cisco IOS XE SD-WAN commands qualified for use in Cisco vManage CLI templates, see List of Commands Qualified in Cisco IOS XE Release 17.x. For information about specific commands, see the appropriate chapter in Cisco IOS XE SD-WAN Qualified Command Reference Guide.

- Overview of Operational Commands, on page 565
- clear aaa login, on page 567
- clear app cflowd flow-all, on page 567
- clear app cflowd flows, on page 568
- clear app cflowd statistics, on page 570
- clear app dpi all, on page 570
- clear app dpi apps, on page 571
- clear app dpi flows, on page 573
- clear app log flow-all, on page 574
- clear app log flows, on page 575
- clear arp, on page 577
- clear bfd transitions, on page 578
- clear bgp all, on page 579
- clear bgp neighbor, on page 579
- clear bridge mac, on page 580
- clear bridge statistics, on page 581
- clear cellular errors, on page 581
- clear cellular session statistics, on page 582
- clear cloudexpress computations, on page 583
- clear cloudinit data, on page 584
- clear control connections, on page 584
- clear control connections-history, on page 585
- clear control port-index, on page 586
- clear crash, on page 586
- clear dhcp server-bindings, on page 587
- clear dhcp state, on page 588
- clear dns cache, on page 589

- clear dot1x client, on page 590
- clear history, on page 591
- clear igmp interface, on page 591
- clear igmp protocol, on page 592
- clear igmp statistics, on page 592
- clear installed-certificates, on page 593
- clear interface statistics, on page 595
- clear ip leak routes vpn, on page 596
- clear ip mfib record, on page 596
- clear ip mfib stats, on page 597
- clear ip nat filter, on page 597
- clear ip nat statistics, on page 598
- clear ipv6 dhcp state, on page 599
- clear ipv6 neighbor, on page 600
- clear ipv6 policy, on page 601
- clear omp all, on page 601
- clear omp peer, on page 602
- clear omp routes, on page 604
- clear omp tlocs, on page 604
- clear orchestrator connections-history, on page 605
- clear ospf all, on page 606
- clear ospf database, on page 607
- clear pim interface, on page 607
- clear pim neighbor, on page 608
- clear pim protocol, on page 609
- clear pim rp-mapping, on page 610
- clear pim statistics, on page 611
- clear policer statistics, on page 612
- clear policy, on page 613
- clear policy zbfw filter-statistics, on page 613
- clear policy zbfw global-statistics, on page 614
- clear policy zbfw sessions, on page 614
- clear pppoe statistics, on page 615
- clear reverse-proxy context, on page 616
- clear system statistics, on page 618
- clear tunnel statistics, on page 620
- clear wlan radius-stats, on page 620
- clock, on page 621
- commit, on page 622
- complete-on-space, on page 623
- config, on page 623
- controller-mode, on page 624
- debug, on page 625
- debug packet-trace condition, on page 632
- debug platform condition mpls match-inner, on page 633
- debug-vdaemon, on page 634

- debug vdaemon peer, on page 635
- exit, on page 636
- file list, on page 637
- file show, on page 637
- help, on page 638
- history, on page 639
- idle-timeout, on page 639
- job stop, on page 640
- logout, on page 641
- monitor event-trace sdwan, on page 641
- monitor start, on page 643
- monitor stop, on page 643
- nslookup, on page 644
- paginate, on page 645
- ping, on page 646
- poweroff, on page 648
- prompt1, on page 649
- prompt2, on page 651
- quit, on page 652
- reboot, on page 652
- request aaa unlock-user, on page 654
- request admin-tech, on page 655
- request certificate, on page 658
- request container image install, on page 659
- request container image remove, on page 660
- request control-tunnel add, on page 660
- request control-tunnel delete, on page 661
- request controller add serial-num, on page 661
- request controller delete serial-num, on page 662
- request controller-upload serial-file, on page 663
- request csr upload, on page 664
- request daemon ncs restart, on page 665
- request device, on page 665
- request device-upload, on page 666
- request download, on page 668
- request execute, on page 669
- request firmware upgrade, on page 670
- request interface-reset, on page 670
- request ipsec ike-rekey, on page 671
- request ipsec ipsec-rekey, on page 672
- request nms all, on page 672
- request nms application-server, on page 674
- request nms cluster diagnostics, on page 677
- request nms cluster-orchestrator, on page 679
- request nms configuration-db, on page 681
- request nms coordination-server, on page 683

- request nms messaging-server, on page 684
- request nms olap-db, on page 686
- request nms statistics-db, on page 687
- request nms server-proxy, on page 690
- request nms server-proxy set ratelimit, on page 691
- request on-vbond-controller, on page 692
- request on-vbond-vsmart, on page 692
- request platform software sdwan bootstrap-config save, on page 692
- request port-hop, on page 693
- request reset configuration, on page 694
- request reset logs, on page 697
- request sla-dampening-reset color, on page 698
- request root-ca-crl, on page 699
- request root-cert-chain, on page 700
- request security ipsec-rekey, on page 700
- request software activate, on page 701
- request software install, on page 702
- request software install-image, on page 704
- request software remove, on page 705
- request software reset, on page 706
- request software secure-boot, on page 707
- request software set-default, on page 708
- request software upgrade-confirm, on page 708
- request software verify-image, on page 710
- request stream capture, on page 711
- request upload, on page 712
- request vedge, on page 712
- request vedge-cloud activate, on page 713
- request vsmart add serial-num, on page 714
- request vsmart delete serial-num, on page 714
- request vsmart-upload serial-file, on page 715
- screen-length, on page 716
- screen-width, on page 716
- set platform software trace, on page 717
- show aaa usergroup, on page 718
- show alarms, on page 720
- show app cflowd collector, on page 722
- show app cflowd flow-count, on page 723
- show app cflowd flows, on page 724
- show app cflowd statistics, on page 726
- show app cflowd template, on page 727
- show app dpi applications, on page 728
- show app dpi flows, on page 729
- show app dpi summary statistics, on page 731
- show app dpi supported-applications, on page 732
- show app log flow-count, on page 738

- show app log flows, on page 739
- show app tcp-opt, on page 741
- show app-route sla-class, on page 742
- show app-route stats, on page 744
- show arp, on page 746
- show bfd history, on page 747
- show bfd sessions, on page 748
- show bfd summary, on page 750
- show bfd tloc-summary-list, on page 751
- show bgp neighbor, on page 753
- show bgp routes, on page 755
- show bgp summary, on page 758
- show boot-partition, on page 759
- show bridge interface, on page 760
- show bridge mac, on page 761
- show bridge table, on page 762
- show cellular modem, on page 763
- show cellular network, on page 764
- show cellular profiles, on page 765
- show cellular radio, on page 766
- show cellular sessions, on page 767
- show cellular status, on page 768
- show certificate installed, on page 769
- show certificate reverse-proxy, on page 771
- show certificate root-ca-cert, on page 772
- show certificate root-ca-crl, on page 774
- show certificate serial, on page 775
- show certificate signing-request, on page 776
- show certificate validity, on page 777
- show cli, on page 778
- show clock, on page 779
- show cloudexpress applications, on page 780
- show cloudexpress gateway-exits, on page 781
- show cloudexpress local-exits, on page 782
- show configuration commit list, on page 783
- show container images, on page 784
- show container instances, on page 785
- show control affinity config, on page 786
- show control affinity status, on page 787
- show control connection-info, on page 788
- show control connections, on page 788
- show control connections-history, on page 791
- show control local-properties, on page 794
- show control statistics, on page 799
- show control summary, on page 800
- show control valid-vedges, on page 801

- show control valid-vsmarts, on page 802
- show crash, on page 803
- show crypto pki trustpoints status, on page 804
- show devices, on page 805
- show dhcp interface, on page 806
- show dhcp server, on page 807
- show dot1x clients, on page 808
- show dot1x interfaces, on page 809
- show dot1x radius, on page 810
- show hardware alarms, on page 812
- show hardware environment, on page 813
- show hardware inventory, on page 816
- show hardware poe, on page 817
- show hardware real time information, on page 818
- show hardware temperature-thresholds, on page 820
- show history, on page 821
- show igmp groups, on page 822
- show igmp interface, on page 823
- show igmp statistics, on page 824
- show igmp summary, on page 826
- show interface, on page 827
- show interface arp-stats, on page 833
- show interface description, on page 835
- show interface errors, on page 836
- show interface packet-sizes, on page 840
- show interface port-stats, on page 841
- show interface queue, on page 843
- show interface sfp detail, on page 844
- show interface sfp diagnostic, on page 849
- show interface statistics, on page 851
- show ip dns-snoop, on page 853
- show ip fib, on page 854
- show ip mfib oil, on page 859
- show ip mfib stats, on page 860
- show ip mfib summary, on page 861
- show ip nat filter, on page 862
- show ip nat interface, on page 863
- show ip nat interface-statistics, on page 864
- show ip routes, on page 865
- show ipsec ike inbound-connections, on page 868
- show ipsec ike outbound-connections, on page 870
- show ipsec ike sessions, on page 872
- show ipsec inbound-connections, on page 873
- show ipsec local-sa, on page 874
- show ipsec outbound-connections, on page 875
- show ipv6 dhcp interface, on page 877

- show ipv6 fib, on page 878
- show ipv6 interface, on page 879
- show ipv6 neighbor, on page 882
- show ipv6 policy access-list-associations, on page 882
- show ipv6 policy access-list-counters, on page 883
- show ipv6 policy access-list-names, on page 884
- show ipv6 policy access-list-policers, on page 885
- show ipv6 routes, on page 885
- show jobs, on page 887
- show licenses, on page 888
- show log, on page 890
- show logging, on page 891
- show logging process, on page 892
- show logging profile sdwan, on page 893
- show monitor event-trace sdwan, on page 896
- show multicast replicator, on page 897
- show multicast rpf, on page 899
- show multicast topology, on page 900
- show multicast tunnel, on page 901
- show nms-server running, on page 902
- show notification stream, on page 903
- show ntp associations, on page 904
- show ntp peer, on page 905
- show omp cloudexpress, on page 906
- show omp multicast-auto-discover, on page 907
- show omp multicast-routes, on page 909
- show omp peers, on page 910
- show omp routes, on page 914
- show omp services, on page 919
- show omp summary, on page 921
- show omp tlocs, on page 924
- show omp verify-routes, on page 928
- show orchestrator connections, on page 930
- show orchestrator connections-history, on page 932
- show orchestrator local-properties, on page 935
- show orchestrator reverse-proxy-mapping, on page 937
- show orchestrator statistics, on page 937
- show orchestrator summary, on page 939
- show orchestrator valid-vedges, on page 940
- show orchestrator valid-vmanage-id, on page 941
- show orchestrator valid-vsmarts, on page 942
- show ospf database, on page 943
- show ospf database-summary, on page 944
- show ospf interface, on page 945
- show ospf neighbor, on page 947
- show ospf process, on page 948

- show ospf routes, on page 950
- show packet-capture, on page 952
- show packet-trace, on page 953
- show parser dump, on page 955
- show pim interface, on page 956
- show pim neighbor, on page 957
- show pim rp-mapping, on page 958
- show pim statistics, on page 959
- show platform resources, on page 960
- show platform software trace level, on page 961
- show policer, on page 963
- show policy access-list-associations, on page 964
- show policy access-list-counters, on page 965
- show policy access-list-names, on page 966
- show policy access-list-policers, on page 967
- show policy data-policy-filter, on page 968
- show policy ef-stats, on page 970
- show policy from-vsmart, on page 971
- show policy service-path, on page 973
- show policy tunnel-path, on page 974
- show policy zbfw filter-statistics, on page 975
- show policy zbfw global-statistics, on page 976
- show policy zbfw sessions, on page 980
- show ppp interface, on page 981
- show pppoe session, on page 981
- show pppoe statistics, on page 982
- show reboot history, on page 983
- show running-config, on page 984
- show sdwan, on page 987
- show sdwan alarms detail, on page 988
- show sdwan alarms summary, on page 989
- show sdwan appqoe, on page 990
- show sdwan appqoe flow closed, on page 994
- show sdwan appqoe flow flow-id, on page 995
- show sdwan appqoe flow vpn-id, on page 997
- show sdwan cloudexpress applications, on page 997
- show sdwan cloudexpress gateway-exits, on page 998
- show sdwan cloudexpress local-exits, on page 999
- show sdwan cloudexpress service-area-applications, on page 1000
- show sdwan policy, on page 1001
- show sdwan policy service-path, on page 1002
- show sdwan policy tunnel-path, on page 1004
- show security-info, on page 1005
- show nms server-proxy ratelimit, on page 1006
- show software, on page 1006
- show support omp peer, on page 1007

- show system buffer-pool-status, on page 1011
- show system netfilter, on page 1012
- show system on-demand, on page 1013
- show system statistics, on page 1015
- show system status, on page 1019
- show tech-support, on page 1023
- show tenant-mapping, on page 1025
- show tenant omp peers, on page 1026
- show tenant omp routes, on page 1027
- show tenant-summary, on page 1028
- show transport connection, on page 1029
- show tunnel gre-keepalives, on page 1030
- show tunnel inbound-connections, on page 1031
- show tunnel local-sa, on page 1032
- show tunnel statistics, on page 1033
- show umbrella deviceid, on page 1034
- show uptime, on page 1035
- show users, on page 1036
- show version, on page 1036
- show vrrp, on page 1037
- show wlan clients, on page 1038
- show wlan interfaces, on page 1039
- show wlan radios, on page 1040
- show wlan radius, on page 1042
- show ztp entries, on page 1043
- tcpdump, on page 1044
- test policy match control-policy , on page 1045
- timestamp, on page 1048
- tools ip-route, on page 1048
- tools iperf, on page 1049
- tools minicom, on page 1051
- tools netstat, on page 1052
- tools nping, on page 1054
- tools ss, on page 1062
- tools stun-client, on page 1064
- traceroute, on page 1066
- vshell, on page 1068

Overview of Operational Commands

The operational command reference pages describe the CLI commands that you use to display the properties and operational status of vSmart controllers, vEdge routers, and vBond orchestrators in the overlay network. When you log in to the CLI on a Cisco vEdge device, you are in operational mode.

In the CLI, operational commands are organized alphabetically, and many commands are organized into functional hierarchies. The top-level operational commands and command hierarchies are:

- clear—Zero or erase information stored on the device or collected data.
- clock—Set the time.
- commit—Confirm a pending commit operation.
- complete-on-space—Enable the ability to type a space to have the CLI complete unambiguous commands.
- config—Enter configuration mode.
- exit—Configure basic system parameters.
- file—Configure the properties of a VPN, including the interfaces that participate in the VPN and the routing protocols that are enabled in the VPN.
- help—Display help information about CLI commands.
- history—Control the CLI command history cache.
- idle-timeout—Set how long a CLI session can be idle before the user is logged out.
- logout—Exit from the CLI session.
- no—Negate or cancel a command.
- nslookup—Perform a DNS name lookup.
- paginate—Set the number of lines of command output to display.
- ping—Ping a network device.
- poweroff—Power down the device.
- prompt1—Set the operational mode prompt.
- prompt2—Set the configuration mode prompt.
- pwd—Display the current path mode.
- quit—Exit from the CLI session.
- reboot—Reboot the device.
- request—Install various files onto the device.
- screen-length—Set the CLI screen length.
- screen-width—Set the CLI screen width.
- show—Display information about the status of the device or information stored on the device.
- tcpdump—Perform a TCP dump operation.
- timestamp—Enable timestamping.
- traceroute—Perform a traceroute operation.
- vshell—Exit to the shell on the device.

To filter operational command output, use the filters described in Command Filters for CLI Operational Commands.

clear aaa login

Use the **clear aaa login** command in privileged EXEC mode on an SD-WAN Manager, Controller, or Validator host to close a user CLI session opened by Telnet or SSH.

clear aaa login *session*

Syntax Description

session	Session ID of the session to close. Use the **show users command** on an SD-WAN Manager, Controller, or Validator host to list all active user sessions.

Command Default

The command has no default.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.18.1	The command was introduced.

Usage Guidelines

To close a user session, execute the show users command on an SD-WAN Manager, Controller, or Validator host to list all active user CLI sessions, with session numbers. Find the session to close. Use the **clear aaa login** command to close the session.

Example

This closes user session 10020 on an SD-WAN Manager instance.

```
manager# clear aaa login 10020
Connection to 10.0.1.1 closed by remote host.
Connection to 10.0.1.1 closed.
```

clear app cflowd flow-all

Clear the cflowd flows in all VPNs (on vEdge routers only).

clear app cflowd flow-all

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# show cflowd flows
                                                                    TCP
```

```
                                        SRC    DEST         IP     CNTRL  ICMP             EGRESS
      INGRESS     TOTAL  TOTAL  MIN  MAX  START   TIME TO
VPN   SRC IP      DEST IP        PORT   PORT   DSCP  PROTO  BITS   OPCODE  NHOP IP  INTF
      INTF        PKTS   BYTES  LEN  LEN  TIME    EXPIRE
-------------------------------------------------------------------------------------------------------
1    10.20.24.15  172.16.255.15  49142  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          3745446565
1    10.20.24.15  172.16.255.15  49143  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          4
1    10.20.24.15  172.16.255.15  49144  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          9
1    10.20.24.15  172.16.255.15  49145  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          14
1    10.20.24.15  172.16.255.15  49146  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          19
1    10.20.24.15  172.16.255.15  49147  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          24
1    10.20.24.15  172.16.255.15  49148  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          29
1    10.20.24.15  172.16.255.15  49149  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          34
1    10.20.24.15  172.16.255.15  49150  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          39
1    10.20.24.15  172.16.255.15  49151  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          44
1    10.20.24.15  172.16.255.15  49152  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          49
1    10.20.24.15  172.16.255.15  49153  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          54
1    10.20.24.15  172.16.255.15  49154  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78          59

vEdge# clear app cflowd flow-all
vEdge# show app cflow flows
%  No entries found.
vEdge#
```

Related Topics

cflowd-template, on page 121
clear app cflowd flows, on page 568
show app cflowd flows, on page 724

clear app cflowd flows

Clear the cflowd flows in a specific VPN (on vEdge routers only).

clear app cflowd flows vpn *vpn-id* [*flow-property*]

Syntax Description

flow-property	Specific Flow To Clear: Narrow down the exact flow to clear. *flow-property* can be one of: **dest-ip** *prefix/length* **dest-port** *port-number*(0 through 65535) **dscp** *dscp-value*(0 through 255) **ip-proto** *protocol-number*(0 through 255) **src-ip** *prefix/length* **src-port** *port-number*(0 through 65535)
vpn *vpn-id*	VPN: Specify the VPN in which to clear all cflowd flows.

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# show cflowd flows
                                                                    TCP

                                    SRC    DEST         IP     CNTRL  ICMP             EGRESS
      INGRESS     TOTAL  TOTAL  MIN  MAX  START   TIME TO
VPN   SRC IP      DEST IP        PORT   PORT   DSCP  PROTO  BITS   OPCODE  NHOP IP  INTF
      INTF        PKTS   BYTES  LEN  LEN  TIME    EXPIRE
-------------------------------------------------------------------------------------------------
1    10.20.24.15  172.16.255.15  49142  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           3745446565
1    10.20.24.15  172.16.255.15  49143  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           4
1    10.20.24.15  172.16.255.15  49144  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           9
1    10.20.24.15  172.16.255.15  49145  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           14
1    10.20.24.15  172.16.255.15  49146  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           19
1    10.20.24.15  172.16.255.15  49147  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           24
1    10.20.24.15  172.16.255.15  49148  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           29
1    10.20.24.15  172.16.255.15  49149  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           34
1    10.20.24.15  172.16.255.15  49150  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           39
1    10.20.24.15  172.16.255.15  49151  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           44
1    10.20.24.15  172.16.255.15  49152  13322  0     6      2      0       0.0.0.0  4294967295
```

```
  4294967295  1      78     78   78           49
1    10.20.24.15  172.16.255.15  49153  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           54
1    10.20.24.15  172.16.255.15  49154  13322  0     6      2      0       0.0.0.0  4294967295
  4294967295  1      78     78   78           59

vEdge# clear app cflowd flows vpn 1
vEdge# show app cflow flows
%  No entries found.
vEdge#
```

Related Topics

cflowd-template, on page 121
clear app cflowd flow-all, on page 567
show app cflowd flows, on page 724

clear app cflowd statistics

Zero cflowd packet statistics (on vEdge routers only).

clear app cflowd statistics

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# show app cflowd statistics
      data_pkts                :      539
      template_pkts            :      15
      total-pkts               :      0
      flow-refresh             :      269
      flow-ageout              :      270
vEdge# clear app cflowd statistics
vEdge# show app cflowd statistics
      data_pkts                :      2
      template_pkts            :      0
      total-pkts               :      0
      flow-refresh             :      1
      flow-ageout              :      1
```

Related Topics

cflowd-template, on page 121
show app cflowd statistics, on page 726

clear app dpi all

Clear all DPI flows on the vEdge router (on vEdge routers only).

clear app dpi all

Command History

Release	Modification
15.2	Command introduced.

Examples

```
vEdge# show app dpi flows

                                    Source  Dest

VPN  SRC IP          DST IP         Port    Port   Protocol  APPLICATION  FAMILY
  ACTIVE SINCE
-------------------------------------------------------------------------------------------------------------
1    10.192.42.2     74.125.20.95   20581   443    udp       unknown      Standard
  2015-05-04T14:07:46+00:00
1    10.192.42.2     74.125.25.188  55742   5228   tcp       gtalk        Instant Messaging
  2015-05-03T21:06:57+00:00
1    10.192.42.2     74.125.28.95   36597   443    tcp       google       Web
  2015-05-04T14:12:43+00:00
1    10.192.42.2     74.125.28.95   36598   443    tcp       google       Web
  2015-05-04T14:12:45+00:00
1    10.192.42.2     192.168.15.3   63665   53     udp       dns          Network Service
  2015-05-04T14:14:40+00:00
1    10.192.42.2     216.58.192.14  40616   443    tcp       https        Web
  2015-05-04T14:12:02+00:00
1    10.192.42.2     216.58.192.36  45889   443    tcp       https        Web
  2015-05-04T14:14:40+00:00
1    10.192.42.2     216.58.192.36  45903   443    tcp       https        Web
  2015-05-04T14:14:40+00:00
1    10.192.42.2     216.115.20.77  10000   10000  udp       sip          Audio/Video
  2015-05-03T08:22:51+00:00
1    192.168.20.83   1.1.42.1       51586   22     tcp       ssh          Encrypted
  2015-05-04T13:28:03+00:00

vEdge# clear app dpi all
vEdge# show app dpi flows
% No entries found.
vEdge#
```

Related Topics

app-visibility, on page 69
clear app dpi apps, on page 571
clear app dpi flows, on page 573
show app dpi applications, on page 728
show app dpi flows, on page 729
show app dpi supported-applications, on page 732

clear app dpi apps

Clear specific applications in a particular VPN on the vEdge router (on vEdge routers only).

clear app dpi apps vpn *vpn-id* [**application** *name*] [**source-prefix** *prefix* | *length*]

Syntax Description

application *name*	Application Name: Name of the application to clear.
source-prefix *prefix*|*length*	Source IP address: Source IP prefix for the application or applications to clear.
vpn *vpn-id*	VPN: VPN in which the application participates.

Command History

Release	Modification
15.2	Command introduced.

Examples

```
vEdge# show app dpi applications

VPN  SRC IP       APPLICATION         FAMILY
-------------------------------------------------------------
1    2.51.88.142  bittorrent          Peer to Peer
1    10.192.42.1  syslog              Application Service
1    10.192.42.1  tcp                 Network Service
1    10.192.42.1  unknown             Standard
1    10.192.42.2  addthis             Web
1    10.192.42.2  adobe               Web
1    10.192.42.2  adobe_update        Web
1    10.192.42.2  akamai              Web
1    10.192.42.2  alexa               Web
1    10.192.42.2  alibaba             Web
1    10.192.42.2  aliexpress          Web
1    10.192.42.2  amazon              Web
1    10.192.42.2  amazon_adsystem     Web
1    10.192.42.2  amazon_aws          Web
1    10.192.42.2  amazon_cloud_drive  Web
1    10.192.42.2  aol                 Web
1    10.192.42.2  apple               Web
...

vEdge# clear app dpi apps vpn 1 application aol
vEdge# show app dpi applications

VPN  SRC IP       APPLICATION         FAMILY
-------------------------------------------------------------
1    2.51.88.142  bittorrent          Peer to Peer
1    10.192.42.1  syslog              Application Service
1    10.192.42.1  tcp                 Network Service
1    10.192.42.1  unknown             Standard
1    10.192.42.2  addthis             Web
1    10.192.42.2  adobe               Web
1    10.192.42.2  adobe_update        Web
```

```
1     10.192.42.2  akamai              Web
1     10.192.42.2  alexa               Web
1     10.192.42.2  alibaba             Web
1     10.192.42.2  aliexpress          Web
1     10.192.42.2  amazon              Web
1     10.192.42.2  amazon_adsystem     Web
1     10.192.42.2  amazon_aws          Web
1     10.192.42.2  amazon_cloud_drive  Web
1     10.192.42.2  apple               Web
...
```

Related Topics

app-visibility, on page 69
clear app dpi all, on page 570
clear app dpi flows, on page 573
show app dpi applications, on page 728
show app dpi flows, on page 729
show app dpi supported-applications, on page 732

clear app dpi flows

Clear specific DPI flows in a particular VPN on the vEdge router (on vEdge routers only).

clear app dpi flows vpn *vpn-id* [**destination-prefix** *prefix/length*] [**destination-port** *number*] [**ip-protocol** *protocol*] [**source-prefix** *prefix/length*] [**src-port** *number*]

Syntax Description

destination-prefix *prefix/length* **source-prefix** *prefix/length*	IP Prefix: Destination or source IP prefix of the flow.
destination-port *number* **source-port** *number*	Port Number: Destination or source port number of the flow.
ip-protocol *protocol*	Protocol: Destination or source port number of the flow.
vpn *vpn-id*	VPN: VPN in which the flow participates.

Command History

Release	Modification
15.2	Command introduced.

Examples

```
vEdge# show app dpi flows

                                    Source  Dest

VPN  SRC IP         DST IP         Port    Port   PROTOCOL  APPLICATION  FAMILY
  ACTIVE SINCE
-------------------------------------------------------------------------------------------------------------
1    10.192.42.2    74.125.20.95   20581   443    udp       unknown      Standard
  2015-05-04T14:07:46+00:00
1    10.192.42.2    74.125.25.188  55742   5228   tcp       gtalk        Instant Messaging
  2015-05-03T21:06:57+00:00
1    10.192.42.2    74.125.28.95   36597   443    tcp       google       Web
  2015-05-04T14:12:43+00:00
1    10.192.42.2    74.125.28.95   36598   443    tcp       google       Web
  2015-05-04T14:12:45+00:00
1    10.192.42.2    192.168.15.3   63665   53     udp       dns          Network Service
  2015-05-04T14:14:40+00:00
1    10.192.42.2    216.58.192.14  40616   443    tcp       https        Web
  2015-05-04T14:12:02+00:00
1    10.192.42.2    216.58.192.36  45889   443    tcp       https        Web
  2015-05-04T14:14:40+00:00
1    10.192.42.2    216.58.192.36  45903   443    tcp       https        Web
  2015-05-04T14:14:40+00:00
1    10.192.42.2    216.115.20.77  10000   10000  udp       sip          Audio/Video
  2015-05-03T08:22:51+00:00
1    192.168.20.83  1.1.42.1       51586   22     tcp       ssh          Encrypted
  2015-05-04T13:28:03+00:00

vEdge# clear app dpi flows vpn 1
vEdge# show app dpi flows
% No entries found.
vEdge#
```

Related Topics

app-visibility, on page 69
clear app dpi all, on page 570
clear app dpi apps, on page 571
show app dpi applications, on page 728
show app dpi flows, on page 729
show app dpi supported-applications, on page 732

clear app log flow-all

Clear all logged flows(on vEdge routers only).

clear app log flow-all

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show app log flow-count

VPN   COUNT
------------
0     7

vEdge# clear app log flow-all
vEdge# show app log flow-count
% No entries found.
vEdge#
```

Related Topics

clear app log flows, on page 575
log-frequency, on page 295
clear app log flow-all, on page 574
show app log flows, on page 739
show system statistics, on page 1015

clear app log flows

Clear the information logged about flows (on vEdge routers only). After you issue this command, collection of information about the flow resumes immediately.

clear app log flows [**dest-ip** *prefix*] [**dest-port** *number*] [**ip-proto** *number*] [**src-ip** *prefix*] [**src-port** *number*] **vpn** *vpn-id*

Syntax Description

none	Clear information logged about all flows on the router.
dest-ip *prefix*	Destination IP Prefix: Clear information logged about flows with the specified destination IP prefix.
dest-port *number*	Destination Port Number: Clear information logged about flows with the specified destination port number.
ip-protocol *number*	IP Protocol: Clear information logged about flows with the specified IP protocol number.
src-ip *prefix*	Source IP Prefix: Clear information logged about flows with the specified source IP prefix.
src-port *number*	Source Port Number: Clear information logged about flows with the specified source port number.
vpn *vpn-id*	Specific VPN: Clear the logged flows in the specified VPN.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show app log flows | tab

                                                                  TCP
                                    TIME    EGRESS  INGRESS
                                SRC     DEST        IP      CNTRL  ICMP                TOTAL
TOTAL                               TO      INTF    INTF      POLICY     POLICY  POLICY
VPN  SRC IP       DEST IP     PORT    PORT    DSCP  PROTO   BITS   OPCODE  NHOP IP     PKTS
BYTES  START TIME                   EXPIRE  NAME    NAME      NAME       ACTION  DIRECTION
-------------------------------------------------------------------------------------------------------------------
0    10.0.5.11    10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  102
28942  Thu Dec  8 11:42:38 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.5.11    10.1.15.15  12366  12366  48    17      0      0       10.1.15.15  10
1910   Thu Dec  8 11:42:28 2016  14      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.5.19    10.1.15.15  12446  12346  48    17      0      0       10.1.15.15  73
17458  Thu Dec  8 11:42:34 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.5.21    10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  102
28942  Thu Dec  8 11:42:38 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.5.21    10.1.15.15  12366  12366  48    17      0      0       10.1.15.15  11
2101   Thu Dec  8 11:42:28 2016  15      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.12.20   10.1.15.15  12446  12346  48    17      0      0       10.1.15.15  76
17887  Thu Dec  8 11:42:34 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.12.26   10.1.15.15  0      0      0     1       0      0       10.1.15.15  17
1666   Thu Dec  8 11:42:33 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.12.26   10.1.15.15  12346  12346  48    17      0      0       10.1.15.15  28
7167   Thu Dec  8 11:42:33 2016  28      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.14.14   10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  106
32230  Thu Dec  8 11:42:38 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.14.14   10.1.15.15  12366  12366  48    17      0      0       10.1.15.15  11
2101   Thu Dec  8 11:42:28 2016  15      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.16.16   10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  102
28942  Thu Dec  8 11:42:38 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.16.16   10.1.15.15  12366  12366  48    17      0      0       10.1.15.15  11
2101   Thu Dec  8 11:42:28 2016  15      cpu     ge0/0     BlackBird  accept  inbound-acl

vEdge# clear app log flows
Value for 'vpn' (<0..65530>): 0
vEdge# show app log flows | tab

                                                                  TCP
                                    TIME    EGRESS  INGRESS
                                SRC     DEST        IP      CNTRL  ICMP                TOTAL
TOTAL                               TO      INTF    INTF      POLICY     POLICY  POLICY
VPN  SRC IP       DEST IP     PORT    PORT    DSCP  PROTO   BITS   OPCODE  NHOP IP     PKTS
BYTES  START TIME                   EXPIRE  NAME    NAME      NAME       ACTION  DIRECTION
-------------------------------------------------------------------------------------------------------------------
0    10.0.5.11    10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  3
573    Thu Dec  8 11:43:33 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.0.5.21    10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  3
573    Thu Dec  8 11:43:33 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.14.14   10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  3
573    Thu Dec  8 11:43:33 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
0    10.1.16.16   10.1.15.15  12366  12346  48    17      0      0       10.1.15.15  3
573    Thu Dec  8 11:43:33 2016  59      cpu     ge0/0     BlackBird  accept  inbound-acl
```

Related Topics

clear app log flow-all, on page 574
log-frequency, on page 295
show app log flow-count, on page 738
show app log flows, on page 739
show system statistics, on page 1015

clear arp

Refresh dynamically created IPv4 entries in the Address Resolution Protocol (ARP) cache (on vEdge routers and vSmart controllers only).

To clear IPv6 entries in the ARP cache, use the **clear ipv6 neighbor** command.

clear arp [**interface** *interface-name*] [*ip-address*] [**vpn** *vpn-id*]

Syntax Description

none	Refresh all dynamic ARP cache entries.
interface *interface-name*	Interface: Refresh the dynamic ARP cache entries associated with the specific interface.
ip-address	IP Address: Refresh the dynamic ARP cache entries for the specified IP address.
vpn *vpn-id*	VPN: Refresh the dynamic ARP cache entries for the specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show arp
     IF
VPN  NAME   IP           MAC                STATE    IDLE TIMER  UPTIME
-------------------------------------------------------------------------------
0    ge0/0  10.0.11.1    00:0c:29:86:ea:83  static   0:00:00:00  0:13:02:02
0    ge0/7  10.0.100.11  00:0c:29:86:ea:c9  static   0:00:00:00  0:13:03:58
512  eth0   10.0.1.1     00:50:56:c0:00:01  dynamic  0:00:13:34  0:00:15:25
512  eth0   10.0.1.11    00:50:56:00:01:01  static   0:00:00:00  0:13:04:22
512  eth0   10.0.1.254   00:50:56:fe:2a:d4  dynamic  0:00:19:34  0:00:03:25

vEdge# clear arp entries
vEdge# show arp
     IF
VPN  NAME   IP           MAC                STATE   IDLE TIMER  UPTIME
```

```
------------------------------------------------------------------------------
0    ge0/0  10.0.11.1    00:0c:29:86:ea:83  static  0:00:00:00  0:13:02:08
0    ge0/7  10.0.100.11  00:0c:29:86:ea:c9  static  0:00:00:00  0:13:04:04
512  eth0   10.0.1.11    00:50:56:00:01:01  static  0:00:00:00  0:13:04:29
```

Related Topics

clear ipv6 neighbor, on page 600
show arp, on page 746
show ipv6 neighbor, on page 882

clear bfd transitions

Clear the counters for BFD transitions (on vEdge routers only).

clear bfd transitions

Command History

Release	Modification
15.1.1	Command introduced.

Examples

```
vEdge# show bfd sessions system-ip 1.1.1.1
                                        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

------------------------------------------------------------------------------------------------------------------------
1.1.1.1          1        up          default          public-internet  192.168.1.104
69.181.135.19    34601       ipsec  3           1000           3:17:22:43      5

vEdge# clear bfd transitions
vEdge# show bfd sessions system-ip 1.1.1.1
                                        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

------------------------------------------------------------------------------------------------------------------------
1.1.1.1          1        up          default          public-internet  192.168.1.104
69.181.135.19    34601       ipsec  3           1000           3:17:22:43      0
```

Related Topics

bfd color, on page 106
show bfd history, on page 747
show bfd sessions, on page 748

clear bgp all

Reset BGP peering sessions with all neighbors in a specific VPN (on vEdge routers only).

clear bgp all vpn *vpn-id*

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show bgp neighbor vpn 1
                         MSG   MSG   OUT
VPN   PEER ADDR    AS    RCVD  SENT  Q    UPTIME      STATE        AFI
-------------------------------------------------------------------------------
1     10.20.25.16  1     4884  4892  0    0:00:18:31  established  ipv4-unicast

vEdge# clear bgp all vpn 1
vEdge# show bgp neighbor vpn 1
                         MSG   MSG   OUT
VPN   PEER ADDR    AS    RCVD  SENT  Q    UPTIME  STATE  AFI
-----------------------------------------------------------------
1     10.20.25.16  1     4895  4904  0    -       idle   ipv4-unicast
```

Related Topics

clear bgp neighbor, on page 579
show bgp neighbor, on page 753

clear bgp neighbor

Reset the peering sessions with a specific BGP neighbor in a VPN (on vEdge routers only).

clear bgp neighbor *ip-address* **vpn** *vpn-id* [**soft** (**in** | **out**)]

Syntax Description

*ip-address***vpn** *vpn-id*	Neighbor Address and VPN: Reset the connection to the specific BGP neighbor in the specified VPN.
soft (in | out)	Soft Reset: Perform a reset when the routing policy changes so that the new policy can take effect. With a soft reset, the route table is reconfigured and reactivated, but the BGP session itself is not reset. Use the **in** option to generate inbound route table updates from the BGP neighbor, and use the **out** option to have the local router send a new set of updated to the BGP neighbor.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# clear bgp neighbor 10.20.25.16 vpn 1
vEdge# show bgp neighbor

                     MSG   MSG   OUT
VPN  PEER ADDR    AS RCVD  SENT  Q    UPTIME  STATE  AFI
-------------------------------------------------------------------
1    10.20.25.16  1  8102  8122  0    -       idle   ipv4-unicast

vEdge# show bgp neighbor
                     MSG   MSG   OUT
VPN  PEER ADDR    AS RCVD  SENT  Q    UPTIME      STATE        AFI
-------------------------------------------------------------------------------
1    10.20.25.16  1  7971  7988  0    0:00:48:56  established  ipv4-unicast

vEdge# clear bgp neighbor 10.20.25.16 vpn 1 soft out
vEdge# show bgp neighbor
VPN  PEER ADDR    AS RCVD  SENT  Q    UPTIME      STATE        AFI
-------------------------------------------------------------------------------
1    10.20.25.16  1  7986  8004  0    0:00:49:12  established  ipv4-unicast
```

Related Topics

clear bgp all, on page 579
show bgp neighbor, on page 753

clear bridge mac

Clear the MAC addresses that this vEdge router has learned (on vEdge routers only). The router restarts its MAC address learning process, performing flooding until all the MAC addresses are relearned.

clear bridge mac

Command History

Release	Modification
15.3	Command introduced.

Examples

```
vEdge# show bridge mac

                                                  RX    RX      TX    TX
BRIDGE  INTERFACE  MAC ADDR           STATE       PKTS  OCTETS  PKTS  OCTETS
-------------------------------------------------------------------------
1       ge0/5      aa:01:05:05:00:01  dynamic     2     248     0     0
1       ge0/5      aa:01:05:05:00:02  dynamic     2     248     0     0
```

```
1       ge0/5      aa:01:05:05:00:03  dynamic  2     248     0     0
1       ge0/5      aa:01:05:05:00:04  dynamic  2     248     0     0
1       ge0/5      aa:01:05:05:00:05  dynamic  2     248     0     0
2       ge0/5      aa:02:05:05:00:01  dynamic  2     248     0     0
2       ge0/5      aa:02:05:05:00:02  dynamic  2     248     0     0
2       ge0/5      aa:02:05:05:00:03  dynamic  2     248     0     0
2       ge0/5      aa:02:05:05:00:04  dynamic  1     124     0     0
2       ge0/5      aa:02:05:05:00:05  dynamic  1     124     0     0

vEdge# clear bridge mac
vEdge# show bridge mac
% No entries
vEdge#
```

Related Topics

bridge, on page 115
show bridge mac, on page 761

clear bridge statistics

Clear the bridging statistics (on vEdge routers only).

clear bridge statistics

Command History

Release	Modification
15.3	Command introduced.

Related Topics

bridge, on page 115
clear bridge mac, on page 580
show bridge interface, on page 760
show bridge mac, on page 761
show bridge table, on page 762

clear cellular errors

Clear errors associated with cellular interfaces (on vEdge routers only).

clear cellular errors

Command History

Release	Modification
16.1	Command introduced.

Examples

```
vEdge# show cellular status
           MODEM   SIM     SIGNAL     NETWORK
INTERFACE  STATUS  STATUS  STRENGTH   STATUS     LAST SEEN ERROR
-------------------------------------------------------------------------
cellular0  Online  Ready   Excellent  Registered  Device has no service

vEdge# clear cellular errors
vEdge# show cellular status
           MODEM   SIM     SIGNAL     NETWORK
INTERFACE  STATUS  STATUS  STRENGTH   STATUS     LAST SEEN ERROR
-------------------------------------------------------------------------
cellular0  Online  Ready   Excellent  Registered None
```

Related Topics

cellular, on page 119
clear cellular session statistics, on page 582
profile, on page 403
show cellular modem, on page 763
show cellular network, on page 764
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

clear cellular session statistics

Clear the statistics for cellular sessions (on vEdge routers only).

clear cellular session statistics

Command History

Release	Modification
16.1	Command introduced.

Examples

```
vEdge# clear cellular session statistics
vEdge# show cellular session statistics
            SESSION  DATA     DORMANCY  ACTIVE    RX        RX      RX       RX          TX
 TX      TX       TX          RX        TX                  IPV4                IPV4 DNS
INTERFACE  ID       BEARER   STATE     PROFILE   PACKETS   DROPS   ERRORS   OVERFLOWS   PACKETS
 DROPS   ERRORS   OVERFLOWS   OCTETS    OCTETS    IPV4 ADDR  MASK    IPV4 GW       PRI
IPV4 DNS SEC
-------------------------------------------------------------------------------------------------------------------------------
cellular0  0        LTE      Active    1         0          0       0        0           0
 0       0       0           0         0         10.12.15.6  30     10.12.15.5    10.12.15.1
255.255.255.255
```

Related Topics

clear cellular errors, on page 581
show cellular modem, on page 763
show cellular network, on page 764
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

clear cloudexpress computations

Clear the computations performed by Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only). Cloud OnRamp for SaaS computations include application loss, latency, and best interface.

clear cloudexpress computations [**application** *application*]

Syntax Description

(none)	Clear all computations for all applications in all VPNs configured with Cloud OnRamp for SaaS.
application	Specific Application: Clear computations for a specific application configured for Cloud OnRamp for SaaS. Values: amazon_aws, box_net, concur, dropbox, google_apps, gotomeeting, intuit, jira, office365, oracle, salesforce, sap, sugar_crm, webex, zendesk, zoho_crm

Command History

Release	Modification
16.3	Command introduced.
17.1	Removed **vpn** command option.

Examples

Clear the Cloud OnRamp for SaaS computations

```
vEdge# show cloudexpress applications
                                      GATEWAY
                                EXIT  SYSTEM
VPN  APPLICATION                TYPE  IP       INTERFACE  LATENCY  LOSS
-------------------------------------------------------------------------
100  salesforce                 local -        ge0/2      81       1
100  office365                  local -        ge0/2      61       1
100  amazon_aws                 local -        ge0/2      105      2
100  oracle                     local -        ge0/0      79       1
100  sap                        local -        ge0/2      61       1
100  box_net                    local -        ge0/0      18       1
100  dropbox                    local -        ge0/2      30       1
```

```
100  jira                 local  -        ge0/0      83       2
100  intuit               local  -        ge0/0      35       3
100  concur               local  -        ge0/2      62       1
100  zoho_crm             local  -        ge0/0      14       1
100  zendesk              local  -        ge0/2      6        0
100  gotomeeting          local  -        ge0/0      13       1
100  webex                local  -        ge0/0      69       2
100  google_apps          local  -        ge0/0      19       0

vEdge# clear cloudexpress computations
vEdge# show cloudexpress applications
                                  GATEWAY
                             EXIT SYSTEM
VPN  APPLICATION             TYPE IP       INTERFACE  LATENCY  LOSS
-------------------------------------------------------------------
100  salesforce              none -        -          0        0
100  office365               none -        -          0        0
100  amazon_aws              none -        -          0        0
100  oracle                  none -        -          0        0
100  sap                     none -        -          0        0
100  box_net                 none -        -          0        0
100  dropbox                 none -        -          0        0
100  jira                    none -        -          0        0
100  intuit                  none -        -          0        0
100  concur                  none -        -          0        0
100  zoho_crm                none -        -          0        0
100  zendesk                 none -        -          0        0
100  gotomeeting             none -        -          0        0
100  webex                   none -        -          0        0
100  google_apps             none -        -          0        0
```

Related Topics

show cloudexpress local-exits, on page 782

clear cloudinit data

Clear bootstrap information received from cloud-init in order to attach a new cloud-init file. Cloud-init information includes a token, vBond orchestrator IP address, and organization name (on vEdge Cloud routers only).

clear cloudinit data

Command History

Release	Modification
17.1	Command introduced.

clear control connections

Reset the DTLS connections from the local device to all Cisco SD-WAN devices.

clear control connections

Note This command will reset all the Bidirectional Forwarding Detection (BFD) tunnels on the device.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vSmart# show control connections
                                                                                  PEER                  PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER                  PRIVATE  PEER         PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP            PORT     PUBLIC IP    PORT   REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------------
vedge    dtls     172.16.255.14    400         1           10.1.14.14            12350    10.1.14.14   12350  lte              up              0:14:01:50
vedge    dtls     172.16.255.15    500         1           10.1.15.15            12346    10.1.15.15   12346  lte              up              0:00:01:58
vedge    dtls     172.16.255.16    600         1           10.1.16.16            12346    10.1.16.16   12346  lte              up              0:14:01:47
vsmart   dtls     172.16.255.20    200         1           10.0.12.20            12346    10.0.12.20   12346  default          up              0:14:01:37
vbond    dtls     -                0           0           10.1.14.14            12346    10.1.14.14   12346  default          up              0:14:01:54
vmanage  dtls     172.16.255.22    200         1           10.0.12.22            12346    10.0.12.22   12346  default          up              0:14:01:43

vSmart# clear control connections
vSmart# show control connections
                                                                                  PEER                  PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER                  PRIVATE  PEER         PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP            PORT     PUBLIC IP    PORT   REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------------
vsmart   dtls     172.16.255.20    200         1           10.0.12.20            12346    10.0.12.20   12346  default          up              0:00:00:02
vbond    dtls     -                0           0           10.1.14.14            12346    10.1.14.14   12346  default          up              0:00:00:03
vmanage  dtls     172.16.255.22    200         1           10.0.12.22            12346    10.0.12.22   12346  default          up              0:00:00:02

Release Information Edit section
```

Related Topics

clear omp all, on page 601
show control connections, on page 788
show omp peers, on page 910

clear control connections-history

Erase the connection history on the local device.

clear control connections-history

Examples

```
vEdge# show control connections-history

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.                ORPTMO    - Server's peer timed out.
BIDNTVRFD   - Peer Board ID Cert not verified.         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.         SSLNFAIL  - Failure to create new SSL context.
CTORGNMMIS  - Certificate Org name mismatch.           SERNTPRES - Serial Number not present.
DCONFAIL    - DTLS connection failure.                 SYSIPCHNG - System-IP changed.
DEVALC      - Device memory Alloc failures.            TMRALC    - Memory Failure.
DHSTMO      - DTLS HandShake Timeout.                  TUNALC    - Memory Failure.
DISCVBD     - Disconnect vBond after register reply.   TXCHTOBD  - Failed to send challenge to BoardID.
DISTLOC     - TLOC Disabled.                           UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSER      - Duplicate Serial Number.                 UNAUTHEL  - Recd Hello from Unauthenticated peer.
DUPCLHELO   - Recd a Dup Client Hello, Reset Gl Peer.  VBDEST    - vDaemon process terminated.
HAFAIL      - SSL Handshake failure.                   VECRTREV  - vEdge Certification revoked.
IP_TOS      - Socket Options failure.                  VSCRTREV  - vSmart Certificate revoked.
LISFD       - Listener Socket FD Error.                VB_TMO    - Peer vBond Timed out.
MGRTBLCKD   - Migration blocked. Wait for local TMO.
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.        XTVSTRDN  - Extra vSmart tear down.

                                                                  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          10.1.14.14     12346    10.1.14.14     12346   lte          tear_down  DISCVBD   NOERR      0
2016-02-23T16:33:30-0800
vbond    dtls     -               0          0          10.1.14.14     12346    10.1.14.14     12346   lte          connect    DCONFAIL  NOERR      4
2016-02-23T16:32:51-0800

vEdge# clear control connections-history
vEdge# show control connections-history
vEdge#
```

Command History

Release	Modification
16.1	Command introduced.

Related Topics

clear orchestrator connections-history, on page 605
show control connections, on page 788
show control connections-history, on page 791
show orchestrator connections-history, on page 932

clear control port-index

To reset port-hop back to the base port on Cisco vEdge devices, use the **clear control port-index** command in privileged EXEC mode.

clear 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 SD-WAN Release 20.6.1	This command was introduced.

Usage Guidelines

Use the **clear control port-index** command to reach back to 12346 base port on all the WAN interfaces.

Examples

The following example shows how to clear the port-hopping bucket index:

```
Device# clear control port-index
```

clear crash

Delete the core files on the local device. Core files are saved in the /var/crash directory on the local device.

clear crash *number*

Syntax Description

(none)	Clear all core and information files on the device.
number	Specific Core File: Clear the specific core file. *number* is the index number listed in the **show crash** output.

Command History

Release	Modification
15.2	Command introduced.

Examples

```
vSmart# show crash

INDEX  CORE TIME                 CORE FILENAME
-------------------------------------------------------------------
0      Tue Sep  2 17:13:43 2014  core.ompd.866.vsmart.1409703222

vSmart# clear crash
Are you sure you want to clear core and info files? [yes, NO]
vSmart# yes
vSmart# show crash
% No entries found.
```

Related Topics

file list, on page 637
file show, on page 637
show crash, on page 803

clear dhcp server-bindings

Clear the bindings to DHCP servers (on vEdge routers only).

clear dhcp server-bindings vpn *vpn-id* **interface** *interface-name* [**client-mac** *mac-address*]

Syntax Description

interface *interface-name*	Interface to DHCP Server: Interface to use to reach the DHCP server.
client-mac *client-mac*	MAC Address of DHCP Server: Clear the entry for a single DHCP host based on the host's MAC address.
vpn *vpn-id*	VPN: Clear the DHCP bindings in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.
15.1	**client-mac** option added.

Related Topics

clear dhcp state, on page 588
dhcp-helper, on page 179
dhcp-server, on page 181
show dhcp interface, on page 806
show dhcp server, on page 807

clear dhcp state

Clear IPv4 DHCP state on the local device (on vEdge routers and vSmart controllers only).

clear dhcp state interface *interface-name* [**vpn** *vpn-id*]

Syntax Description

interface *interface-name*	Clear the DHCP state of a specific interface.
vpn *vpn-id*	Clear the DHCP state of an interface in the specified VPN.

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# clear dhcp state interface ge0/0
vEdge# show dhcp interface state init
                    ACQUIRED    LEASE   TIME
VPN   IFNAME   STATE  IP          TIME    REMAINING   GATEWAY
-------------------------------------------------------------
0     ge0/0    init   0.0.0.0/0   -       -           0.0.0.0
```

Related Topics

clear ipv6 dhcp state, on page 599
show dhcp interface, on page 806
show dhcp server, on page 807
show ipv6 dhcp interface, on page 877

clear dns cache

Clear the cache of DNS entries on the local device. Use this command to clear stale entries from the DNS cache.

The DNS cache is populated when the device establishes a connection with the vBond orchestrator. For a vEdge router, this connection is transient, and the DNS cache is cleared when its connection to the vBond orchestrator is closed. For a vSmart controller, the connection to a vBond orchestrator is permanent.

clear dns cache

Command History

Release	Modification
15.3	Command introduced.

Examples

In the example output below, the entries in the DNS cache are highlighted in bold. After the DNS cache is cleared, it takes about 30 seconds for the vSmart controller to reestablish its connection with the vBond orchestrator and to repopulate its DNS cache.

```
vSmart# show control local-properties
organization-name            Cisco Inc
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Jun 29 18:00:05 2015 GMT
certificate-not-valid-after  Jun 28 18:00:05 2016 GMT

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     23456
system-ip                    172.16.255.19
chassis-num/unique-id        faa123ce-d281-43f1-a3f6-c95925d66869
serial-num                   12345602
register-interval            0:00:00:30
retry-interval               0:00:00:15
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:30:00
port-hopped                  FALSE
time-since-last-port-hop     0:00:00:00
number-vbond-peers           1

INDEX   IP                PORT

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

0       10.1.14.14         12346

number-active-wan-interfaces 1

                PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                                  ADMIN     OPERATION  LAST
INDEX  INTERFACE IP              PORT    IP               PORT     VSMARTS  VMANAGES  COLOR           CARRIER          STATE     STATE      CONNECTION
-------------------------------------------------------------------------------------------------------------------------------------------------------
0      eth1      10.0.5.19       12346   10.0.5.19        12346    1        1         default         default          up        up         0:00:00:08

vSmart# clear dns cache
vSmart# show control local-properties
organization-name            Cisco Inc
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Jun 29 18:00:05 2015 GMT
certificate-not-valid-after  Jun 28 18:00:05 2016 GMT

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     23456
system-ip                    172.16.255.19
```

```
chassis-num/unique-id        faa123ce-d281-43f1-a3f6-c95925d66869
serial-num                   12345602
register-interval            0:00:00:30
retry-interval               0:00:00:15
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:30:00
port-hopped                  FALSE
time-since-last-port-hop     0:00:00:00
number-vbond-peers           0
number-active-wan-interfaces 1

                  PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                                  ADMIN     OPERATION  LAST
INDEX  INTERFACE  IP               PORT    IP               PORT     VSMARTS  VMANAGES  COLOR            CARRIER          STATE     STATE      CONNECTION
-------------------------------------------------------------------------------------------------------------------------------------------------------
0      eth1       10.0.5.19        12346   10.0.5.19        12346    1        1         default          default          up        up         0:00:00:16

vSmart# about 30 seconds elapse
vSmart# show control local-properties
organization-name            Cisco Inc
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Jun 29 18:00:05 2015 GMT
certificate-not-valid-after  Jun 28 18:00:05 2016 GMT

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     23456
system-ip                    172.16.255.19
chassis-num/unique-id        faa123ce-d281-43f1-a3f6-c95925d66869
serial-num                   12345602
register-interval            0:00:00:30
retry-interval               0:00:00:15
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:30:00
port-hopped                  FALSE
time-since-last-port-hop     0:00:00:00
number-vbond-peers           1

INDEX   IP                  PORT
-------------------------------
0       10.1.14.14          12346

number-active-wan-interfaces 1

                  PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                                  ADMIN     OPERATION  LAST
INDEX  INTERFACE  IP               PORT    IP               PORT     VSMARTS  VMANAGES  COLOR            CARRIER          STATE     STATE      CONNECTION
-------------------------------------------------------------------------------------------------------------------------------------------------------
0      eth1       10.0.5.19        12346   10.0.5.19        12346    1        1         default          default          up        up         0:00:00:03
```

Related Topics

timer, on page 486
show control local-properties, on page 794

clear dot1x client

Deauthenticate a client connected on an 802.1X or 802.11i interface (on vEdge routers only). Reauthentication occurs automatically if the client attempts to use the interface again.

clear dot1x client *mac-address* **interface** *interface-name*

Syntax Description

mac-address	Client MAC Address: MAC address of the client to deauthenticate. To determine a client's MAC address, use the **show dot1x clients** command.
interface *interface-name*	Interface Name: Interface through which the client is reachable. To determine the interface name, use the **show dot1x interfaces** command.

Command History

Release	Modification
16.3	Command introduced.

Related Topics

show dot1x clients, on page 808
show dot1x interfaces, on page 809
show dot1x radius, on page 810

clear history

Clear the history of the commands issued in operational mode.

clear history

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show history
23:20:03 -- show arp
23:20:08 -- clear arp entries
23:20:10 -- show arp
23:22:28 -- clear dhcp
23:22:34 -- clear dhcp state
23:22:43 -- show dhcp
23:22:53 -- clear dhcp inter eth0
23:23:17 -- clear dhcp state interface eth0
23:23:28 -- show dhcp
23:23:50 -- show interface
23:24:13 -- show dhcp
23:26:01 -- history
23:26:09 -- show history
vEdge# clear history
vEdge# show history
23:26:18 -- show history
vEdge#
```

Related Topics

history, on page 639
show history, on page 821

clear igmp interface

Clear the interfaces on which IGMP is enabled on the router (on vEdge routers only).

Syntax Description

interface-name	Interface Name: Name of the interface to clear. *interface-name* has the format **ge***slot*/*port*.
vpn *vpn-id*	VPN: Clear IGMP information in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Related Topics

clear igmp protocol, on page 592
clear igmp statistics, on page 592
igmp, on page 235
show igmp interface, on page 823

clear igmp protocol

Flush all IGMP groups and relearn them (on vEdge routers only).

clear igmp interface vpn *vpn-id*

Syntax Description

vpn *vpn-id*	VPN: Flush all IGMP groups in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Related Topics

clear igmp interface, on page 591
clear igmp statistics, on page 592
igmp, on page 235
show igmp groups, on page 822

clear igmp statistics

Zero IGMP statistics (on vEdge routers only).

clear igmp statistics [**vpn** *vpn-id*]

Syntax Description

(none)	Clear IGMP statistics for all VPNs.
vpn *vpn-id*	VPN: Clear IGMP statistics in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# show igmp statistics

     RX       RX                                                  TX       TX
     GENERAL  GROUP  RX V1   RX V2   RX     RX       RX     GENERAL  GROUP  TX
VPN  QUERY    QUERY  REPORT  REPORT  LEAVE  UNKNOWN  ERROR  QUERY    QUERY  ERROR
-------------------------------------------------------------------------------
1    0        0      0       0       0      0        0      238      0      0

vEdge# clear igmp statistics
vEdge# show igmp statistics

     RX       RX                                                  TX       TX
     GENERAL  GROUP  RX V1   RX V2   RX     RX       RX     GENERAL  GROUP  TX
VPN  QUERY    QUERY  REPORT  REPORT  LEAVE  UNKNOWN  ERROR  QUERY    QUERY  ERROR
-------------------------------------------------------------------------------
1    0        0      0       0       0      0        0      0        0      0
```

Related Topics

clear igmp interface, on page 591
clear igmp protocol, on page 592
igmp, on page 235
show igmp statistics, on page 824

clear installed-certificates

Clear all the certificates on the local device, including the public and private keys and the root certificate, and return the device to the factory-default state.

clear installed-certificates

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vSmart# show control local-properties
organization-name            Cisco Inc
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Apr 07 20:03:36 2014 GMT
certificate-not-valid-after  Apr 07 20:03:36 2015 GMT

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
system-ip                    172.16.255.19
register-interval            0:00:00:30
retry-interval               0:00:00:15
dns-cache-ttl                0:00:30:00
number-vbond-peers           1

INDEX   IP                  PORT
-------------------------------
0       10.1.14.14          12346

number-active-wan-interfaces 1

       PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                  ADMIN     OPERATION
INDEX  IP               PORT    IP               PORT     VSMARTS  COLOR            CARRIER          STATE     STATE
-------------------------------------------------------------------------------------------------------------------------
0      10.0.5.19        12346   10.0.5.19        12346    2        default          default          up        up

vSmart# clear installed-certificates
Are you sure you want to clear installed certificates? [yes,NO] yes

vSmart# show control local-properties
organization-name            Cisco Inc
certificate-status           Not-Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Apr 07 20:03:36 2014 GMT
certificate-not-valid-after  Apr 07 20:03:36 2015 GMT

dns-name                     10.1.14.14
site-id                      100
domain-id                    1
system-ip                    172.16.255.19
register-interval            0:00:00:30
retry-interval               0:00:00:15
dns-cache-ttl                0:00:30:00
number-vbond-peers           1

INDEX   IP                  PORT
-------------------------------
0       10.1.14.14          12346

number-active-wan-interfaces 1

       PUBLIC           PUBLIC  PRIVATE          PRIVATE                                                  ADMIN     OPERATION
INDEX  IP               PORT    IP               PORT     VSMARTS  COLOR            CARRIER          STATE     STATE
-------------------------------------------------------------------------------------------------------------------------
0      10.0.5.19        12346   10.0.5.19        12346    2        default          default          up        up
```

Related Topics

reboot, on page 652
request certificate, on page 658
request csr upload, on page 664
request root-cert-chain, on page 700
request vsmart-upload serial-file, on page 715
show control local-properties, on page 794

clear interface statistics

Zero interface statistics.

clear interface statistics [**interface** *interface-name*] [**queue** *queue-number*] [**vpn** *vpn-id*]

Syntax Description

(none)	Zero the statistics on all interfaces and all queues.
queue *queue-number*	Interface Queue: Zero the statistics on the specified queue.
interface *interface-name*	Specific Interface: Zero the statistics on the specified interface.
vpn *vpn-id*	VPN: Zero the interface statistics for interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show interface statistics

                    RX                      RX      RX       TX                    TX      TX      RX   RX    TX   TX
VPN  INTERFACE      PACKETS    RX OCTETS    ERRORS  DROPS    PACKETS   TX OCTETS   ERRORS  DROPS   PPS  KBPS  PPS  KBPS
-------------------------------------------------------------------------------------------------------------------
0    ge0/0          10756769   2545508661   0       1693399  9460046   1401233512  0       1       14   15    15   16
0    ge0/1          0          0            0       0        0         0           0       0       0    0     0    0
0    ge0/2          0          0            0       0        0         0           0       0       0    0     0    0
0    ge0/4          0          0            0       0        0         0           0       0       0    0     0    0
0    ge0/5          0          0            0       0        0         0           0       0       0    0     0    0
0    ge0/6          0          0            0       0        0         0           0       0       0    0     0    0
0    ge0/7          0          0            0       0        0         0           0       0       0    0     0    0
0    system         0          0            0       0        0         0           0       0       0    0     0    0
1    ge0/3          214082     68435255     0       37160    156849    14532821    0       3       4    2     4    2
512  mgmt0          0          0            0       0        0         0           0       0       0    0     0    0

vEdge# clear interface statistics
vEdge# show interface statistics

                    RX       RX       RX       RX       TX       TX       TX       TX       RX   RX    TX   TX
VPN  INTERFACE      PACKETS  OCTETS   ERRORS   DROPS    PACKETS  OCTETS   ERRORS   DROPS    PPS  KBPS  PPS  KBPS
-------------------------------------------------------------------------------------------------------------
0    ge0/0          57       13592    0        8        51       7336     0        0        17   46    13   14
0    ge0/1          0        0        0        0        0        0        0        0        0    0     0    0
0    ge0/2          0        0        0        0        0        0        0        0        0    0     0    0
0    ge0/4          0        0        0        0        0        0        0        0        0    0     0    0
0    ge0/5          0        0        0        0        0        0        0        0        0    0     0    0
0    ge0/6          0        0        0        0        0        0        0        0        0    0     0    0
0    ge0/7          0        0        0        0        0        0        0        0        0    0     0    0
0    system         0        0        0        0        0        0        0        0        0    0     0    0
1    ge0/3          42       3744     0        0        26       2772     0        0        4    2     4    2
512  mgmt0          0        0        0        0        0        0        0        0        0    0     0
```

Related Topics

show interface, on page 827
show interface statistics, on page 851

clear ip leak routes vpn

To clear leaked routes for a VPN, use the **clear ip leak routes vpn** command.

clear ip leak routes vpn *vpn-id*

Command History

Release	Modification
Cisco SD-WAN Release 20.3.1	Command introduced.

clear ip mfib record

Clear the statistics for a particular group, source, or VPN from the Multicast Forwarding Information Base (MFIB) (on vEdge routers only).

clear ip mfib record group *group-address* **source** *source-address* **vpn** *vpn-id* [**upstream-iif** *interface-name*] [**upstream-tunnel** *ip-address*]

Syntax Description

group *group-address* **source** *source-address* **vpn** *vpn-id*	Clear Statistics from the MFIB: Clear the statistics for a particular group, source, or VPN from the MFIB.
upstream-iif *interface-name*	Upstream Interface: Clear the MFIB statistics for the specified upstream interface.
upstream-tunnel *ip-address*	Upstream Tunnel: Clear the MFIB statistics for the specified tunnel to a remote system.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# clear ip mfib record group 254.1.1.1 vpn 1 source 255.1.1.1
vEdge#
```

Related Topics

clear ip mfib stats, on page 597
show ip mfib summary, on page 861

clear ip mfib stats

Clear all statistics from the Multicast Forwarding Information Base (MFIB) (on vEdge routers only).

clear ip mfib stats

Examples

```
vEdge# clear ip mfib stats
vEdge#
```

Command History

Release	Modification
14.2	Command introduced.

Related Topics

clear ip mfib record, on page 596
show ip mfib stats, on page 860

clear ip nat filter

Clear the NAT translational filters (on vEdge routers only).

clear ip nat filter [*parameter*]

Syntax Description

parameter	Filter Parameter: Clear NAT translation filters associated with the specified parameter. *parameter* can be nat-ifname, nat-vpn-id, private-dest-address, private-dest-port, private-source-address, private-source-port, private-vpn-id, and proto. These parameters correspond to some of the column headers in the **show ip nat filter** command output.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# show ip nat filter nat-vpn
                                PRIVATE     PRIVATE     PRIVATE  PRIVATE  PUBLIC      PUBLIC      PUBLIC  PUBLIC
NAT  NAT                        SOURCE      DEST        SOURCE   DEST     SOURCE      DEST        SOURCE  DEST    FILTER       IDLE         OUTBOUND
OUTBOUND  INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS     ADDRESS     PORT     PORT     ADDRESS     ADDRESS     PORT    PORT    STATE        TIMEOUT      PACKETS
OCTETS    PACKETS  OCTETS
-------------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  4697     4697     10.1.15.15  10.1.14.14  64931   64931   established  0:00:00:41   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  14169    14169    10.1.15.15  10.1.14.14  28467   28467   established  0:00:00:44   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  21337    21337    10.1.15.15  10.1.14.14  44555   44555   established  0:00:00:47   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  28505    28505    10.1.15.15  10.1.14.14  40269   40269   established  0:00:00:50   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  39513    39513    10.1.15.15  10.1.14.14  31859   31859   established  0:00:00:53   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  46681    46681    10.1.15.15  10.1.14.14  1103    1103    established  0:00:00:56   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  57176    57176    10.1.15.15  10.1.14.14  38730   38730   established  0:00:00:35   1
98        1        98
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  64600    64600    10.1.15.15  10.1.14.14  33274   33274   established  0:00:00:38   1
98        1        98
0    ge0/0   0    udp        10.1.15.15  10.0.5.19   12346    12346    10.1.15.15  10.0.5.19   64236   12346   established  0:00:19:59   38
8031      23       5551
0    ge0/0   0    udp        10.1.15.15  10.0.12.20  12346    12346    10.1.15.15  10.0.12.20  64236   12346   established  0:00:19:59   36
7470      23       5551
0    ge0/0   0    udp        10.1.15.15  10.0.12.22  12346    12346    10.1.15.15  10.0.12.22  64236   12346   established  0:00:19:59   679
598771    434      92925
0    ge0/0   0    udp        10.1.15.15  10.1.14.14  12346    12346    10.1.15.15  10.1.14.14  64236   12346   established  0:00:19:59   34
3825      9        3607
0    ge0/0   0    udp        10.1.15.15  10.1.14.14  12346    12350    10.1.15.15  10.1.14.14  64236   12350   established  0:00:19:59   38
5472      23       3634
0    ge0/0   0    udp        10.1.15.15  10.1.16.16  12346    12346    10.1.15.15  10.1.16.16  64236   12346   established  0:00:19:59   38
5472      23       3634

vEdge# clear ip nat filter proto icmp
vEdge# show ip nat filter nat-vpn
                                PRIVATE     PRIVATE     PRIVATE  PRIVATE  PUBLIC      PUBLIC      PUBLIC  PUBLIC
NAT  NAT                        SOURCE      DEST        SOURCE   DEST     SOURCE      DEST        SOURCE  DEST    FILTER       IDLE         OUTBOUND
OUTBOUND  INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS     ADDRESS     PORT     PORT     ADDRESS     ADDRESS     PORT    PORT    STATE        TIMEOUT      PACKETS
OCTETS    PACKETS  OCTETS
-------------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0   0    icmp       10.1.15.15  10.1.14.14  59484    59484    10.1.15.15  10.1.14.14  17148   17148   established  0:00:00:58   1
98        1        98
0    ge0/0   0    udp        10.1.15.15  10.0.5.19   12346    12346    10.1.15.15  10.0.5.19   64236   12346   established  0:00:19:59   143
25726     128      23166
0    ge0/0   0    udp        10.1.15.15  10.0.12.20  12346    12346    10.1.15.15  10.0.12.20  64236   12346   established  0:00:19:59   141
25165     128      23166
0    ge0/0   0    udp        10.1.15.15  10.0.12.22  12346    12346    10.1.15.15  10.0.12.22  64236   12346   established  0:00:19:59   788
617422    537      110350
0    ge0/0   0    udp        10.1.15.15  10.1.14.14  12346    12346    10.1.15.15  10.1.14.14  64236   12346   established  0:00:19:59   129
9335      9        3607
0    ge0/0   0    udp        10.1.15.15  10.1.14.14  12346    12350    10.1.15.15  10.1.14.14  64236   12350   established  0:00:19:59   227
32688     212      33496
0    ge0/0   0    udp        10.1.15.15  10.1.16.16  12346    12346    10.1.15.15  10.1.16.16  64236   12346   established  0:00:19:59   227
32688     212      33496
```

Related Topics

clear ip nat statistics, on page 598
nat, on page 346
show ip nat filter, on page 862

clear ip nat statistics

Clear the NAT translational interface statistics (on vEdge routers only).

clear ip nat statistics [**interface** *interface-name*] [**vpn** *vpn-id*]

Syntax Description

interface *interface-name* **vpn** *vpn-id*	Specific Interface: Clear NAT translation statistics associated with the specified interface.
vpn *vpn-id*	Specific VPN: Clear NAT translation statistics associated with the specified VPN.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# show ip nat interface-statistics
                                                NAT   NAT     NAT     NAT                                          INBOUND
             NAT       NAT       NAT     NAT    MAP   FILTER  FILTER  STATE  NAT      OUTBOUND  INBOUND  ICMP              NAT        NAT
             OUTBOUND  INBOUND   ENCODE  DECODE ADD   ADD     LOOKUP  CHECK  POLICER  ICMP      ICMP     ERROR    NAT      FRAGMENTS  UNSUPPORTED
VPN  IFNAME  PACKETS   PACKETS   FAIL    FAIL   FAIL  FAIL    FAIL    FAIL   DROPS    ERROR     ERROR    DROPS    FRAGMENTS FAIL       PROTO
-------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0   3852      3360      0       0      0     0       0       0      0        0         0        0        0          0          0

vEdge# clear ip nat statistics
vEdge# show ip nat interface-statistics
                                                NAT   NAT     NAT     NAT                                          INBOUND
             NAT       NAT       NAT     NAT    MAP   FILTER  FILTER  STATE  NAT      OUTBOUND  INBOUND  ICMP              NAT        NAT
             OUTBOUND  INBOUND   ENCODE  DECODE ADD   ADD     LOOKUP  CHECK  POLICER  ICMP      ICMP     ERROR    NAT      FRAGMENTS  UNSUPPORTED
VPN  IFNAME  PACKETS   PACKETS   FAIL    FAIL   FAIL  FAIL    FAIL    FAIL   DROPS    ERROR     ERROR    DROPS    FRAGMENTS FAIL       PROTO
-------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0   44        41        0       0      0     0       0       0      0        0         0        0        0          0          0
```

Related Topics

clear ip nat filter, on page 597
nat, on page 346
show ip nat interface-statistics, on page 864

clear ipv6 dhcp state

Clear IPv6 DHCP state on the local device (on vEdge routers and vSmart controllers only).

clear ipv6 dhcp state interface *interface-name* [**vpn** *vpn-id*]

Syntax Description

interface *interface-name*	Interface: Clear the DHCP state of a specific interface.
vpn *vpn-id*	VPN: Clear the DHCP state of an interface in the specified VPN.

Command History

Release	Modification
16.3	Command introduced.

Related Topics

clear dhcp state, on page 588
show dhcp interface, on page 806
show dhcp server, on page 807
show ipv6 dhcp interface, on page 877

clear ipv6 neighbor

Refresh dynamically created IPv6 entries in the Address Resolution Protocol (ARP) cache (on vEdge routers and vSmart controllers only).

To clear IPv4 entries in the ARP cache, use the **clear arp** command.

clear ipv6 neighbor [**interface** *interface-name*] [*ip-address*] [**vpn** *vpn-id*]

Syntax Description

(none)	Refresh all dynamic ARP cache entries.
interface *interface-name*	Interface: Refresh the dynamic ARP cache entries associated with the specific interface.
ip-address	IP Addresss: Refresh the dynamic ARP cache entries for the specified IP address.
vpn *vpn-id*	VPN: Refresh the dynamic ARP cache entries for the specific VPN.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
Edge# show ipv6 neighbor

     IF
VPN  NAME   IP                          MAC               STATE    IDLE TIMER  UPTIME
-------------------------------------------------------------------------------------
0    ge0/0  2001::a01:f0d               00:0c:29:57:29:31  dynamic  0:00:00:00  0:00:06:07
0    ge0/0  2001::a01:f0f               00:0c:29:20:77:53  static   -           0:00:08:31
0    ge0/0  fe80::20c:29ff:fe20:7753    00:0c:29:20:77:53  static   -           0:00:26:32
0    ge0/0  fe80::20c:29ff:fe57:2931    00:0c:29:57:29:31  dynamic  0:00:00:00  0:00:08:06
0    ge0/1  2001::a01:110f              00:0c:29:20:77:5d  static   -           0:00:08:29
0    ge0/1  fe80::20c:29ff:fe20:775d    00:0c:29:20:77:5d  static   -           0:00:08:29
0    ge0/2  fe80::20c:29ff:fe20:7767    00:0c:29:20:77:67  static   -           0:00:26:36
0    ge0/3  2001::a00:140f              00:0c:29:20:77:71  static   -           0:00:08:29
0    ge0/3  fe80::20c:29ff:fe20:7771    00:0c:29:20:77:71  static   -           0:00:08:29
0    ge0/6  2001::3900:10f              00:0c:29:20:77:8f  static   -           0:00:08:28
0    ge0/6  fe80::20c:29ff:fe20:778f    00:0c:29:20:77:8f  static   -           0:00:08:28
0    ge0/7  fe80::20c:29ff:fe20:7799    00:0c:29:20:77:99  static   -           0:00:26:06

vEdge# clear ipv6 neighbor
```

```
vEdge# show ipv6 neighbor

     IF
VPN  NAME   IP                          MAC               STATE    IDLE TIMER  UPTIME
-------------------------------------------------------------------------------------
0    ge0/0  2001::a01:f0f               00:0c:29:20:77:53  static   -           0:00:08:31
0    ge0/0  fe80::20c:29ff:fe20:7753    00:0c:29:20:77:53  static   -           0:00:26:32
0    ge0/1  2001::a01:110f              00:0c:29:20:77:5d  static   -           0:00:08:29
0    ge0/1  fe80::20c:29ff:fe20:775d    00:0c:29:20:77:5d  static   -           0:00:08:29
0    ge0/2  fe80::20c:29ff:fe20:7767    00:0c:29:20:77:67  static   -           0:00:26:36
0    ge0/3  2001::a00:140f              00:0c:29:20:77:71  static   -           0:00:08:29
0    ge0/3  fe80::20c:29ff:fe20:7771    00:0c:29:20:77:71  static   -           0:00:08:29
0    ge0/6  2001::3900:10f              00:0c:29:20:77:8f  static   -           0:00:08:28
0    ge0/6  fe80::20c:29ff:fe20:778f    00:0c:29:20:77:8f  static   -           0:00:08:28
0    ge0/7  fe80::20c:29ff:fe20:7799    00:0c:29:20:77:99  static   -           0:00:26:06
```

Related Topics

clear arp, on page 577
show arp, on page 746
show ipv6 neighbor, on page 882

clear ipv6 policy

Reset all counters for IPv6 access lists (on vEdge routers only).

clear policy access-list name *acl-name*

Syntax Description

name *acl-name*	Access List Counters: Zero the counters associated with the specified access list.

Command History

Release	Modification
16.3	Command introduced.

Related Topics

clear policy, on page 613
show ipv6 policy access-list-counters, on page 883
show ipv6 policy access-list-names, on page 884

clear omp all

Reset OMP peering sessions with all OMP peers (on vSmart controllers and vEdge routers only).

clear omp all

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show omp peers
R -> routes received
I -> routes installed
S -> routes sent
Peer             Type    Domain-ID  Site-ID  State    Uptime           R/I/S
-------------------------------------------------------------------------------
1.1.200.2        vsmart  1          3        up       7:17:00:04       65/51/15
1.1.200.3        vsmart  1          11740    up       3:00:29:33       65/0/15

vEdge# clear omp all
vEdge# show omp peers
Peer             Type    Domain-ID  Site-ID  State    Uptime           R/I/S
-------------------------------------------------------------------------------
1.1.200.2        vsmart  1          3        idle     -                65/51/15
1.1.200.3        vsmart  1          11740    idle     -                65/0/15
```

Related Topics

clear control connections, on page 584
clear omp peer, on page 602
clear omp routes, on page 604
clear omp tlocs, on page 604
show omp peers, on page 910

clear omp peer

Reset the OMP peering sessions with a specific peer (on vSmart controllers and vEdge routers only). When you reset a peering session, the routes to that peer are removed from the OMP route table, and they are reinstalled when the peer comes back up.

clear omp peer *ip-address* [**soft** (**in** |**out**)]

Syntax Description

(none)	Reset the specific peering session.
soft in |**out**	Refresh the Peering Session: Re-apply the inbound or outbound policy to the specific peering session.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show 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       0:00:08:32       11/11/0
172.16.255.20    vsmart  1         200       up       0:00:08:31       11/0/0

vEdge# show omp routes
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS                                      PATH
FAMILY   VPN  PREFIX             FROM PEER      ID    LABEL  STATUS  TLOC IP         COLOR  ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------------------------
ipv4     1    10.2.2.0/24        172.16.255.19  133   3806   C,I,R   172.16.255.11   lte    ipsec  -
                                 172.16.255.20  43    3806   C,R     172.16.255.11   lte    ipsec  -
         1    10.2.3.0/24        172.16.255.19  134   16355  C,I,R   172.16.255.21   lte    ipsec  -
                                 172.16.255.20  44    16355  C,R     172.16.255.21   lte    ipsec  -
         1    10.20.24.0/24      172.16.255.19  127   34885  C,I,R   172.16.255.15   lte    ipsec  -
                                 172.16.255.20  20    34885  C,R     172.16.255.15   lte    ipsec  -
         1    10.20.25.0/24      172.16.255.19  131   61944  C,I,R   172.16.255.16   lte    ipsec  -
                                 172.16.255.20  17    61944  C,R     172.16.255.16   lte    ipsec  -
         1    56.0.1.0/24        172.16.255.19  126   34885  C,I,R   172.16.255.15   lte    ipsec  -
                                 172.16.255.20  19    34885  C,R     172.16.255.15   lte    ipsec  -
         1    60.0.1.0/24        172.16.255.19  130   61944  C,I,R   172.16.255.16   lte    ipsec  -
                                 172.16.255.20  16    61944  C,R     172.16.255.16   lte    ipsec  -
         1    61.0.1.0/24        172.16.255.19  129   61944  C,I,R   172.16.255.16   lte    ipsec  -
                                 172.16.255.20  15    61944  C,R     172.16.255.16   lte    ipsec  -
         1    172.16.255.112/32  172.16.255.19  135   3806   C,I,R   172.16.255.11   lte    ipsec  -
                                 172.16.255.19  136   16355  C,I,R   172.16.255.21   lte    ipsec  -
                                 172.16.255.20  45    3806   C,R     172.16.255.11   lte    ipsec  -
                                 172.16.255.20  46    16355  C,R     172.16.255.21   lte    ipsec  -
         1    172.16.255.117/32  172.16.255.19  128   34885  C,I,R   172.16.255.15   lte    ipsec  -
                                 172.16.255.20  21    34885  C,R     172.16.255.15   lte    ipsec  -
         1    172.16.255.118/32  172.16.255.19  132   61944  C,I,R   172.16.255.16   lte    ipsec  -
                                 172.16.255.20  18    61944  C,R     172.16.255.16   lte    ipsec  -

vEdge# clear omp peer 172.16.255.19

vm4# show 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       0:00:00:00       0/0/0
172.16.255.20    vsmart  1         200       up       0:00:09:01       11/11/0

vEdge# show omp routes
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS                                      PATH
FAMILY   VPN  PREFIX             FROM PEER      ID    LABEL  STATUS  TLOC IP         COLOR  ENCAP  PREFERENCE
-----------------------------------------------------------------------------------------------------------------
ipv4     1    10.2.2.0/24        172.16.255.20  43    3806   C,I,R   172.16.255.11   lte    ipsec  -
         1    10.2.3.0/24        172.16.255.20  44    16355  C,I,R   172.16.255.21   lte    ipsec  -
         1    10.20.24.0/24      172.16.255.20  20    34885  C,I,R   172.16.255.15   lte    ipsec  -
         1    10.20.25.0/24      172.16.255.20  17    61944  C,I,R   172.16.255.16   lte    ipsec  -
         1    56.0.1.0/24        172.16.255.20  19    34885  C,I,R   172.16.255.15   lte    ipsec  -
         1    60.0.1.0/24        172.16.255.20  16    61944  C,I,R   172.16.255.16   lte    ipsec  -
```

```
1    61.0.1.0/24         172.16.255.20  15    61944  C,I,R   172.16.255.16  lte    ipsec  -
1    172.16.255.112/32   172.16.255.20  45    3806   C,I,R   172.16.255.11  lte    ipsec  -
                         172.16.255.20  46    16355  C,I,R   172.16.255.21  lte    ipsec  -
1    172.16.255.117/32   172.16.255.20  21    34885  C,I,R   172.16.255.15  lte    ipsec  -
1    172.16.255.118/32   172.16.255.20  18    61944  C,I,R   172.16.255.16  lte    ipsec  -
```

Related Topics

clear omp all, on page 601
clear omp routes, on page 604
clear omp tlocs, on page 604
show omp peers, on page 910

clear omp routes

Recalculate the OMP routes and resend the routes to the IP route table (on vSmart controllers and vEdge routers only).

clear omp routes

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# clear omp routes
vEdge#
```

Related Topics

clear omp all, on page 601
clear omp peer, on page 602
clear omp tlocs, on page 604
show omp routes, on page 914

clear omp tlocs

Recalculate the OMP TLOCs and resend the TLOCs to the route table (on vSmart controllers and vEdge routers only).

clear omp tlocs

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# clear omp tlocs
vEdge#
```

Related Topics

clear omp all, on page 601
clear omp peer, on page 602
clear omp routes, on page 604
show omp tlocs, on page 924

clear orchestrator connections-history

Clear the history of connections and connection attempts made by the vBond orchestrator (on vBond orchestrators only).

clear orchestrator connections-history

Command History

Release	Modification
16.1	Command introduced.

Examples

Show orchestrator connections-history

```
vEdge# show orchestrator connections-history
Legend for Errors
BDSGVERFL  - Board ID signature verify failure        ORPTMO    - Remote client peer timeout
BIDNTPR    - Board ID not initialized                 RMGSPR    - Remove global saved peer
BIDNTVRFD  - Peer board ID certificate not verified   RXTRDWN   - Received teardown
CRTREJSER  - Challenge response rejected by peer      RDSIGFBD  - Read signature from board ID failed
CRTVERFL   - Fail to verify peer certificate          SSLNFAIL  - Failure to create new SSL context
CTORGNMMIS - Certificate organization name mismatch   SERNTPRES - Serial number not present
DCONFAIL   - DTLS connection failure                  TMRALC    - Memory failure
DEVALC     - Device memory allocation failures        TUNALC    - Memory failure
DHSTMO     - DTLS handshake timeout                   UNMSGBDRG - Unknown message type or bad register message
DISCVBD    - Disconnect vBond after register reply    UNAUTHEL  - Recd hello from unauthenticated peer
DISTLOC    - TLOC disabled                            VBDEST    - vDaemon process terminated
DUPSER     - Duplicate serial number                  VECRTREV  - vEdge certification revoked
IP_TOS     - Socket options failure                   VSCRTREV  - vSmart certificate revoked
LISFD      - Listener socket FD error                 VB_TMO    - Peer vBond timed out
MEMALCFL   - Memory allocation failure                VM_TMO    - Peer vManage timed out
NOACTVB    - No active vBond found to connect to      VP_TMO    - Peer vEdge timed out
NOERR      - No error                                 VS_TMO    - Peer vSmart timed out
NOSLPRCRT  - Unable to get peer's certificate         XTVSTRDN  - Extra vSmart teardown

                                                                  PEER     PEER             PEER
PEER     PEER     PEER             SITE       DOMAIN     PEER             PRIVATE  PEER             PUBLIC                  LAST                                TIME WHEN
TYPE     PROTOCOL SYSTEM IP        ID         ID         PRIVATE IP       PORT     PUBLIC IP        PORT    REMOTE COLOR    STATE               LOCAL/REMOTE    LAST CHANGED
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
vedge    dtls     172.16.255.14    400        1          10.1.14.14       12350    10.1.14.14       12350   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:23:14
vedge    dtls     172.16.255.16    600        1          10.1.16.16       12346    10.1.16.16       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:23:14
vedge    dtls     172.16.255.15    500        1          10.1.15.15       12346    10.1.15.15       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:23:00
vedge    dtls     172.16.255.15    500        1          10.1.15.15       12346    10.1.15.15       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:22:44
vedge    dtls     172.16.255.16    600        1          10.1.16.16       12346    10.1.16.16       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:22:43
vedge    dtls     172.16.255.14    400        1          10.1.14.14       12350    10.1.14.14       12350   lte             trying              RXTRDWN/DISCVBD   2014-07-21T18:22:28
vmanage  dtls     172.16.255.22    200        0          10.0.12.22       12346    10.0.12.22       12346   default         tear_down            VM_TMO/NOERR     2014-07-21T18:22:28
vedge    dtls     172.16.255.15    500        1          10.1.15.15       12346    10.1.15.15       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:47
vedge    dtls     172.16.255.14    400        1          10.1.14.14       12350    10.1.14.14       12350   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:46
vedge    dtls     172.16.255.16    600        1          10.1.16.16       12346    10.1.16.16       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:46
vedge    dtls     172.16.255.15    500        1          10.1.15.15       12346    10.1.15.15       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:31
vedge    dtls     172.16.255.14    400        1          10.1.14.14       12350    10.1.14.14       12350   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:31
vedge    dtls     172.16.255.16    600        1          10.1.16.16       12346    10.1.16.16       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:31
vsmart   dtls     172.16.255.20    100        1          10.0.12.20       12346    10.0.12.20       12346   default          up                 RXTRDWN/DISTLOC   2014-07-21T13:39:15
vedge    dtls     172.16.255.16    600        1          10.1.16.16       12346    10.1.16.16       12346   lte             trying              RXTRDWN/DISCVBD   2014-07-21T13:39:10
```

```
vedge    dtls    172.16.255.14    400        1          10.1.14.14      12350   10.1.14.14      12350   lte            trying           RXTRDWN/DISCVBD   2014-07-21T13:39:10
vedge    dtls    172.16.255.15    500        1          10.1.15.15      12346   10.1.15.15      12346   lte            trying           RXTRDWN/DISCVBD   2014-07-21T13:39:10
vBond# clear orchestrator connections-history
vBond# show orchestrator connections-history
vBond#
```

Related Topics

clear control connections-history, on page 585
show control connections, on page 788
show orchestrator connections-history, on page 932
show orchestrator local-properties, on page 935
show orchestrator statistics, on page 937

clear ospf all

Reset OSPF in a VPN (on vEdge routers only).

clear ospf all *vpn vpn-id*

Syntax Description

vpn *vpn-id*	VPN: Reset OSPF in the specified VPN.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show ospf neighbor vpn 1
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List

                  IF     IF                                    DEAD
VPN  ADDRESS      INDEX  NAME   NEIGHBOR ID    STATE  PRI  TIME  DBsmL  RqstL  RXmtL
-------------------------------------------------------------------------------------
1    10.20.24.17  0      ge0/4  172.16.255.17  full   1    31    0      0      0

vEdge# clear ospf all vpn 1
vEdge# show ospf neighbor vpn 1
%  No entries found.
```

Related Topics

show ospf neighbor, on page 947

clear ospf database

Delete the entries in the OSPF link-state database learned from OSPF neighbors (on vEdge routers only). Use this command for troubleshooting OSPF or to reset the link-state database if you suspect that it has been corrupted.

clear ospf database vpn *vpn-id*

Syntax Description

vpn *vpn-id*	VPN: Clear the OSPF link-state database of entries from the specified VPN.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# show ospf database router
            LSA                 LINK              ADVERTISING
VPN  AREA   TYPE                ID                ROUTER            AGE      CHECKSUM  SEQ#
-------------------------------------------------------------------------------------------
1    0      router              172.16.255.15     172.16.255.15     143      0x27ee    0x8000000f
1    0      router              172.16.255.17     172.16.255.17     24       0x27ea    0x8000000d

vEdge# clear ospf database vpn 1
vEdge# show ospf database router
            LSA                 LINK              ADVERTISING
VPN  AREA   TYPE                ID                ROUTER            AGE      CHECKSUM  SEQ#
-------------------------------------------------------------------------------------------
1    0      router              172.16.255.15     172.16.255.15     164      0x27ee    0x8000000f
```

Related Topics

show ospf database, on page 943

clear pim interface

Clear PIM interfaces, and relearn all PIM neighbors and joins (on vEdge routers only).

clear pim interface vpn *vpn-id* [*interface-name*]

Syntax Description

interface-name **vpn** *vpn-id*	Interface Name: Release the PIM neighbors and joins on a specific interface in a specific VPN.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# clear pim interface interface ge0/0 vpn 1
vEdge#
```

Related Topics

clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

clear pim neighbor

Clear a PIM neighbor (on vEdge routers only).

clear pim neighbor *ip-address* **vpn** *vpn-id*

Syntax Description

ip-address **vpn** *vpn-id*	Neighbor To Clear: Clear a specific neighbor in the specified VPN.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# clear pim neighbor 254.1.1.1 vpn 1
vEdge#
```

Related Topics

clear pim interface, on page 607
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

clear pim protocol

Clear all PIM protocol state (on vEdge routers only).

clear pim protocol vpn *vpn-id*

Syntax Description

vpn *vpn-id*	VPN: Clear the PIM protocol state for the specified VPN.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# clear pim protocol vpn 1
vEdge#
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901

show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

clear pim rp-mapping

Clear the mappings of multicast groups to RPs (on vEdge routers only).

clear pim rp-mapping [**vpn** *vpn-id*]

Syntax Description

(none)	Clear all group-to-RP mappings.
vpn *vpn-id*	VPN: Clear the group-to-RP mappings for a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vEdge# show pim rp-mapping
VPN TYPE     GROUP            RP ADDRESS
---------------------------------------
1     Auto-RP 224.0.0.0/4 60.0.1.100
2     Auto-RP 224.0.0.0/4 60.0.2.100
vEdge# clear pim rp-mapping
vEdge# show pim rp-mapping
%  No entries found.
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957

show pim rp-mapping, on page 958
show pim statistics, on page 959

clear pim statistics

Clear all PIM-related statistics on the router, and relearn all PIM neighbors and joins (on vEdge routers only).

clear pim statistics [**vpn** *vpn-id*]

Syntax Description

(none)	Clear all PIM statistics, neighbors, and joins, and then relearn them.
vpn *vpn-id*	VPN: Clear the PIM statistics, neighbors, and joins in the specified VPN, and then relearn them.

Command History

Release	Modification
14.2	Command introduced.

Examples

```
vEdge# show pim statistics
VPN 1 STATISTICS
-----------------------------------------
MESSAGE TYPE         RECEIVED          SENT
-----------------------------------------
Hello                    2455          2528
Join-Prune                115            82
AutoRP Announce             0             -
AutoRP Mapping              0             -
Unsupported                 0             -
Unknown                     0             -
Bad                      1440             -
vEdge# clear pim statistics
vEdge# show pim statistics
VPN 1 STATISTICS
-----------------------------------------
MESSAGE TYPE         RECEIVED          SENT
-----------------------------------------
Hello                       0             0
Join-Prune                  0             0
AutoRP Announce             0             -
AutoRP Mapping              0             -
Unsupported                 0             -
Unknown                     0             -
Bad                         0             -
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609

clear pim rp-mapping, on page 610
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

clear policer statistics

Clear the policer out-of-specification (OOS) packet statistics (on vEdge routers only). A policed packet is out of specification when the policer does not allow it to pass. Depending on the policer configuration, these packets are either dropped or they are remarked, which sets the packet loss priority (PLP) value on the egress interface to high.

clear policer statistics

Command History

Release	Modification
16.3	Command introduced.

Examples

Clear the policer OOS packet statistics

```
vEdge# show policer
                                                          OOS     OOS
NAME       INDEX  DIRECTION  RATE          BURST  ACTION  PKTS
-------------------------------------------------------------------
ge0_0_llq  10     out        200000000000  15000  drop    2499
ge0_3_llq  11     out        200000000000  15000  drop    3212

vEdge# clear policer statistics
vEdge# show policer
                                                          OOS     OOS
NAME       INDEX  DIRECTION  RATE          BURST  ACTION  PKTS
-------------------------------------------------------------------
ge0_0_llq  10     out        200000000000  15000  drop    0
ge0_3_llq  11     out        200000000000  15000  drop    0
```

Related Topics

show policer, on page 963
show policy data-policy-filter, on page 968
show policy from-vsmart, on page 971

clear policy

Reset all counters for IPv4 access lists or data policies (on vSmart controllers and vEdge routers only).

clear policy (**access-list** *acl-name* | **app-route-policy** *policy-name* | **data-policy** *policy-name*)

Syntax Description

access-list *acl-name*	Access List Counters: Zero the counters associated with the specified access list.
app-route-policy *policy-name*	Application-Aware Routing Policy Counter: Zero the counters associated with the specified application-aware routing policy.
data-policy *policy-name*	Data Policy Counters: Zero the counters associated with the specified data policy.

Command History

Release	Modification
14.1	Command introduced.

Related Topics

clear ipv6 policy, on page 601

clear policy zbfw filter-statistics

Clear the count of the packets that match a zone-based firewall's match criteria and the number of bytes that match the criteria (on vEdge routers only).

clear policy zbfw filter-statistics

Command History

Release	Modification
18.2	Command introduced.

Examples

Display statistics about packets that the router has processed with zone-based firewall policy

```
vEdge# show policy zbfw filter-staatistics

NAME           COUNTER NAME   PACKETS  BYTES
-----------------------------------------------
ZONE-POLICY-1  counter_seq_1  2        196
```

```
vEdge# show policy zbfw filter-staatistics
vEdge#
```

Related Topics

show policy zbfw filter-statistics, on page 975

clear policy zbfw global-statistics

Zero the statistics about the packets processed by zone-based firewalls (on vEdge routers only).

clear policy zbfw global-statistics

Command History

Release	Modification
18.2	Command introduced.

Examples

Clear the statistics about packets that the router has processed with zone-based firewalls

```
vEdge# clear zbfw global-statistics
vEdge# show zbfw global-statistics
        fragments                   : 0
        fragments fail              : 0
        state check fail            : 0
        flow add fail               : 0
        unsupported proto           : 0
        number of flow entries      : 0
        max half open exceeded      : 0

        Packets Implicitly Dropped  :
          During Policy Change      : 0
          No Pair for Diff Zone     : 0
          Zone to No Zone           : 0

        Packets Implicitly Allowed  :
          No Pair Same Zone         : 0
          No Zone to No Zone        : 0
```

Related Topics

show policy zbfw global-statistics, on page 976

clear policy zbfw sessions

Clear the session flow information for zone pairs configured with a zone-based firewall policy (on vEdge routers only).

show policy zbfw sessions [**name** *pair-name*]

Syntax Description

(none)	Clear the session flow entries for all zone pairs.
name *pair-name*	Zone Pair Name: Clear the session flow entries for the specified zone pair.

Command History

Release	Modification
18.2	Command introduced.

Examples

Clear all session flow information

```
vEdge# show policy zbfw sessions

ZONE PAIR      SOURCE IP    DESTINATION  SOURCE  DESTINATION           SOURCE  DESTINATION  IDLE        OUTBOUND  OUTBOUND  INBOUND  INBOUND
FILTER
NAME      VPN  ADDRESS      IP ADDRESS   PORT    PORT         PROTOCOL  VPN     VPN          TIMEOUT     PACKETS   OCTETS    PACKETS  OCTETS   STATE

-------------------------------------------------------------------------------------------------------------------------------------------------
zp1       1    10.20.24.17  10.20.25.18  44061   5001         TCP       1       1            0:00:59:59  12552     17581337  6853     463590
established
zp1       1    10.20.24.17  10.20.25.18  44062   5001         TCP       1       1            0:01:00:00  10151     14217536  5561     375290
established
zp1       1    10.20.24.17  10.20.25.18  44063   5001         TCP       1       1            0:00:59:59  7996      11198381  4262     285596
established
zp1       1    10.20.24.17  10.20.25.18  44064   5001         TCP       1       1            0:00:59:59  7066      9895451   3826     257392
established
zp1       1    10.20.24.17  10.20.25.18  44065   5001         TCP       1       1            0:00:59:59  13471     18868856  7440     504408
established
zp1       1    10.20.24.17  10.20.25.18  44066   5001         TCP       1       1            0:00:59:59  8450      11834435  4435     295718
established
vEdge# clear policy zbfw sessions
vEdge# show policy zbfw sessions

ZONE PAIR      SOURCE IP    DESTINATION  SOURCE  DESTINATION           SOURCE  DESTINATION  IDLE        OUTBOUND  OUTBOUND  INBOUND  INBOUND
FILTER
NAME      VPN  ADDRESS      IP ADDRESS   PORT    PORT         PROTOCOL  VPN     VPN          TIMEOUT     PACKETS   OCTETS    PACKETS  OCTETS   STATE

-------------------------------------------------------------------------------------------------------------------------------------------------
zp1       1    10.20.24.17  10.20.25.18  44061   5001         TCP       1       1            0:00:59:59  0         0         0        0
established
zp1       1    10.20.24.17  10.20.25.18  44062   5001         TCP       1       1            0:01:00:00  0         0         0        0
established
zp1       1    10.20.24.17  10.20.25.18  44063   5001         TCP       1       1            0:00:59:59  0         0         0        0
established
zp1       1    10.20.24.17  10.20.25.18  44064   5001         TCP       1       1            0:00:59:59  0         0         0        0
established
zp1       1    10.20.24.17  10.20.25.18  44065   5001         TCP       1       1            0:00:59:59  0         0         0        0
established
zp1       1    10.20.24.17  10.20.25.18  44066   5001         TCP       1       1            0:00:59:59  0         0         0        0
established
```

Related Topics

show policy zbfw sessions, on page 980

clear pppoe statistics

Zero PPPoE statistics.

clear pppoe statistics

Command History

Release	Modification
15.3.3	Command introduced.

Examples

```
vEdge# show pppoe statistics

      pppoe_tx_pkts             :      73
      pppoe_rx_pkts             :      39
      pppoe_tx_session_drops    :      0
      pppoe_rx_session_drops    :      0
      pppoe_inv_discovery_pkts  :      0
      pppoe_ccp_pkts            :      12
      pppoe_ipcp_pkts           :      16
      pppoe_lcp_pkts            :      35
      pppoe_padi_pkts           :      4
      pppoe_pado_pkts           :      2
      pppoe_padr_pkts           :      2
      pppoe_pads_pkts           :      2
      pppoe_padt_pkts           :      2

vEdge# clear pppoe statistics
vEdge# show pppoe statistics

      pppoe_tx_pkts             :      0
      pppoe_rx_pkts             :      0
      pppoe_tx_session_drops    :      0
      pppoe_rx_session_drops    :      0
      pppoe_inv_discovery_pkts  :      0
      pppoe_ccp_pkts            :      0
      pppoe_ipcp_pkts           :      0
      pppoe_lcp_pkts            :      0
      pppoe_padi_pkts           :      0
      pppoe_pado_pkts           :      0
      pppoe_padr_pkts           :      0
      pppoe_pads_pkts           :      0
      pppoe_padt_pkts           :      0
```

Related Topics

show ppp interface, on page 981
show pppoe session, on page 981
show pppoe statistics, on page 982

clear reverse-proxy context

Clear an installed proxy certificate and reset the control connections that are associated with the proxy (on vEdge routers only).

clear reverse-proxy context

Command History

Release	Modification
18.2	Command introduced.

Examples

Clear the installed proxy certificate on a vEdge router

```
vEdge# show certificate reverse-proxy

Reverse proxy certificate
-------------------

Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 2 (0x2)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, O=Viptela, OU=ViptelaVmanage,
CN=813fd02c-acca-4c19-857b-119da60f257f
        Validity
            Not Before: May 11 21:43:29 2018 GMT
            Not After : May  4 21:43:29 2048 GMT
       Subject: C=US, ST=California, CN=47bd1f2b-3abe-41cd-9b9f-e84db7fd2377, O=ViptelaClient

        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:2e:f3:68:8b:0d:7b:3f:0d:ca:a3:74:7c:dd:
                    70:0c:25:26:ac:8b:8f:37:60:00:4b:fc:4d:3f:11:
                    d9:94:df:31:4c:f8:a5:88:8b:65:e8:d5:21:7c:47:
                    21:34:8e:93:c7:7f:24:6d:2b:4c:51:9b:a7:f8:8f:
                    0f:e2:f4:85:0e:49:dd:ed:6b:ed:40:d2:5e:a0:7c:
                    a6:7f:26:d2:ff:2b:a4:39:34:51:0f:3d:7f:85:31:
                    b4:c9:ec:06:d4:37:03:ac:41:5a:34:3d:96:4f:d9:
                    cd:be:e3:22:7a:9b:24:1b:3b:c9:5c:c5:48:97:5d:
                    7a:7a:8e:80:ab:e8:a2:8f:b3:35:45:07:b0:46:2e:
                    b9:d5:4c:8c:42:6a:1e:8a:90:a4:11:76:6f:61:07:
                    1d:2a:c9:9d:57:42:87:3f:5b:d1:91:0b:7c:8c:f2:
                    62:68:a7:e3:d5:da:c9:40:a3:c4:1a:ae:4f:d5:6c:
                    2e:ec:2e:dc:2f:06:31:a8:da:13:b0:e4:3a:16:17:
                    2d:7a:30:ee:b2:e0:d5:93:a9:53:ee:e5:b2:68:5a:
                    d9:2b:82:93:5e:65:7d:63:8f:0a:8c:39:0b:f0:64:
                    ec:4a:cb:91:c0:59:37:31:dc:31:75:40:df:2c:8f:
                    67:f1:bf:b6:5e:40:ce:a5:c6:59:d0:c4:e2:11:2b:
                    0c:c3
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         0b:5e:9d:30:29:dd:4a:25:5f:44:6d:02:15:35:72:d9:44:33:
         fa:a7:b5:d5:f5:68:09:47:81:ba:22:46:1a:c5:aa:a6:69:10:
         93:40:8c:18:34:b5:1f:57:a3:2d:7d:9f:86:76:b9:51:2d:2c:
         5f:ce:74:1c:66:5e:1d:e5:8c:26:02:e4:63:fe:b1:1b:a5:e2:
         3a:03:07:23:ca:43:38:93:49:cf:3c:d0:5d:c3:33:cd:d6:26:
         8b:a9:b8:5f:63:80:99:09:d6:dd:fb:14:43:bf:17:03:6b:2d:
         59:c5:cb:41:6d:7e:9e:c8:27:13:10:d5:05:df:cc:b2:7a:81:
         b1:9f:11:60:3a:69:67:25:b4:f3:ab:36:a7:d1:88:bb:7b:72:
         b2:b4:63:df:4b:42:74:7f:99:04:4a:bb:76:0a:46:53:71:1a:
         db:8a:1c:93:8f:fa:ae:5b:8d:9e:e5:10:07:a1:5d:d9:88:a1:
```

```
        2d:04:13:9f:11:c8:8b:6b:b0:59:f9:48:14:c8:c4:9e:ff:6a:
        38:12:92:e3:20:fa:f7:f0:58:34:16:62:7c:6a:c9:32:41:7e:
        53:4e:e4:8c:af:4a:e3:14:77:b3:b7:d4:0e:17:1e:f6:13:b1:
        f0:9c:af:6e:38:3c:cc:24:79:3e:01:4b:3f:d2:12:f2:1c:f5:
        75:c6:6c:f3
vEdge# clear reverse-proxy context
vEdge# show reverse-proxy certificate
vEdge#
```

Related Topics

show certificate reverse-proxy, on page 771
show control connections, on page 788

clear system statistics

Clear system-wide forwarding statistics.

clear system statistics

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show system statistics
                        rx_pkts:         13330516
                       rx_drops:              322
                         ip_fwd:         18810968
                     ip_fwd_arp:               10
                ip_fwd_to_egress:          9597667
                ip_fwd_null_nhop:              109
                   ip_fwd_to_cpu:          2134168
                ip_fwd_rx_ipsec:          7149794
                        rx_bcast:               29
                        rx_mcast:           118251
             rx_mcast_link_local:           118251
           rx_implicit_acl_drops:            41570
                 rx_ipsec_decap:          7148928
              rx_spi_ipsec_drops:              854
                 rx_replay_drops:               12
                 rx_non_ip_drops:          1731850
           bfd_tx_record_changed:            13924
         rx_arp_rate_limit_drops:               43
          rx_arp_non_local_drops:            17226
                    rx_arp_reqs:           176215
                rx_arp_replies:            23142
                  arp_add_fail:              311
                        tx_pkts:         24625271
                       tx_bcast:               85
                       tx_mcast:           118187
                ip_disabled_tx:                3
             tx_fragment_needed:             2918
              fragment_df_drops:              279
                   tx_fragments:             5278
```

```
                      tx_ipsec_pkts:          7560752
                     tx_ipsec_encap:          7560752
                  tx_pre_ipsec_pkts:          7558392
                 tx_pre_ipsec_encap:          7558392
                     tx_arp_replies:           176217
                        tx_arp_reqs:            23163
                     tx_no_arp_drop:                1
                        bfd_tx_pkts:          7510883
                        bfd_rx_pkts:          7119130
                      bfd_rec_down:                18
                      rx_pkt_qos_0:          2148610
                      rx_pkt_qos_1:           157403
                      rx_pkt_qos_2:         16623962
                      rx_pkt_qos_4:               10
                      rx_pkt_qos_7:          9251604
            icmp_rx.echo_requests:               15
             icmp_rx.echo_replies:           257071
             icmp_rx.host_unreach:               13
             icmp_rx.port_unreach:               58
          icmp_rx.dst_unreach_other:             11
          icmp_rx.fragment_required:             28
                icmp_rx.ttl_expired:              9
            icmp_tx.echo_requests:           257764
             icmp_tx.echo_replies:                2
           icmp_tx.network_unreach:               28
             icmp_tx.port_unreach:              137
          icmp_tx.fragment_required:            279

vEdge# clear system statistics

vEdge# show system statistics
                           rx_pkts:               67
                            ip_fwd:               90
                  ip_fwd_to_egress:               44
                     ip_fwd_to_cpu:               17
                   ip_fwd_rx_ipsec:               30
                           rx_mcast:                1
                rx_mcast_link_local:                1
                     rx_ipsec_decap:               30
                    rx_non_ip_drops:                6
                     rx_arp_replies:                1
                           tx_pkts:              106
                      tx_ipsec_pkts:               31
                     tx_ipsec_encap:               31
                  tx_pre_ipsec_pkts:               31
                 tx_pre_ipsec_encap:               31
                        tx_arp_reqs:                1
                        bfd_tx_pkts:               31
                        bfd_rx_pkts:               30
                      rx_pkt_qos_0:               14
                      rx_pkt_qos_1:                2
                      rx_pkt_qos_2:               67
                      rx_pkt_qos_7:               46
               icmp_rx.echo_replies:                1
              icmp_tx.echo_requests:                1
```

Related Topics

show system statistics, on page 1015

clear tunnel statistics

Zero the information about the packets transmitted and received on the IPsec connections that originate on the local router (on vEdge routers only).

clear tunnel statistics

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# clear tunnel statistics

vEdge# show tunnel statistics
Tunnel[986]: Tunnel Type IPSec 10.0.0.8->75.21.94.46
                        rx_pkts:               2
                      rx_octets:             284
                        tx_pkts:               4
                      tx_octets:             388
Tunnel[986] BFD Record Index 1740:
                        tx_pkts:               2
                        rx_pkts:               2
                    Tx Err Code:            None
                    Rx Err Code:            None
Tunnel[1697]: Tunnel Type IPSec 10.0.0.8->25.6.101.120
                        rx_pkts:               2
                      rx_octets:             284
                        tx_pkts:               4
                      tx_octets:             388
Tunnel[1697] BFD Record Index 1717:
                        tx_pkts:               2
                        rx_pkts:               2
                    Tx Err Code:            None
                    Rx Err Code:            None
...
```

Related Topics

show tunnel statistics, on page 1033

clear wlan radius-stats

Clear the statistics about the sessions with RADIUS servers being used for WLAN authentication (on vEdge routers only).

clear wlan radius-stats [**vap** *number*]

Syntax Description

vap *number*	VAP Interface: Virtual access point instance. Range: 0 through 3.

Command History

Release	Modification
17.1	Command introduced.

Related Topics

show interface, on page 827
show wlan clients, on page 1038
show wlan interfaces, on page 1039
show wlan radios, on page 1040
show wlan radius, on page 1042

clock

Set the time and date on the device. If you have configured NTP on the device, the NTP time overwrites the time and date that you set with the **clock** command.

clock set date *ccyy-mm-dd*

clock set time *hh*:*mm*:*ss.sss*

Syntax Description

ccyy-mm-dd	Date: Set the date by specifying four-digit year, two-digit month, and two-digit day. The year can be from 2000 to 2060.
hh:*mm*:*ss.sss*	Time: Set the time by two-digit hour (using a 24-hour clock), two-digit minute, two-digit seconds, and an optional three-digit hundredths of seconds.

Note You must set the time and date in a single command, but the order in which you specify them does not matter.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# clock set time 14:30:00 date 2013-11-25
vEdge# show uptime
14:30:03 up 13:51, 1 user, load average: 0.00, 0.01, 0.05
```

Related Topics

ntp, on page 356
show uptime, on page 1035

commit

Confirm or cancel a pending commit operation. You issue this **commit** command from operational mode. You establish a pending commit operation by using the **commit confirmed** configuration session management command.

commit (**abort** | **confirm**) [**persist-id** *id*]

Syntax Description

confirm	Confirm a Pending Commit Operation: Confirm a pending commit operation that was issued with the **commit confirmed** configuration command. You must confirm the commit operation with the time specified with the **commit confirmed** command; otherwise, the commit is canceled.
abort	Halt a Pending Commit Operation: Halt a pending commit operation that was issued with the **commit confirmed** command. This is the default operation for a pending commit operation. The commit is also canceled if the CLI session is terminated before you issue a **commit confirm** command.
persist-id *id*	Token to Identify the Pending Commit Operation: If you specified a token, *id*, when you initiated the pending commit operation, specify that token to either cancel or confirm the commit.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# commit confirm
Commit complete. Configuration is now permanent.
```

Related Topics

commit, on page 1074
show configuration commit list, on page 783

complete-on-space

Have the CLI automatically complete a command name when you type an unambiguous string and then press the space bar, or have the CLI list all possible completions when you type an ambiguous string and then press the space bar.

complete-on-space (**false** | **true**)

Syntax Description

false	Do Not Perform Command Completion: Do not have the CLI perform command completion when you press the space bar. This is the default setting.
true	Perform Command Completion: Have the CLI perform command completion when you press the space bar.

Command History

Release	Modification
14.1	Command introduced.
14.2	Default changed from **true** to **false** in Release 14.2.

Examples

```
vEdge# complete-on-space false
vEdge# hel
----------^
syntax error: expecting
vEdge# complete-on-space true
vEdge# help
```

Related Topics

show cli, on page 778

config

Enter configuration mode for vEdge devices. In configuration mode, you are editing a copy of the running configuration, called the candidate configuration, not the actual running configuration. Your changes take effect only when you issue a **commit** command.

Note Cisco IOS XE routers such as aggregation and integrated services routers should use the command **config-transaction** to enter configuration mode. The **config terminal** command is not supported on SD-WAN routers.

config (**exclusive** | **no-confirm** | **shared** | **terminal**)

Syntax Description

(none)	Edit a private copy of the running configuration. This private copy is not locked, so another user could also edit it at the same time.
terminal	Allow Editing from This Terminal Only: Edit a private copy of the running configuration. This private copy is not locked, so another user could also edit it at the same time.
no-confirm	Do Not Allow a Commit Confirmation: Edit a private copy of the running configuration and do not allow the **commit confirmed** command to be used to commit the configuration.
exclusive	Exclusive Edit: Lock the running configuration and the candidate configuration, and edit the candidate configuration. No one else can edit the candidate configuration as long as it is locked.
shared	Shared Edit: Edit the candidate configuration without locking it. This option allows another person to edit the candidate configuration at the same time.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# config
Entering configuration mode terminal
vEdge(config)#
```

Related Topics

file list, on page 637
load, on page 1079

controller-mode

To switch from autonomous mode to controller and from controller mode to autonomous mode use the controller-mode command in Privileged EXEC mode.

controller-mode { **enable** | **disable** | **reset** }

Syntax Description

enable	Enables controller mode.
disable	Disables controller mode.
reset	Resets device to day 0 configuration mode.

Command Default

The device exists in the day 0 configuration mode.

Command Modes Privileged EXEC #

Command History

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

Usage Guidelines When you switch the device mode from autonomous to controller, the startup configuration and the information in NVRAM (certificates), are erased. This action is same as the **write erase**. If you switch back to autonomous mode, the IOS XE configuration is not restored because the startup configuration is empty. You have to manually restore configuration from the backup..

When you switch the device mode from controller to autonomous, all Yang-based configuration is preserved and can be reused if you switch back to controller mode. If you switch back to controller mode, the original configuration in controller mode is preserved.

If the mode change CLI is invoked from a Telnet terminal, the mode change operation is not permitted unless auto-boot variables are set in ROMmon.

Example

Use the **controller-mode disable** command the device to autonomous mode.

```
Device# controller-mode disable
```

Use the **controller-mode enable** command switches the device to Controller mode.

```
Device# controller-mode enable
```

debug

Enable and disable debugging mode for all or selected software function. Debug output is placed in the /var/log/tmplog/vdebug file on the local device.

[**no**] **debug all**

[**no**] **debug aaa login** (**radius** | **tacacs**)

[**no**] **debug bgp** (**all** | **events** | **fsm** | **ipcs** | **packets**) **vpn** *vpn-id*

[**no**] **debug cflowd** (**cli** | **events** | **ipc** | **misc** | **pkt_tx**) [**level** (**high** | **low**)]

[**no**] **debug chmgr all**

[**no**] **debug cloudexpress** (**events** | **ftm** | **omp** | **rtm** | **ttm**) [**level** (**high** | **low**)]

[**no**] **debug confd** (**developer-log** [**level** (**high** | **low**)] | **snmp**)

[**no**] **debug config-mgr** (**events** | **pppoe** | **ra**) [**level** (**high** | **low**)]

[**no**] **debug dbgd** (**events**)

[**no**] **debug dhcp-client** (**all** | **events** | **packets**)

[**no**] **debug dhcp-helper** (**all** | **events** | **packets**)

[**no**] **debug fpm** (**all** | **config** | **dpi** | **policy** | **ttm**)

[**no**] **debug ftm all**

[**no**] **debug igmp** (**config** | **events** | **fsm** | **ipc** | **packets**) [**level** (**high** | **low**)]

[**no**] **debug iked** (**all** | **confd** | **error** | **events** | **misc**) [**level** (**high** | **low**)]

[**no**] **debug netconf traces**

[**no**] **debug omp** (**all** | **events** | **ipcs** | **packets**)

[**no**] **debug ospf** (**all** | **events** | **ipcs** | **ism** | **lsa** | **nsm** | **nssa** | **packets**) **vpn** *vpn-id*

[**no**] **debug pim** (**auto-rp** | **events** | **fsm** | **ipcs** | **packets**) [**level** (**high** | **low**)] **vpn** *vpn-id*

[**no**] **debug platform software sdwan tracker**

[**no**] **debug resolver events** [**level** (**high** | **low**)]

[**no**] **debug rtm** (**events** | **ipc** | **next-hop** | **packets** | **rib**) **vpn** *vpn-id*

[**no**] **debug snmp events** [**level** (**high** | **low**)]

[**no**] **debug sysmgr all**

[**no**] **debug transport events** [**level** (**high** | **low**)]

[**no**] **debug tcpd** [**level** (**high** | **low**)]

[**no**] **debug ttm events**

[**no**] **debug vrrp** (**all** | **events** | **packets**) **vpn** *vpn-id*

Syntax Description

[**no**] **debug all**	All: Control debugging for all software functions that can be debugged.
[**no**] **debug aaa login** (**radius** | **tacacs**)	AAA Login via RADIUS or TACACS: Control debugging for login attempts using RADIUS or TACACS.
[**no**] **debug bgp** (**all** | **events** | **fsm** | **ipcs** | **packets**) **vpn** *vpn-id*	BGP: Control debugging for BGP: • **all**—Control the debugging of all BGP events, finite-state machine transitions, interprocess communications, and packets. • **events**—Control the debugging of BGP events, including damping events, finite-state machine events and transitions, keepalive message events, next-hop events, and routing table update events. • **fsm**—Control the debugging of BGP finite-state machine transitions. • **ipcs**—Control the debugging of all BGP interprocess communications. • **packets**—Control the debugging of all BGP protocol packets. • **vpn** *vpn-id*—Specify the VPN in which to perform debugging.

[**no**] **debug cflowd** (**cli** | **events** | **ipc** | **misc** | **pkt_tx**) [**level** (**high** | **low**)]	Cflowd Traffic Flow Monitoring: Control debugging for cflowd: • **cli** —Control the debugging of messages that are logged as the result of a configuration change made either directly on the vEdge router or because the changes have been pushed from the vSmart controller to the router. • **events** —Control the debugging of events to which the cflowd process (daemon) responds, including when the process connects with a collector or loses connectivity with it, and when the source-interface as configured in the vSmart template is removed. • **ipc** —Control the debugging of all cflowd interprocess communications. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team. • **misc** —Control the debugging of miscellaneous cflowd events. • **pkt_tx** —Control the debugging of cflowd packet transmissions.
[**no**] **debug chmgr all**	Chassis Manager: Control debugging for the chassis manager.
[**no**] **debug cloudexpress** (**events** | **ftm** | **omp** | **rtm** | **ttm**) [**level** (**high** | **low**)]	Cloud OnRamp for SaaS: Control debugging for Cloud OnRamp for SaaS (formerly CloudExpress service). • **events**—Control the debugging of events to which the Cloud OnRamp for SaaS process (daemon) responds, including when the process connects with a collector or loses connectivity with it, and when the source-interface as configured in the vSmart template is removed. • **ftm**—Control debugging of the communication between Cloud OnRamp for SaaS and the forwarding table manager. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team. • **omp**—Control the debugging of all Cloud OnRamp for SaaS OMP operations. • **rtm**—Control the debugging of communication between the Cloud OnRamp for SaaS and the route table manager. • **ttm**—Control the debugging of communication between the Cloud OnRamp for SaaS and the tunnel table manager.

[**no**] **debug config-mgr** (**events** | **pppoe** | **ra**) [**level** (**high** | **low**)]	Configuration Manager: Control debugging for the configuration manager. • **events**—Control the debugging of events to which the configuration manager process (daemon) responds, including when the process connects with a collector or loses connectivity with it, and when the source-interface as configured in the vSmart template is removed. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco engineering team. • **pppoe**—Control the debugging of all Cloud OnRamp for SaaS OMP operations. • **ra**—Control the debugging of route advertisements to which the configuration manager responds.
[**no**]**debug dbgd events**	Debugger Process: Control debugging for the debugger process itself. • **events**—Control the debugging of events to which the debugger process (daemon) responds.
[**no**] **debug dhcp-client** (**all** | **events** | **packets**)	DHCP Client: Control the debugging of Dynamic Host Configuration Protocol (DHCP) client activities. • **all**—Control the debugging of all DHCP client events and packets. • **events**—Control the debugging of DHCP client protocol events. • **packets**—Control the debugging of all DHCP client packets.
[**no**] **debug dhcp-helper** (**all** | **events** | **packets**)	DHCP Helper: Control the debugging of Dynamic Host Configuration Protocol (DHCP) helper activities. • **all**—Control the debugging of all DHCP helper events and packets. • **events**—Control the debugging of DHCP helper protocol events. • **packets**—Control the debugging of all DHCP helper packets.

[**no**] **debug fpm** (**all** | **config** | **dpi** | **policy** | **ttm**)	Forwarding Policy Manager: Control debugging for the forwarding policy manager: • **all**—Control 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**—Control the debugging of messages that are logged as a result of a policy configuration change made either directly on the vEdge router or because the changes have been pushed from the vSmart controller to the router. • **dpi**—Control the debugging of all application-aware routing (deep packet inspection) events. • **policy**—Control the debugging of messages that are logged as the result of policy programming events. • **ttm**—Control the debugging of communication between the forwarding policy manager and the tunnel table manager.
[**no**] **debug ftm all**	Forwarding Table Manager: Control debugging for the forwarding table manager operations.
[**no**] **debug igmp** (**config** | **events** | **fsm** | **ipc** | **packets**) [**level** (**high** | **low**)]	IGMP: Control debugging for IGMP. • **events**—Control the debugging of IGMP events, including finite-state machine events and transitions, keepalive message events, next-hop events, and routing table update events. • **fsm**—Control the debugging of IGMP finite-state machine transitions. • **ipcs**—Control the debugging of all IGMP interprocess communications. • **packets**—Control the debugging of all IGMP protocol packets.
[**no**] **debug iked** (**all** | **confd** | **error** | **events** | **misc**) [**level** (**high** | **low**)]	IKE: Control debugging for the forwarding policy manager. • **all**—Control the debugging of all events related to IKE. • **confd**—Control the debugging of Netconf activity to log all IKE-related Netconf configuration messages between the local device and the vManage NMS. • **error**—Control the debugging of IKE errors. • **events**—Control the debugging of IKE protocol events. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team. • **misc**—Control the debugging of miscellaneous IKE events.

[**no**] **debug netconf traces**	Netconf: Enable and disable Netconf activity to log all Netconf configuration messages between the local device and the vManage NMS. Netconf debug messages are logged to the /var/log/confd/netconf.trace file.
[**no**] **debug omp** (**all** | **events** | **ipcs** | **packets**)	OMP: Control the debugging of OMP. • **all**—Control the debugging of all OMP events, interprocess communications, and packets. • **events**—Control the debugging of OMP events. • **ipcs**—Control the debugging of all OMP interprocess communications. • **packets**—Control the debugging of all OMP protocol packets.
[**no**] **debug ospf** (**all** | **events** | **ipcs** | **ism** | **lsa** | **nsm** | **nssa** | **packets**) **vpn** *vpn-id*	OSPF: Control the debugging of OSPF. • **all**—Control the debugging of all OSPF functions. • **events**—Control the debugging of OSPF events, including adjacencies, flooding information, designated router selection, and shortest path first (SPF) calculations. • **ipcs**—Control the debugging of all OSPF interprocess communications. • **ism**—Control the debugging of OSPF interface state machine transitions. • **nsm**—Control the debugging of OSPF network tate machine transitions. • **lsa**—Control the debugging of OSPF LSA messages. • **nssa**—Control the debugging of OSPF NSSA messages. • **packets**—Control the debugging of all OSPF protocol packets.
[**no**] **debug pim** (**auto-rp** | **events** | **fsm** | **ipcs** | **packets**) [**level** (**high** | **low**)] **vpn** *vpn-id*	PIM: Control debugging for PIM. • **all**—Control the debugging of all PIM events, finite-state machine transitions, interprocess communications, and packets. • **events**—Control the debugging of PIM events, including finite-state machine events and transitions, keepalive message events, next-hop events, and routing table update events. • **fsm**—Control the debugging of PIM finite-state machine transitions. • **ipcs**—Control the debugging of all PIM interprocess communications. • **packets**—Control the debugging of all PIMP protocol packets. • **vpn** *vpn-id*—Specify the VPN in which to perform debugging.
[**no**] **debug platform software sdwan tracker**	Service chaining: (Cisco IOS XE Catalyst SD-WAN devices) Display the service log for the tracker, which probes service devices periodically to test whether the devices are reachable.

[**no**] **debug resolver events** [**level** (**high** | **low**)]	Resolver: Control debugging for all resolver process events. The resolver process handles a plethora of tasks, including tracking ARP, MAC addresses, DNS, and connected interfaces. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team.
[**no**] **debug rtm** (**events** | **ipc** | **next-hop** | **packets** | **rib**) **vpn** *vpn-id*	Route Table Manager: Control debugging for the route table manager. • **events**—Control the debugging of route table manager events. • **ipc**—Control the debugging of all route table manager interprocess communications. • **next-hop**—Control the debugging of the route table manager handling of next hops. • **packets**—Control the debugging of the route table manager handling of route exchange packets. • **rib**—Control the debugging of route table manager communication with the route table. • **vpn** *vpn-id*—Specify the VPN in which to perform debugging.
[**no**] **debug snmp events** [**level** (**high** | **low**)]	SNMP: Control debugging for all SNMP events. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team.
[**no**] **debug sysmgr all**	System Manager: Control debugging for the system manager.
[**no**] **debug tcpd** [**level** (**high** | **low**)]	TCP Optimization Process: Control debugging for TCP optimization. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team.
[**no**] **debug transport events** [**level** (**high** | **low**)]	Transport Process: Control debugging for all vtracker transport process events. The vtracker process pings the vBond orchestrator every second. • **level** (**high** | **low**)—Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco SD-WAN engineering team.

[**no**] **debug ttm events**	Tunnel Table Manager: Control debugging for all tunnel table manager events.
[**no**] **debug vrrp** (**all** | **events** | **packets**) **vpn** *vpn-id*	VRRP: Control debugging for the Virtual Router Redundancy Protocol (VRRP). • **all**—Control the debugging of all VRRP events and packets. • **events**—Control the debugging of VRRP events. • **packets**—Control the debugging of VRRP packets.

Command History

Release	Modification
14.1	Command introduced.
16.3	Starting with Release 16.3, output is placed in the /var/log/tmplog/vdebug file, not the /var/log/vdebug file.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Added **debug platform software sdwan tracker**.

debug packet-trace condition

To enable packet tracing on Cisco vEdge devices, use the **debug packet-trace condition** command in privileged EXEC mode.

debug packet-trace condition [**start** | **stop**] [**bidirectional**] [**circular**] [**destination-ip** *ip-address*] [**global-stat**] [**ingress-if** *interface*] [**logging**] [**source-ip** *ip-address*] [**vpn-id** *vpn-id*]

Syntax Description

bidirectional	(Optional) Enables bidirectional flow debug for source IP and destination IP.
circular	(Optional) Enables circular packet tracing. In this mode, the 1024 packets in the buffer are continuously over-written.
clear	(Optional) Clears all debug configurations and packet tracer memory.
destination-ip	(Optional) Specifies destination IPv4 address.
global-stat	(Optional) Specifies the match on select global statistic counter name.
ingress-if	(Optional) Specifies ingress interface name. Note: It is must to choose VPN to configure the interface.
logging	(Optional) Enables packet tracer debug logging.
source-ip	(Optional) Specifies source IP address.
start	(Optional) Starts conditional debugging.
stop	(Optional) Stops conditional debugging.

vpn-id	(Optional) Enables packet tracing for the specified VPN.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.5.1	This command was introduced.
Cisco SD-WAN Release 20.8.1	A new keyword **global-stat** is added.

Usage Guidelines

The parameters after the keywords **start** and **stop** in the command syntax 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 10.1.1.1
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 mpls match-inner

To match IPv4 or IPv6 traffic over an MPLS network on Cisco vEdge devices, use the **debug platform condition mpls match-inner** command in privileged EXEC mode.

debug platform condition [interface { *interface-name interface-number* } **]**
mpls *depth-of-mpls-label* **match-inner {ipv4 | ipv6}** { *ipv4-source-prefix* | *any* | *host* | *payload-offset* | *protocol* } { *ipv4-destination-prefix* | *any* | *host* } { **application** | **both** | **ingress** | **egress** } [**bidirection**] [**allow-no-label**]

no debug platform condition [interface { *interface-name interface-number* } **]**
mpls *depth-of-mpls-label* **match-inner {ipv4 | ipv6}** { *ipv4-source-prefix* | *any* | *host* | *payload-offset* | *protocol* } { *ipv4-destination-prefix* | *any* | *host* } { **application** | **both** | **ingress** | **egress** } [**bidirection**] [**allow-no-label**]

Syntax Description

debug	Debug device operations, generated or received traffic, and any error messages.
platform	Debug specific network platforms based on your requirement.
condition	Specify conditions to debug based on your requirement.
interface	(Optional) Debug a specific interface of your choice.
interface-name	Specify the the interface name.
interface-number	Specify the interface number.

mpls	Debug the MPLS network.
source prefix	Specifies IPv4 or IPv6 source prefix.
application	Debug Application conditions.
both	Debug ingress and egress debug simultaneously.
egress	Debug egress only.
ingress	Debug ingress only.
match-inner	Debug inline ACL filters for overlay packet over MPLS.
ipv4	Debug IPv4 conditions .
ipv6	Debug IPv6 conditions.
destination prefix	Specifies IPv4 or IPv6 destination prefix.
any	Specifies any source prefix.
payload-offset	Configures the ineer payload offset to locate the overlap IPv4 and IPv6 header.
host	Specifies a single destination host.
bidirection	(Optional) Allows to fileter packets in bidirection.
allow-no-label	(Optional) Allows to filter packets without MPLS labels.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	A new command **debug platform condition mpls** is added.

Example

The following example shows how to configure conditions for packet tracing:

```
Device# debug platform condition mpls match-inner ipv4
Device# debug platform condition mpls match-inner ipv4 any any
Device# debug platform condition mpls match-inner ipv4 any any both
Device# debug platform condition mpls match-inner ipv4 any any both
Device# debug platform condition mpls match-inner ipv4 any any both allow-no-label
```

debug-vdaemon

Enable and disable debugging mode for vdaemon software function. Debug output is placed in the /var/log/tmplog/vdebug file on the local device.

debug vdaemon { **all** | **confd** | **error** | **events** | **hello** | **misc** | **packets** } [**high** | **low**]
no debug vdaemon { **all** | **confd** | **error** | **events** | **hello** | **misc** | **packets** } [**high** | **low**]

Syntax Description

{**all** | **confd** | **error** | **events** | **hello** | **misc** | **packets**} {**high** | **low**}	vDaemon Process: Control debugging for vDaemon, the Cisco SD-WAN software process: • **all**: Control the debugging of all vdaemon process functions. • **confd**: Control the debugging of vdaemon process CLI functions. • **error**: Control the debugging error of vdaemon actions. • **events**: Control the debugging of vdaemon process events. • **hello**: Control the debugging of vdaemon hello packets. • **misc**: Control the debugging of miscellaneous vdaemon process events. • **packets**: Control the debugging of all vdaemon process packets. • **high**: Displays verbose logging. • **low**: Displays minimal logging.

Command History

Release	Modification
14.1	Command introduced.
16.3	Starting with Release 16.3, output is placed in the /var/log/tmplog/vdebug file, not the /var/log/vdebug file.
Cisco SD-WAN Release 20.5.1	Added **hello** keyword for **debug vdaemon** command.

debug vdaemon peer

Enable and disable debugging mode for vdaemon software function. Debug output is placed in the /var/log/tmplog/vdebug file on the local device.

debug vdaemon peer public-ip *ip-address* **public-port** *port-address* **facility** { **all** | **confd** | **error** | **events** | **hello** | **misc** | **packet** } **level** { **high** | **low** }
no debug vdaemon peer public-ip *ip-address* **public-port** *port-address* **facility** { **all** | **confd** | **error** | **events** | **hello** | **misc** | **packet** } **level** { **high** | **low** }

Syntax Description

public-ip *ip-address*	Speicifes peer public ip address.
public-port *port-address*	Specifies peer public port address. Range: 0 to 65535

facility{**all** | **confd** | **error** | **events** | **hello** | **misc** | **packet**}	Facility: Control debugging of miscellaneous vdaemon actions: • **all**: Control the debugging of all vdaemon process functions. • **confd**: Control the debugging of vdaemon process CLI functions. • **error**: Control the debugging error of vdaemon actions. • **events**: Control the debugging of vdaemon process events. • **hello**: Control the debugging of vdaemon hello packets. • **misc**: Control the debugging of miscellaneous vdaemon process events. • **packet**: Control the debugging of all vdaemon process packets.
level{**high** | **low**}	Set the detail of the comments logged by the debugging operation. The default level, **low**, provides comments sufficient to help you understand the actions that are occurring. The level **high** provides greater detail for the live debugging that might typically be performed by the Cisco engineering team.

Command History

Release	Modification
Cisco SD-WAN Release 20.5.1	This command was introduced.

Examples

The following is a sample output for **debug vdaemon peer** command. Verbose logs for a particular peer can be enabled, and hello log is displayed:

```
Device# debug vdaemon peer public-ip 10.0.12.22 public-port 23456 facility all level high

IP addr: 10.0.12.22 | Port: 23456 | Peer exist: true |  misc:high  events:high  confd:high
  pkt:high  hello:high  error:high

Mar 10 11:32:56 vm6 VDAEMON[1592]: vbond_proc_msg[4957]: %VDAEMON_DBG_HELLO-3: peer publoc:
 10.0.12.22:23456
Received a Hello from .. 10.0.12.22:23456 on loopback2 (my count 2 hello_vsmart_count 0)
(my count 1 hello_vmanage_count 1)
Mar 10 11:32:56 vm6 VDAEMON[1592]: vdaemon_vm_rebalance_needed[805]: %VDAEMON_DBG_ERROR-3:
 peer publoc: 10.0.12.22:23456
Peer vmanage sys-ip 172.16.255.22 is the chosen one
```

exit

Exit from the CLI session. The **exit** and **quit** commands do the same thing.

exit

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# exit
My-MacBook-Pro:~ me$
```

Related Topics

quit, on page 652
vshell, on page 1068

file list

List the files in a directory on the Cisco SD-WAN device.

file list *directory*

Syntax Description

directory	Name of a Directory: List the files in the specified directory on the Cisco SD-WAN device.

Examples

```
vEdge# file list /var
backups
confd
crash
lib
local
lock
log
run
spool
tmp
volatile
```

Command History

Release	Modification
14.1	Command introduced.

Related Topics

file show, on page 637
save, on page 1114

file show

Display the contents of a file on the Cisco SD-WAN device.

file show *filename*

Syntax Description

filename	Name of a Directory: Name of a file on the Cisco SD-WAN device.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# file list
x.csr
vEdge# file show x.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDOzCCAiMCAQAwgboxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEOMAwGA1UECxMFYXZpdmExFDASBgNVBAoTC3ZJ
UHRlbGEgSW5jMTkwNwYDVQQDFDBWU21hcnRfMDdfMDFfMjAxNF8yM18yM181Ml80
MDc2Mzg1NzcudmlwdGVsYS5jb20xIjAgBgkqhkiG9w0BCQEWE3N1cHBvcnRAdmlw
dGVsYS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2ebu1o5FJ
419xtFhQOf0E7OjDzRvDvC9IUcOPayMMnJgN54EXi3ReVNjsQCn3+P8nPa9hQFjD
3wI03vMVqw4DCVsNmv/lhVsK0PpiV2ALThu4sWtLUPhOJcBOjW8sRcgYP6FKeWaH
Bolx4e+V5vIP52pbTzyIIF/ISdQqKaoMTDcugvKUkrP/xTKpQvvNrOz7eyJUbc8B
IrHyAirm32gFZc8kPeOM6QZTRtVWn4u0cjU9i/DYzByu5HpJqRucrFG5YiM/Ev9p
f8nalbT1Nrmh7RTkTyE276g+nLl8IyTIIrQlbG58bxX0x2inoJP12zV828Fm2AuA
KEEKXzN/bBTfAgMBAAGgOzA5BgkqhkiG9w0BCQ4xLDAqMAkGA1UdEwQCMAAwHQYD
VR0OBBYEFNcvAamf8WANRkKbFjBo3Hwi83BxMA0GCSqGSIb3DQEBBQUAA4IBAQA9
/0fCrER0il0JSqjeOVUppILAmApkWbUaEegdR2s8wzCJDNrV8P6ZPpu98xv3LblY
9tiI8ShZPGHPU0ypnLnvGvzhMUmOaL5VRQeXSwvRSVaxN2fBaFKHXclTZbCIF/p8
fPasc7n84/uOsQU/+PaIFwFDUv4GKMiPNLT5HKpHIQM1j4PwYcNgKL+gU6lfe1y2
Wi80ZrwqYRZ5jxVZSTc6qnEA6i1DvxgdDirF5o5Hgt8pHB5JWcBBNrT+/jiBiiyT
rjN2VSOzx5WiIDvdfZcfO8ajXItvhcuuNxBTQEHTfd7p8G1fDGKdtrKybvxKxv/u
fVZLIZN2tDkqsdbZMT9+
-----END CERTIFICATE REQUEST-----
```

Related Topics

file list, on page 637

help

Display help information about a CLI command.

help

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# help ping
Help for command: ping
    Verify IP (ICMP) connectivity to a host
```

Related Topics

show parser dump, on page 955

history

Set the number of history items that the CLI tracks in operational mode.

show history *number*

Syntax Description

show history *number*	Number of History Items: Set the number of commands tracked by the CLI history. *number* can be a value from 0 through 1000. The default is 100 commands. To disable the history feature, set the number to 0.
no history	Return to Default Number of History Items: Restore the default history queue length of 100 commands.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# history 100
vEdge#
```

Related Topics

clear history, on page 591
show history, on page 821

idle-timeout

Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires.

idle-timeout *seconds*

Syntax Description

idle-timeout *seconds*	Timeout Value: Number of seconds that the CLI is idle before the user is logged out of the CLI. A value of 0 (zero) sets the time to infinity, so the user is never logged out. Range: 0 through 8192 seconds. Default: 1800 seconds (30 minutes).

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# idle-timeout 3600
```

Related Topics

exit, on page 636
idle-timeout, on page 234
show cli, on page 778

job stop

Stop a job that is monitoring a file on the local device. This command is the same as the UNIX kill command.

job stop *job-number*

Syntax Description

job-number	Job Number: Number of the job to stop. This number is in the JOBS column in the **show jobs** command output.

Command History

Release	Modification
15.4	Command introduced.

Examples

Stop the job that is monitoring a file

```
vEdge# show jobs
JOB COMMAND
1   monitor start /var/log/vsyslog
vEdge# log:local7.notice: Dec 16 14:55:26 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:26 2015
```

```
(timezone 'America/Los_Angeles')
log:local7.notice: Dec 16 14:55:27 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:27 2015  (timezone
 'America/Los_Angeles')

vEdge# job stop 1
vEdge# show jobs
JOB COMMAND
vEdge#
```

Related Topics

monitor start, on page 643
monitor stop, on page 643
show jobs, on page 887

logout

Terminate the current CLI session, a specific CLI session, or the session of a specific user.

logout [**session** *session-number*] [**user** *username*]

Syntax Description

(none)	Terminate the current CLI session.
session *session-number*	Specific Session: Terminate a specific CLI session.
user *username*	Specific User: Terminate the CLI session of a specific user.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# logout session 16
vEdge#
Message from admin@vEdge at 2013-11-27 15:00:10...
Your session has been terminated by admin
EOF
```

Related Topics

exit, on page 636

monitor event-trace sdwan

To monitor and control the event trace function for a Cisco SD-WAN subsystem, use the **monitor event-trace** command in the privileged EXEC mode. Event trace provides the functionality to capture the SD-WAN traces between the viptela daemons and SD-WAN subsystems.

monitor event-trace *sdwan* { **clear** | **continuous** | **disable** | **dump** | **enable** | **one-shot** }

Syntax Description

sdwan	Name of the Cisco SD-WAN subsystem that is the subject of the event trace. To get a list of components that support event tracing, use the **monitor event-trace ?** command.
clear	Clears existing trace messages for the specified component from memory on the networking device.
continuous	Displays the latest event trace entries.
disable	Turns off event tracing for the specified component.
dump	The trace messages are saved in binary format.
enable	Enables event tracing for the specified component.
one-shot	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified.

Command Default

The event trace function is disabled by default.

Command Modes

Privileged EXEC

Global Configuration Mode

Command History

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

Usage Guidelines

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command in global configuration mode for each instance of a trace.

Use the **show monitor event-trace** command to display trace messages.

Use the **monitor event-trace** *sdwan* **dump** command to save trace message information for a single event. By default, trace information is saved in binary format.

Examples

The following example shows the privileged EXEC commands to stop event tracing, clear the current contents of memory, and reenable the trace function for the component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace sdwan disable
Router# monitor event-trace sdwan clear
Router# monitor event-trace sdwan enable
```

The following example shows how the **monitor event-trace one-shot** command accomplishes the same function as the previous example except in one command. In this example, once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace sdwan one-shot
```

The following example shows the command for writing trace messages for an event in binary format. In this example, the trace messages for the SD-WAN component are written to a file.

```
Router# monitor event-trace sdwan dump
```

monitor start

Begin monitoring a file on the local device. When a file is monitored, any logging information is displayed on the console as it is added to the file.

monitor start *filename*

Syntax Description

filename	Filename To Monitor: Name of the file to monitor.

Command History

Release	Modification
15.4	Command introduced.

Examples

Start and stop monitoring a file, and view the files that are being monitored

```
vEdge# monitor start /var/log/vsyslog
vEdge# show jobs
JOB COMMAND
1   monitor start /var/log/vsyslog
vEdge# log:local7.notice: Dec 16 14:55:26 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:26 2015  (timezone 'America/Los_Angeles')

log:local7.notice: Dec 16 14:55:27 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:27 2015  (timezone 'America/Los_Angeles')

vEdge# monitor stop /var/log/vsyslog
vEdge#
```

Related Topics

job stop, on page 640
monitor stop, on page 643
show jobs, on page 887

monitor stop

Stop monitoring a file on the local device. When a file is monitored, any logging information is displayed on the console as it is added to the file.

monitor stop *filename*

Syntax Description

filename	File to Monitor: Name of the file to monitor.

Command History

Release	Modification
15.4	Command introduced.

Examples

Start and stop monitoring a file, and view the files that are being monitored

```
vEdge# monitor start /var/log/vsyslog
vEdge# show jobs
JOB COMMAND
1   monitor start /var/log/vsyslog
vEdge# log:local7.notice: Dec 16 14:55:26 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:26 2015  (timezone 'America/Los_Angeles')

log:local7.notice: Dec 16 14:55:27 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:27 2015  (timezone 'America/Los_Angeles')

vEdge# monitor stop /var/log/vsyslog
vEdge#
```

Related Topics

job stop, on page 640
monitor start, on page 643
show jobs, on page 887

nslookup

Perform a DNS lookup.

nslookup [**vpn-id** *vpn-id*] *dns-name*

Syntax Description

dns-name	DNS Name: Perform a DNS lookup to map a fully qualified domain name to one or more IP addresses. *dns-name* can be a hostname string, or an IPv4 or IPv6 address.
vpn-id *vpn-id*	VPN: Specify the VPN into which to send the ping packets. If you omit the VPN identifier, the default is VPN 0, which is the transport VPN.

Command History

Release	Modification
14.1	Command introduced.
16.3	In Release 16.3, added support for IPv6 addresses in VPN 0.

Examples

```
vEdge# nslookup vedge.dns.com
nslookup in vpn 0:
```

```
Server: 172.16.255.100
Address 1: 172.16.255.100 vedge.dns.com

Name:      vedge
Address 1: 172.16.255.100 vedge.dns.com

vEdge# nslookup vpn 0 fe80::20c:29ff:fe9b:a9bb
nslookup in VPN 0:
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost.localdomain

Name:      fe80::20c:29ff:fe9b:a9bb
Address1:  fe80::20c:29ff:fe9b:a9bb
```

Related Topics

ping, on page 646
traceroute, on page 1066

paginate

Control the pagination of command output.

paginate (**false** | **true**)

Syntax Description

false	Display Command Output Continuously: Display all command output continuously, regardless of the CLI screen height.
true	Paginate Command Output:Display all command output one screen at a time. To display the next screen of output, press the space bar. Pagination is the default setting.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show running-config system
system
host-name vedge-1
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
--More--
vEdge# paginate false
vEdge# show running-config system
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.
  !
!
logging
  disk
   enable
  !
 !
!
vEdge#
```

Related Topics

more, on page 1111
nomore, on page 1112
tab, on page 1117

ping

Verify that a network device is reachable on the network, by sending ICMP ECHO_REQUEST packets to them. This command is effectively identical to the standard UNIX **ping** command.

ping (*hostname* | *ip-address*)

ping vpn *vpn-id* (*hostname* | *ip-address*)

ping [**count** *number*] [**rapid**] [**size** *bytes*] [**source** (*interface-name* | *ip-address*)] [**wait** *seconds*] **vpn** *vpn-id* (*hostname* | *ip-address*)

Syntax Description

(*hostname* | *ip-address*)	Device to Ping: Name or IPv4 or IPv6 address of the host to ping. For an IPv4 address in a service VPN, you can ping the primary and the secondary addresses.
count *number*	Number of Ping Requests to Send: Number of ping requests to send. If you do not specify a count, the command operates until you interrupt it by typing Control-C.
rapid	Rapid Pinging: Send five ping requests in rapid succession and display abbreviated statistics, only for packets transmitted and received, and percentage of packets lost.
size *bytes*	Size of Ping Request Packets: Size of the packet to send. Default: 64 bytes (56 bytes of data plus 8 bytes of ICMP header).
source (*interface-name* | *ip-address*)	Source of Ping Packets: Interface or IP address from which to send to ping packets. You cannot specify the loopback0 interface in this option.
wait *seconds*	Time to Wait between Each Ping Packet: Time to wait for a response to a ping packet. Default: 1 second.
vpn *vpn-id*	VPN in which to Ping: Specify the VPN into which to send the ping packets.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added support for IPv6 host addresses in VPN 0.
17.2.2	Added support for pinging secondary IPv4 addresses.

Examples

```
vEdge# ping vpn 0 10.0.14.4
PING 10.0.14.4 (10.0.14.4): 56 data bytes
64 bytes from 10.0.14.4: seq=0 ttl=63 time=0.642 ms
64 bytes from 10.0.14.4: seq=1 ttl=63 time=0.788 ms
64 bytes from 10.0.14.4: seq=2 ttl=63 time=0.685 ms
64 bytes from 10.0.14.4: seq=3 ttl=63 time=0.666 ms
64 bytes from 10.0.14.4: seq=4 ttl=63 time=0.713 ms
64 bytes from 10.0.14.4: seq=5 ttl=63 time=0.846 ms
^C
--- 10.0.14.4 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.642/0.723/0.846 ms

vEdge# ping vpn 0 rapid 10.0.12.2
Defaulting count to 5
!!!!!
--- 10.0.12.2 statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

```
vEdge# ping vpn 0 10.0.12.3
PING 10.0.12.3 (10.0.12.3): 56 data bytes
64 bytes from 10.0.12.3: seq=0 ttl=64 time=8.127 ms
64 bytes from 10.0.12.3: seq=1 ttl=64 time=0.475 ms
64 bytes from 10.0.12.3: seq=2 ttl=64 time=0.336 ms
64 bytes from 10.0.12.3: seq=3 ttl=64 time=0.576 ms
64 bytes from 10.0.12.3: seq=4 ttl=64 time=0.578 ms
^C
--- 10.0.12.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.336/2.018/8.127 ms
```

```
vEdge# show interface
                                IF      IF                                                              TCP
                                ADMIN   OPER    ENCAP                                           SPEED           MSS                     RX      TX
VPN  INTERFACE  IP ADDRESS      STATUS  STATUS  TYPE    PORT TYPE  MTU   HWADDR               MBPS    DUPLEX  ADJUST  UPTIME          PACKETS PACKETS
-------------------------------------------------------------------------------------------------------------------------------------------------
0    gre4       172.0.101.15/24 Up      Up      null    service    1500  0a:01:0f:0f:00:00    0       full    1420    0:00:06:09      0       0
0    ge0/0      10.1.15.15/24   Up      Up      null    transport  1500  00:0c:29:9c:a2:be    10      full    1420    0:00:26:44      9986    10696
0    ge0/1      10.1.17.15/24   Up      Up      null    service    1500  00:0c:29:9c:a2:c8    10      full    1420    0:00:17:13      3       8
0    ge0/2      -               Down    Up      null    service    1500  00:0c:29:9c:a2:d2    10      full    1420    0:00:26:47      3       0
0    ge0/3      10.0.20.15/24   Up      Up      null    service    1500  00:0c:29:9c:a2:dc    10      full    1420    0:00:17:13      11      9
0    ge0/6      57.0.1.15/24    Up      Up      null    service    1500  00:0c:29:9c:a2:fa    10      full    1420    0:00:17:13      3       9
0    ge0/7      10.0.100.15/24  Up      Up      null    service    1500  00:0c:29:9c:a2:04    10      full    1420    0:00:26:21      753     641
0    system     172.16.255.15/32 Up     Up      null    loopback   1500  00:00:00:00:00:00    10      full    1420    0:00:15:52      0       0
1    gre1       -               Up      Down    null    service    1500  38:00:01:0f:00:00    -       -       1420    -               0       0
1    ge0/4      10.20.24.15/24  Up      Up      null    service    1500  00:0c:29:9c:a2:e6    10      full    1420    0:00:17:10      714     717
1    ge0/5      56.0.1.15/24    Up      Up      null    service    1500  00:0c:29:9c:a2:f0    10      full    1420    0:00:17:10      1       47
1    loopback0  10.20.30.15/24  Up      Up      null    service    1500  00:00:00:00:00:00    10      full    1420    0:00:00:20      0       0
512  eth0       10.0.1.15/24    Up      Up      null    service    1500  00:50:56:00:01:0f    1000    full    0       0:00:26:39      8156    5313

vEdge# ping vpn 1 10.20.25.16 source 10.20.30.15
Ping in VPN 1
PING 10.20.25.16 (10.20.25.16) from 10.20.30.15 : 56(84) bytes of data.
64 bytes from 10.20.25.16: icmp_seq=1 ttl=64 time=1.45 ms
64 bytes from 10.20.25.16: icmp_seq=2 ttl=64 time=1.61 ms
^C
--- 10.20.25.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.458/1.534/1.611/0.085 ms
vEdge# ping vpn 1 10.20.25.16 source loopback0
Ping in VPN 1
PING 10.20.25.16 (10.20.25.16) from 10.20.30.15 : 56(84) bytes of data.
64 bytes from 10.20.25.16: icmp_seq=1 ttl=64 time=1.05 ms
^C
--- 10.20.25.16 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.054/1.054/1.054/0.000 ms
vm5# ping vpn 1 10.20.25.16 source ge0/4
Ping in VPN 1
PING 10.20.25.16 (10.20.25.16) from 10.20.24.15 : 56(84) bytes of data.
64 bytes from 10.20.25.16: icmp_seq=1 ttl=64 time=1.35 ms
64 bytes from 10.20.25.16: icmp_seq=2 ttl=64 time=1.44 ms
^C
--- 10.20.25.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.350/1.397/1.444/0.047 ms
vEdge#
```

Related Topics

tools nping, on page 1054
traceroute, on page 1066

poweroff

Shut down the Cisco SD-WAN device. Issue this command when you need to power down a router. Do not simply unplug the router.

poweroff

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# poweroff
Are you sure you want to power off the system? [yes NO] yes
Starting cleanup
Stopping vedge daemon: sysmgr.
Shutting down

Broadcast message from root@vm4 (pts/1) (Mon Feb 17 09:52:33 2014):

The system is going down for system halt NOW!
My-MacBook-Pro:~ me$
```

Related Topics

exit, on page 636
vshell, on page 1068

prompt1

Set the operational prompt.

prompt1 *string*

Syntax Description

string	Operational Prompt: Set the operational prompt. The prompt can contain regular ASCII characters and the following special characters. Enclose the entire string in quotation marks: • \d—Current date in the format *yyyy-mm-dd* (for example, 2013-12-02). • \h—Hostname up to the first period (.). You configure the hostname with the **system hostname** command. • \H—Full hostname. You configure the hostname with the **system hostname** command. • \s—Source IP address of the local device. • \t—Current time in 24-hour *hh:mm:ss* format. • \A—Current time in 24-hour format. • \T—Current time in 12-hour *hh:mm:ss* format. • \@—Current time in 12-hour *hh:mm* format. • \u—Login username of the current user. • \m—Mode name. • \m{*n*}—Mode name, but the number of trailing components in the displayed path is limited to be a maximum of *n*, which is an integer. Characters removed are replaced with an ellipsis (...). • \M—Mode name in parentheses. • \M{*n*}—Mode name in parentheses, but the number of trailing components in the displayed path is limited to be a maximum of *n*, which is an integer. Characters removed are replaced with an ellipsis (...).

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# prompt1 "\u-\d # "
admin-2013-12-02 #
```

Related Topics

prompt2, on page 651
show cli, on page 778

prompt2

Set the configuration mode prompt.

prompt2 *string*

Syntax Description

string	Operational Prompt: "*string*" Set the operational prompt. The prompt can contain regular ASCII characters and the following special characters. Enclose the entire string in quotation marks: • \d—Current date in the format *yyyy-mm-dd* (for example, 2013-12-02). • \h—Hostname up to the first period (.). You configure the hostname with the **system hostname** command. • \H—Full hostname. You configure the hostname with the **system hostname** command. • \s—Source IP address of the local device. • \t—Current time in 24-hour *hh:mm:ss* format. • \A—Current time in 24-hou *hh:mm* format. • \T—Current time in 12-hour *hh:mm:ss* format. • \@—Current time in 12-hour *hh:mm* format. • \u—Login username of the current user. • \m—Mode name. • \m{*n*}—Mode name, but the number of trailing components in the displayed path is limited to be a maximum of *n*, which is an integer. Characters removed are replaced with an ellipsis (...). • \M—Mode name in parentheses. • \M{*n*}—Mode name in parentheses, but the number of trailing components in the displayed path is limited to be a maximum of *n*, which is an integer. Characters removed are replaced with an ellipsis (...).

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# prompt2 "\A on \h# "
vEdge# config
Entering configuration mode terminal
15:09 on vEdge#
```

Related Topics

prompt1, on page 649
show cli, on page 778

quit

Exit from the CLI session. The **exit** and **quit** commands do the same thing.

quit

Examples

```
vEdge# quit
My-MacBook-Pro:~ me$
```

Command History

Release	Modification
14.1	Command introduced.

Related Topics

exit, on page 636
vshell, on page 1068

reboot

Reboot the Cisco SD-WAN device.

Any user can issue the **reboot** command, but the underlying logging mechanism does not log the user name. If you subsequently issue a **show reboot** history command, it shows that the reboot request was issued by an unnamed user.

Note You cannot issue the **reboot** command while a software upgrade is in progress.

reboot [**now**] **reboot other-boot-partition** [**no-sync**]

Syntax Description

(none)	Reboot the device. The software prompts you to confirm that you really want to reboot.
now	Reboot Immediately: Reboot the device immediately, with no prompt asking you to confirm that you want to reboot.

other-boot-partition	Reboot and Use the Software Image on the Other Disk Partition: (Available in releases 15.3 and earlier.) When rebooting the device, start the software image that is installed on the other disk partition. The software prompts you to confirm that you really want to reboot. If the other partition cannot be mounted or if the directory on the other partition is unreadable, an error message is displayed and the reboot operation is canceled.
other-boot-partition no-sync	Switch to the Other Software Image without Rebooting: (Available in releases 15.3 and earlier.) Switch to the software image that is installed on the other disk partition without rebooting the device. If the other partition cannot be mounted or if the directory on the other partition is unreadable, an error message is displayed and the switch operation is canceled.

Command History

Release	Modification
14.1	Command introduced.
14.2	Starting with the 14.2 release, you cannot issue the **reboot** command when a software upgrade is in progress.
15.3	Starting with the 15.3 release, the **reboot other-boot-partition** command prompts for confirmation.
15.4	Starting with 15.4 release, the **reboot other-boot-partition** command is replaced with the **request software activate** command.

Examples

Reboot

```
vEdge# reboot
Are you sure you want to reboot? [yes,NO] yes
Starting cleanup
Stopping viptela daemon: sysmgr.
Rebooting now

Broadcast message from root@vm4 (pts/1) (Wed Nov 27 13:36:07 2013):

The system is going down for reboot NOW!
user$ ssh vEdge
vEdge# show system status | display xml | include reboot_type
    <reboot_type>Unknown</reboot_type>
vEdge#
```

show boot-partition

```
vEdge# show boot-partition (available in Releases 15.3 and earlier)

PARTITION  ACTIVE  VERSION
```

```
--------------------------------------
1          X       14.2.4
2          -       -

vEdge# reboot other-boot-partition (available in Releases 15.3 and earlier)
No firmware present.
vEdge#
```

reboot other-boot-partition

```
vEdge# reboot other-boot-partition (available in Releases 15.3 and earlier)
Are you sure you want to boot using image in other boot partition? [yes,NO] <CR>
Aborted: by user

vEdge# reboot other-boot-partition no-sync (available in Releases 15.3 and earlier)
Are you sure you want to boot using image in other boot partition? [yes,NO] <CR>
Aborted: by user

vEdge# reboot other-boot-partition no-sync (available in Releases 15.3 and earlier)
Are you sure you want to boot using image in other boot partition? [yes,NO] yes
Stopping processes and rebooting
```

Related Topics

request software activate, on page 701
request software install, on page 702
show boot-partition, on page 759
show reboot history, on page 983
show software, on page 1006
show system status, on page 1019

request aaa unlock-user

Reset a user account that has been locked, on a Cisco vEdge device, or on SD-WAN Manager, SD-WAN Validator, or SD-WAN Controller.

request aaa unlock-user *username* **reason** *lock-reason*

Syntax Description

request aaa unlock-user *username*	User account to reset. **Note** An account gets locked even if no password is entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

reason *lock-reason*	Mandatory from: • Release 20.9.3 and later maintenance releases of 20.9.x • Release 20.11.1 and later Indicate the reason why the account was locked. Unlocking the account requires entering the correct reason. You can view the reason using **show aaa users**. • **administrative**: Administrative reasons. • **faillock**: Too many entries of invalid credentials. • **inactivity**: Account inactivity.

Command History

Release	Modification
15.4	Command introduced.
20.9.3 and later maintenance releases of 20.9.x 20.11.1	Added the **reason** keyword.

Examples

```
vEdge# request aaa unlock-user jdoe reason administrative
user jdoe has been unlocked
vEdge#
```

Related Topics

aaa, on page 24
show users, on page 1036

request admin-tech

Collect 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 file to Cisco SD-WAN customer support.

If your Cisco 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 single device, you can run only one **request admin-tech** command at a time. If a command is in progress, the device does not let a second one start.

When a process (daemon) on a Cisco SD-WAN device fails and that failure results in the device rebooting, the device automatically runs a **request admin-tech exclude-cores exclude-logs** file before the the device is rebooted.

To retrieve the admin-tech file from the Cisco SD-WAN device, use SCP. To do this, you must have login access to the device. To copy the file from the Cisco SD-WAN device, enter the shell from the Cisco SD-WAN CLI and issue a command in the following format:

```
vEdge# vshell
vEdge:~$ scp filename .tar.gz  username@host-name:path-name
```

request admin-tech [**delete-filename** *filename*] [**exclude-cores**] [**exclude-logs**] [**exclude-tech**]

vManage Equivalent

Tools ► Operational Commands ► Select device ► More Actions icon ► Admin Tech

Syntax Description

(none)	Collect all system status information, including core files, log files, and the process (daemon) and operational-related files that are stored in the /var/tech directory on the local device.
exclude-cores	Do Not Include Core Files: Do not include any core files in the compressed tar file. Core files are stored in the /var/crash directory on the local device.
exclude-logs	Do Not Include Log Files: Do not include any log files in the compressed tar file. Log files are stored in the /var/log directory on the local device.
exclude-logs	Do Not Include Process-Related Files: 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 the local device.

Command History

Release	Modification
14.1	Command introduced.
16.1	Added support for running only one **request admin-tech** command at a time.
16.3	Added **delete-file-name**, **exclude-cores**, **exclude-logs**, and **exclude-tech** options.
17.1	Added automatic collection of admin-tech information after a process fails.

Examples

Create an admin tech file and copy it to a user's home directory on a host in the network. For the SCP command, you must specify the full pathname of where to place the copied file.

```
vEdge# request admin-tech
Requested admin-tech initiated.
Created admin-tech file '/home/admin/20170712-123416-admin-tech.tar.gz'
vEdge# vshell
vEdge:~$ ls
```

```
20170712-123416-admin-tech.tar.gz archive_id_rsa.pub cacert.pem vEdge-signed-cert.pem
vEdge.csr vEdge_blank_config
vEdge:~$ tar -xvf 20170712-123416-admin-tech.tar.gz
var/log/auth.log
var/log/cloud-init.log
var/log/confd/
var/log/confd/devel.log
var/log/confd/error.log.siz
var/log/confd/snmp.log
var/log/confd/error.log.1
var/log/confd/error.log.idx
var/log/kern.log
var/log/lastlog
var/log/messages
var/log/messages.1
var/log/messages.2
var/log/messages.3
var/log/messages.4
var/log/pdb/
var/log/quagga/
var/log/tallylog
var/log/tmplog/
var/log/tmplog/vdebug
var/log/vconfd
var/log/vdebug
var/log/vdebug_2017-07-10_18_16_36.tar.gz
var/log/vdebug_2017-07-10_18_55_14.tar.gz
var/log/vmware-vmsvc.log
var/log/vsyslog
var/log/wtmp
var/tech/
var/tech/uboot_env
var/tech/confd
var/tech/system
var/tech/transport
var/tech/cxp
var/tech/dot1x
var/tech/cflowd
var/tech/dpi
var/tech/app_route
var/tech/config
var/tech/fpmd
var/tech/igmp
var/tech/hardware
var/tech/ompd
var/tech/ftmd
var/tech/dhcpd
var/tech/vdaemon
var/tech/snmp
var/tech/pimd
var/tech/vrrpd
var/tech/sysmgrd
var/tech/ttmd
var/tech/host_details
var/crash/
var/crash/core.cfgmgr.vm5
var/crash/info.core.cfgmgr.vm5.529.1499738114
var/confd/rollback/
var/confd/rollback/rollback22
var/confd/rollback/rollback13
var/confd/rollback/rollback8
var/confd/rollback/rollback9
var/confd/rollback/rollback2
var/confd/rollback/rollback27
```

```
var/confd/rollback/rollback5
var/confd/rollback/rollback20
var/confd/rollback/rollback0
var/confd/rollback/rollback1
var/confd/rollback/rollback3
var/confd/rollback/rollback21
var/confd/rollback/rollback25
var/confd/rollback/rollback19
var/confd/rollback/rollback4
var/confd/rollback/rollback23
var/confd/rollback/rollback28
var/confd/rollback/rollback7
var/confd/rollback/rollback18
var/confd/rollback/rollback10
var/confd/rollback/rollback24
var/confd/rollback/rollback12
var/confd/rollback/rollback15
var/confd/rollback/rollback11
var/confd/rollback/rollback6
var/confd/rollback/rollback16
var/confd/rollback/rollback26
var/confd/rollback/rollback14
var/confd/rollback/rollback17
vEdge~$ scp 20170712-123416-admin-tech.tar.gz eve@eve-host:~/.
vEdge-%

eve@eve-host:~$ ls 20170712-123416-admin-tech-tar.gz
20170712-123416-admin-tech-tar.gz
eve@eve-host:~$
```

Related Topics

admin-tech-on-failure, on page 56
show crash, on page 803

request certificate

Install a certificate on the Cisco SD-WAN device (on vSmart controllers and vBond orchestrators only).

request certificate install *file-path* [**vpn** *vpn-id*]

Syntax Description

file-path	Path to Certificate File: Install the certificate in specified filename. The file can be in a your home directory on the local device, or it can be on a remote device reachable through VPN 0 and using FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided. *file-path* can be one of the following: • *filename*—Path to a file in your home directory on the local Cisco SD-WAN device. • ftp: *file-path*—Path to a file on an FTP server. • http:// *url*/*file-path*—Path to a file on a webserver. • scp: *user@host:file-path* • tftp: *file-path*—Path to a file on a TFTP server.

vpn *vpn-id*	Specific VPN: 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. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrieved from VPN 0.

Command History

Release	Modification
14.1	Command introduced.

Related Topics

request csr upload, on page 664
show certificate validity, on page 777

request container image install

Install a vSmart software image on a vSmart controller container host (on vSmart controller container hosts only).

request container image install *filename* [**vpn** *vpn-id*]

Syntax Description

filename	Name of vSmart Software Image: Install the vSmart controller software image in the specified filename. The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided. *filename* has the format viptela-*release-number*-x86_64.tar.gz.
vpn *vpn-id*	When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrived from VPN 0. When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrived from VPN 0.

Command History

Release	Modification
16.2	Command introduced.

Related Topics

container, on page 145
request container image remove, on page 660

request container image remove

Install a vSmart software image on a vSmart controller container host (on vSmart controller container hosts only).

request container image remove *filename*

Syntax Description

filename	Name of vSmart Software Image: Name of image that is installed on the vSmart controller container.

Command History

Release	Modification
16.2	Command introduced.

Related Topics

container, on page 145
request container image install, on page 659

request control-tunnel add

Create a temporary tunnel to use when debugging a failed control connection (on vEdge routers only). One case when you might want to create a temporary tunnel is when a control connection fails to come up because of firewall rules or NAT issues. The Cisco SD-WAN software's forwarding process drops failed connections, so creating a temporary one allows you to triage the problem.

request control-tunnel add local-private-ip *ip-address* **local-private-port** *port-number* **remote-public-ip** *ip-address* **remote-public-port** *port-number*

Syntax Description

local-private-port *ip-address port-number*	Local Private IP Address and Port Number: Private IP address and port number for the local side of the tunnel connection. *port-number* can be a value from 0 through 65535.
remote-public-ip *ip-address* **remote-public-port** *port-number*	Remote Public IP Address and Port Number: Public IP address and port number for the remote side of the tunnel connection. can be a value from 0 through 65535. *port-number*

Command History

Release	Modification
16.1	Command introduced.

Examples

```
vEdge# request control-tunnel add local-private-ip 10.1.14.14
Value for 'local-private-port' (<0..65535>): 22234

Value for 'remote-public-ip' (<IP address>): 10.0.12.20
Value for 'remote-public-port' (<0..65535>): 23456
vEdge#
```

Related Topics

request control-tunnel delete, on page 661
tools nping, on page 1054

request control-tunnel delete

Delete a temporary tunnel that you created to debug a failed control connection (on vEdge routers only). One case when you might want to create a temporary tunnel is when a control connection fails to come up because of firewall rules or NAT issues. The Cisco SD-WAN software's forwarding process drops failed connections, so creating a temporary one allows you to triage the problem.

request control-tunnel delete local-private-ip *ip-address* **local-private-port** *port-number* **remote-public-ip** *ip-address* **remote-public-port** *port-number*

Syntax Description

local-private-ip *ip-address* **local-private-port** *port-number*	Local Private IP Address and Port Number: Private IP address and port number for the local side of the tunnel connection. *port-number* can be a value from 0 through 65535.
remote-public-ip *ip-address* **remote-public-port** *port-number*	Remote Public IP Address and Port Number: Public IP address and port number for the remote side of the tunnel connection. *port-number* can be a value from 0 through 65535.

Command History

Release	Modification
16.1	Command introduced.

Related Topics

request control-tunnel add, on page 660

request controller add serial-num

Send the certificate serial number of a vManage NMS or a vSmart controller to the vBond orchestrator (on vManage NMSs only).

request controller add serial-num *number*

Syntax Description

number	Serial Number: Certificate serial number to send to the vManage or vSmart controller.

Command History

Release	Modification
15.4	Command introduced to replace the **request vsmart add serial-num** command.

Usage Guidelines

Note The **request controller add serial-num** command to add serial numbers is not supported on Cisco SD-WAN 20.x releases as changes are not persistent across reboots. You can add serial numbers through Cisco vManage. For more details on controller serial numbers, see Controller Serial Numbers to Cisco vBond Orchestrator.

Related Topics

request controller-upload serial-file, on page 663
request controller delete serial-num, on page 662
show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

request controller delete serial-num

request controller delete serial-num—Delete a vSmart serial number from the vSmart controller serial number file on the local device.

request controller delete serial-num *number*

Syntax Description

number	Serial Number: vSmart serial number to delete from the vSmart serial number file on the local device.

Command History

Release	Modification
15.4	Command introduced to replace the **request vsmart delete serial-num** command.

Usage Guidelines

Note The **request controller delete serial-num** command to delete serial numbers is not supported on Cisco SD-WAN 20.x releases as changes are not persistent across reboots. You can delete serial numbers through Cisco vManage.

Related Topics

request controller-upload serial-file, on page 663
request controller add serial-num, on page 661
show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

request controller-upload serial-file

request controller-upload serial-file—Upload the controller certificate serial number file to the local device (on vManage NMSs only). The local device retains these serial numbers even after you reboot it.

request controller-upload serial-file *filename* [**vpn** *vpn-id*]

Syntax Description

filename	Name of Certificate File: Install the specified file containing the list of serial numbers for the vManage NMSs and vSmart controllers in the overlay network. The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided.
vpn *vpn-id*	Specific VPN: 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. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrieved from VPN 0.

Command History

Release	Modification
15.4	Command introduced to replace the **request vsmart-upload serial-file** command.

Related Topics

request controller add serial-num, on page 661
request controller delete serial-num, on page 662

request csr upload

request csr upload—Upload a certificate signing request (CSR) to the Cisco SD-WAN device (on vSmart controllers and vBond orchestrators only).

request csr upload *path* [**regen-rsa**] [**regen-uuid**] [**vpn** *vpn-id*]

Syntax Description

path	Path to Certificate File: Upload the CSR in the file at the specified path. The path can be in a directory on the local device or on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided.
regen-rsa	(Optional) Regenerate RSA Key Pair: Generate a new RSA public-private key pair. The RSA key pair is stored in the server.key file in the /usr/share/viptela directory on the local device.
regen-uuid	(Optional) Regenerate UUID: Generate a new CSR with a unique UUID that is different from the previous UUID. You can specify this option only on a vBond orchestrator virtual machine (VM). The option is not available on vEdge router hardware, because the router's UUID is its chassis number.
vpn *vpn-id*	(Optional) Specific VPN: VPN in which the CSR file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrieved from VPN 0.

Command History

Release	Modification
14.1	Command introduced.
14.2	Added the **org-name** and **regen-rsa** options.
15.3	Removed the **org-name** option. The command now prompts for the organization name.
17.1	Added support for multitenancy.

Examples

```
vSmart# request csr upload home/admin/vm9.csr
Uploading CSR via VPN 0
Enter organization name             : Cisco SD-WAN
Re-enter organization name          : Cisco SD-WAN
Generating CSR for this VSmart device
.........[DONE]
Copying ... /home/admin/vm9.csr via VPN 0
CSR upload successful
```

When the vBond orchestrator or vSmart controller is part of a software multitenant architecture, the command also prompts for the service provider organization name.

```
vSmart# request csr upload home/admin/vm9.csr
Uploading CSR via VPN 0
Enter service provider organization name        : SP Inc
Re-enter service provider organization name     : SP Inc
Enter organization name                         : Cisco SD-WAN
Re-enter organization name                      : Cisco SD-WAN
Generating CSR for this vSmart device
.........[DONE]
Copying ... /home/admin/vm9.csr via VPN 0
CSR upload successful
```

Related Topics

organization-name, on page 364
request certificate, on page 658

request daemon ncs restart

request daemon ncs restart—Restart the NCS network configuration process (on vManage NMSs only). This process tracks the configurations of Cisco vEdge devices that are being managed by the vManage NMS.

request daemon ncs restart

Command History

Release	Modification
16.1.1	Command introduced.

Examples

```
vManage# request daemon ncs restart
vManage#
```

Related Topics

request nms application-server, on page 674

request device

request device—Add or delete a vEdge router chassis number on the vBond orchestrator that is acting as a ZTP server.

request device add chassis-number *number* strong>serial-numbernumber **validity** [**invalid** | **valid**] **vbond** *ip-address* **org-name** *name* [**port** *port-number*] [**enterprise-root-ca** *path*] **request device delete chassis-number** *number*

chassis-number *number*	Chassis Number: vEdge router chassis number.

validity invalid | **valid**	Device Validity: Whether the vEdge router is allowed to join the overlay network (**valid**) or is not allowed (**invalid**).
enterprise-root-ca *path*	Enterprise Root CA: Path to the enterprise root CA. The path can be an HTTP, FTP, or TFTP path.
org-name *name*	Organization Name: Name of your organization as specified in the device certificates.
port *port-number*	Port on the vBond Orchestrator: Port to use on the vBond orchestrator to reach the WAN network.
strong>serial-numbernumber	Serial Number: vEdge router serial number.

Command History

Release	Modification
14.3	Command introduced.

Examples

```
vBond# request device add chassis-number 12345 serial-number 6789 validity valid vbond 10.1.14.1 org-name cisco
Adding Chassis number 12345 to the database
Successfully added the chassis-number

Creating Serial file ..
Uploading serial numbers via VPN 0
Copying ... /home/admin/vedge_serial_entries via VPN 0
Successfully loaded the vEdge serial numbers
vBond# show ztp entries

                                                                    ROOT
       CHASSIS  SERIAL                       VBOND  ORGANIZATION  CERT
INDEX  NUMBER   NUMBER  VALIDITY  VBOND IP   PORT   NAME          PATH
-------------------------------------------------------------------------
1      12345    6789    valid     10.1.14.1  12346  cisco       default
```

Related Topics

request device-upload, on page 666
show ztp entries, on page 1043

request device-upload

request device—Add vEdge router chassis numbers by uploading a file that contains the device information onto the vBond orchestrator that is acting as a ZTP server.

request device-upload chassis-file *file-path* [**vpn** *vpn-id*]

chassis-file *file-path*	Filename: Name of a CSV file containing the chassis information required by the ZTP server. *file-path* can be one of the following: • *filename*—Path to a file in your home directory on the local Cisco vEdge device. • **ftp:** *file-path*—Path to a file on an FTP server. • **http://** *url*/*file-path*—Path to a file on a webserver. • **scp:** *user@host:file-path* • *file-path*—Path to a file on a TFTP server. Each row in the CSV file must contain the following information for each vEdge router: • Chassis number • Serial number • Validity (either valid or invalid) • vBond IP address • vBond port number (entering a value is optional) • Organization name • Path to the root certification (entering a value is optional)
file-path **vpn** *vpn-id*	VPN: **vpn** *vpn-id* VPN in which the remote server is located.

Command History

Release	Modification
14.3	Command introduced.

Examples

The following example uploads the device information from the local router. Here, the root CA path is omitted, but the comma preceding its value is required.

```
vBond# vshell
vm4vBond~$ cat ztp-chassis-file
12345,6789,valid,10.1.14.1,12345,cisco,
vBond:~$ exit
exit
vBond request device-upload chassis-file /home/admin/ztp-chassis-file
Uploading chassis numbers via VPN 0
Copying ... /home/admin/ztp-chassis-file via VPN 0
Successfully loaded the chassis numbers file to the database.

Uploading the serial numbers to the vedge-list ...
Uploading serial numbers via VPN 0
Copying ... /home/admin/vedge_serial_entries via VPN 0
```

```
Successfully loaded the vEdge serial numbers
vBond# show ztp entries
                                                                        ROOT
       CHASSIS  SERIAL                        VBOND  ORGANIZATION     CERT
INDEX  NUMBER   NUMBER  VALIDITY  VBOND IP    PORT   NAME             PATH
-------------------------------------------------------------------------
1      12345    6789    valid     10.1.14.1   12345  cisco
```

Related Topics

request device, on page 665
show ztp entries, on page 1043

request download

request download—Download a software image or other file to the Cisco SD-WAN device (on vEdge routers and vSmart controllers only).

request download [**vpn** *vpn-id*] *filename*

Syntax Description

filename	Name of Software Image or File: Download a software image or other file to the local Cisco SD-WAN device. The file can be on a remote device reachable through FTP, HTTP, HTTPS, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided. The file is placed in your home directory on the local device.
vpn *vpn-id*	Specific VPN: VPN in which the remote device containing the file to be downloaded is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image.

Command History

Release	Modification
15.3.3	Command introduced on vEdge 100 routers.
15.4	Available on all routers and on vSmart controllers.

Related Topics

request software activate, on page 701
request software install, on page 702
request software install-image, on page 704
request software remove, on page 705
request software reset, on page 706
request software verify-image, on page 710
request upload, on page 712

request execute

request execute—Execute a shell command from within the Cisco SD-WAN CLI.

request execute [**vpn** *vpn-id*] *command* (in Releases 15.4 and later)

request execute [**vpn** *vpn-id*] "*command*" (in Releases 15.3 and earlier)

Syntax Description

command	Command: Run the specified command in the UNIX shell while still remaining in the Cisco SD-WAN CLI. In Releases 15.3 and earlier, you must enclose the command within quotation marks.
vpn *vpn-id*	VPN: Specific to the VPN in which to execute the command. The default *vpn-id* is VPN 0.

Command History

Release	Modification
14.1	Command introduced.
15.4	Enclosing the shell command in quotation marks is no longer necessary.

Examples

```
vSmart# request execute ls
Execute command in vpn 0 - ls
cacert.pem  vsmart-signed-cert-vm9.pem    vsmart-vm9.csr

vEdge# request execute vpn 512 ssh admin@10.0.1.1
```

To open an SSH connection from a vManage NMS to an IOS XE router, you must specify the port number, which is 830.

```
vManage# request execute vpn 0 ssh 172.16.255.15
ssh: connect to host 172.16.255.15 port 22: Connection refused
vManage# request execute vpn 0 ssh 172.16.255.15 -p 830
admin@172.16.255.15's password:
```

Related Topics

job stop, on page 640
monitor start, on page 643
monitor stop, on page 643
show jobs, on page 887
vshell, on page 1068

request firmware upgrade

request firmware upgrade—Upgrade the boot loader (on vEdge routers only). After running this command, you must reboot the router.

request firmware upgrade *filename*

Syntax Description

filename	Boot Loader Filename: Name of the boot loader file. This file must be on the local device. To get the boot loader file, contact Cisco SD-WAN Customer Support.

Command History

Release	Modification
15.3.5	Command introduced.

Examples

```
vEdge# request firmware upgrade u-boot-n820c.bin
vEdge# reboot
```

Related Topics

reboot, on page 652

request interface-reset

request interface-reset—Reset an interface. This command shuts down and then restarts an interface. The operation occurs so quickly that no indication of the interface's being down is reported in the IF STATUS fields in the output of the **show interface** command.

request interface-reset interface *interface-name* **vpn** *vpn-id*

Syntax Description

interface *interface-name*	Interface Name: Name of the interface to reset.
vpn *vpn-id*	VPN: VPN in which the interface resides.

Command History

Release	Modification
15.3	Command introduced.

Usage Guidelines

For Cisco Catalyst SD-WAN, you can reset only WAN interfaces.

Examples

```
vEdge# request interface-reset interface ge0/4 vpn 1
vEdge#
```

Related Topics

show interface, on page 827

request ipsec ike-rekey

request ipsec ike-rekey—Force the generation of new keys for an IKE session (on vEdge routers only).

request ipsec ike-rekey vpn *vpn-id* **interface ipsec** *number*

Syntax Description

ipsec *number*	Interface Name: Name of the IPsec interface on which to force the generation of new keys for an IKE session.
vpn *vpn-id*	VPN: VPN in which the IPsec interface is located.

Command History

Release	Modification
17.2	Command introduced.

Examples

Generate a new key for an IKE session. After the new key is generated, the SPI for the session changes and the uptime for the sessions resets to zero. You cannot directly display the old and new keys.

```
vEdge# show ipsec ike sessions

     IF                          SOURCE              DEST
VPN  NAME    VERSION  SOURCE IP   PORT    DEST IP     PORT  INITIATOR SPI     RESPONDER SPI     CIPHER SUITE     DH GROUP        STATE        UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
1    ipsec1  2        10.1.16.16  4500    10.1.15.15  4500  d58a40949a1e6ef8  5906334ba438d48c  aes256-cbc-sha1  16 (MODP-4096)  ESTABLISHED  0:00:02:08

vEdge# request ipsec ipsec-rekey vpn 1 interface ipsec1
vEdge# show ipsec ike sessions

     IF                          SOURCE              DEST
VPN  NAME    VERSION  SOURCE IP   PORT    DEST IP     PORT  INITIATOR SPI     RESPONDER SPI     CIPHER SUITE     DH GROUP        STATE        UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
1    ipsec1  2        10.1.16.16  4500    10.1.15.15  4500  ecdc1457fbd38824  1ee5fd9f7a645c44  aes256-cbc-sha1  16 (MODP-4096)  ESTABLISHED  0:00:00:18
```

Related Topics

rekey, on page 421
request ipsec ipsec-rekey, on page 672
show ipsec ike inbound-connections, on page 868

show ipsec ike outbound-connections, on page 870
show ipsec ike sessions, on page 872

request ipsec ipsec-rekey

request ipsec ipsec-rekey—Force the generation of a new security parameter index (SPI) for an IPsec tunnel that is being used for IKE sessions (on vEdge routers only).

request ipsec ipsec-rekey interface ipsec *number* **vpn** *vpn-id*

Syntax Description

ipsec *number*	Interface Name: Name of the IPsec interface on which to force the generation of new keys for an IKE session.
vpn *vpn-id*	VPN: VPN in which the IPsec interface is located.

Command History

Release	Modification
17.2	Command introduced.

Examples

Generate a new SPI for an IKE-enabled IPsec tunnel.

```
vEdge# show ipsec ike inbound-connections

SOURCE                          SOURCE  DEST                          DEST    NEW     OLD     CIPHER           NEW       OLD
IP                              PORT    IP                            PORT    SPI     SPI     SUITE            KEY HASH  KEY HASH
-------------------------------------------------------------------------------------------------------------------------------
10.1.15.15                      4500    10.1.16.16                    4500    263     262     aes256-cbc-sha1  ****2474  ****ea42

vEdge# request ipsec ipsec-rekey vpn 1 interface ipsec1
vEdge# show ipsec ike inbound-connections

SOURCE                          SOURCE  DEST                          DEST    NEW     OLD     CIPHER           NEW       OLD
IP                              PORT    IP                            PORT    SPI     SPI     SUITE            KEY HASH  KEY HASH
-------------------------------------------------------------------------------------------------------------------------------
10.1.15.15                      4500    10.1.16.16                    4500    265     264     aes256-cbc-sha1  ****6653  ****d581
```

Related Topics

rekey, on page 421
request ipsec ike-rekey, on page 671
show ipsec ike inbound-connections, on page 868
show ipsec ike outbound-connections, on page 870
show ipsec ike sessions, on page 872

request nms all

request nms all—Start, stop, and perform other operations on all vManage cluster components running on the local vManage NMS (on vManage NMSs only). The cluster components are the application server (the

HTTP web server for the vManage NMS), the vManage configuration and statistics databases, the messaging and coordination server, and the load balancer.

request nms all (**diagnostics** | **jcmd** *option* | **restart** | **start** | **status** | **stop**)

Syntax Description

status	Determine the Status of All vManage Cluster Components: Determine the status of all vManage cluster components.
jcmd *option*	Display Java Process Information: Display information from Java processes running on all vManage cluster components. *option* can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **thread-print**—Information about the Java threads. • **vm-cmd**—Java virtual machine commands. • **vm-flags**—Java virtual machine flags. • **vm-sys-props**—Java virtual machine system properties. • **vm-uptime**—Java virtual machine uptime. • **vm-ver**—Java virtual machine version .
restart	Restart All vManage Cluster Components.
diagnostics	Run Diagnostics on All vManage Cluster Components.
start	Start All vManage Cluster Components.
stop	Stop All vManage Cluster Components.

Command History

Release	Modification
16.1	Command introduced.
16.2.3	Added the **diagnostics** option.

Examples

```
vManage# request nms all status
NMS application server
    Enabled: true
    Status:  running PID:5877 for 2232s
NMS configuration database
    Enabled: true
```

```
    Status:  running PID:9132 for 235s
NMS coordination server
    Enabled: true
    Status:  running PID:28143 for 9591s
NMS messaging server
    Enabled: true
    Status:  running PID:22267 for 11508s
NMS statistics database
    Enabled: true
    Status:  running PID:472 for 48357s
NMS load balancer
    Enabled: false
    Status:  not running
```

Related Topics

request nms application-server, on page 674
request nms configuration-db, on page 681
request nms coordination-server, on page 683
request nms messaging-server, on page 684
request nms statistics-db, on page 687

request nms application-server

request nms application-server—Start, stop, and perform other operations on a vManage HTTP web server (on vManage NMSs only).

request nms application-server (**diagnostics** | **jcmd** *option* | **resize-data-partition** | **restart** | **software** *option* | **start** | **status** | **stop** | **update-logo** *filename*)

Syntax Description

status	Determine the status of the local vManage web server.

jcmd *option*	Display Java Process Information: Display information from a Java process running on the vManage web server. *option* can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **gc-heap-dump**—Snapshot of the Java garbage collector. • **thread-print**—Information about the Java threads running on the vManage web server. • **vm-cmd**—Java virtual machine commands on the vManage web server. • **vm-flags**—Java virtual machine flags on the vManage web server. • **vm-sys-props**—Java virtual machine system properties on the vManage web server. • **vm-uptime**—Java virtual machine uptime on the vManage web server. • **vm-ver**—Java virtual machine version on the vManage web server.
update-logo *large-logo-filename small-logo-filename*	Load a Custom Logo onto the vManage Web Server: Load a logo image to use in the upper left corner of all vManage web application server screens. You can load two files, a larger version, which is displayed on wider browser screens, and a smaller version, which is displayed when the screen size narrows. Both files must be PNG files located on the local device, and both must be 1 MB or smaller in size. For best resolution, it is recommended that the image for the large logo be 180 x 33 pixels, and for the small logo 30 x 33 pixels.
resize-data-partition	Resize Third vManage Partition: Automatically resize the third partition on the vManage NMS if the hypervisor has increased the size of this partition. This partition is the vManage database volume and contains all vManage databases and information related to them. vManage NMS calculates the size of the database volume only when it is initially created. If the hypervisor capabilities cause the database volume size to increase, the vManage NMS recognizes this space and can utilize it only if you issue the **request nms application-server resize-data-partition** command.
restart	Restart the vManage Web Server: Restart the local vManage web server.
diagnostics	Run Diagnostics on vManage Web Server: Run diagnostics on the vManage web server.
start	Start the local vManage web server.
stop	Stop the vManage Web Server: Stop the local vManage web server.

software *option*	Web Application Server Software Control: Control the software running on the vManage application server. can be: *option* can be: • **reset**—Undo a software upgrade on the vManage server, and return to the previous software image. • **upgrade** *filename*—Upgrade the software on the vManage server to the image in the specified file. • **version**—Display the version of software running on the vManage server.

Command History

Release	Modification
16.1	Command introduced.
16.2.2	Added **version** option.
16.2.3	Added **software** option and move **version** option under **software**, and added **diagnostics** option.
17.2	Added **resize-data-partition**, **software reset**, and **software upgrade** options.
20.4	**gc-heap-dump** jcmd option is visible for netadmin user without unhide command.
20.13.1	Added **status** to the command output. When using the status option, the command output indicates whether there is a schema violation in the configuration database.

Examples

Perform various operations on the local vManage application server

```
vManage# request nms application-server status
NMS application server
    Enabled: true
    Status:  running PID:28271 for 7313s
vManage# request nms application-server stop
vManage# request nms application-server restart
NMS application server is not running
Successfully started NMS application server
vManage# request nms application-server status
NMS application server
    Enabled: true
    Status:  running PID:5877 for 6s
vManage# request nms application-server jcmd vm-uptime
NMS application server
5877:
21.357 s
vManage#
```

Determine the version of software running on the vManage NMS web server

```
vManage# request nms application-server version

NMS application server is running version bamboo-20160805-0008 on vManage version 16.2.2
```

Check for Database Schema Violation

The following example, which includes the status option, displays the NMS application server status. Starting from Cisco Catalyst SD-WAN Manager Release 20.13.1, the command indicates whether there are any schema violations in the configuration database. In this example, the command output includes a message indicating a schema violation. If you encounter a schema violation, contact Cisco Customer Support to resolve the issue.

```
SDWAN-Manager# request nms application-server status
NMS application server
 Enabled: false
 Message: Schema Violation
 Status: not running
SDWAN-Manager#
```

Related Topics

request nms all, on page 672
request nms configuration-db, on page 681
request nms coordination-server, on page 683
request nms messaging-server, on page 684
request nms statistics-db, on page 687

request nms cluster diagnostics

To analyze the health of a Cisco SD-WAN Manager cluster, use the **request nms cluster diagnostics** command in privileged EXEC mode.

request nms cluster diagnostics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco vManage Release 20.9.1	This command was introduced.

Usage Guidelines

Run the command directly on the Cisco SD-WAN Manager device for which you are running the Cisco SD-WAN Manager cluster.

The **request nms cluster diagnostics** command provides Cisco SD-WAN Manager cluster diagnostics information and status information for the following Cisco SD-WAN Manager services:

- Application server
- Messaging server
- Configuration database
- Statistics database service
- Coordination server

Examples

The following is a sample output from the **request nms cluster diagnostics** command:

```
Device# request nms cluster diagnostics

Note: This output only compares the cluster configuration of each service running on this
specific vManage against its operational state.
For overall cluster health, please check the Cluster Status page on UI.

hosts in cluster:
10.0.105.39 10.0.105.38 10.0.105.32

Checking services running on 10.0.105.32

persona: COMPUTE_AND_DATA

****************************************
Check application-server cluster status
status: OK

****************************************
check configuration-db status
Get cluster overview:
id, addresses, databases, groups
"8b82367b-5e47-496f-b9ef-683c61ada642", ["bolt://10.0.105.32:7687",
"http://10.0.105.32:7474"], {neo4j: "LEADER", system: "FOLLOWER"}, []
"b47faeb4-9089-4a3e-9275-fbed96d086a2", ["bolt://10.0.105.38:7687",
"http://10.0.105.38:7474"], {neo4j: "FOLLOWER", system: "FOLLOWER"}, []
"0e20db23-fca6-4767-9bf1-8262323a37dd", ["bolt://10.0.105.39:7687",
"http://10.0.105.39:7474"], {neo4j: "FOLLOWER", system: "LEADER"}, []
status: configuration-db's config & operational states are Consistent

****************************************
check messaging-server cluster status
messaging-server role on this node: Leader
status: messaging-server's config & operational states are Consistent

****************************************
check Elasticsearch cluster status
status: Elasticsearch's config & operational states are Consistent

****************************************
check coordination-server cluster status
server.0=0.0.0.0:2888:3888:participant
server.1=10.0.105.38:2888:3888:participant
server.2=10.0.105.39:2888:3888:participant
status: coordination server's config & operational states are Consistent
```

Related Commands

Commands	Description
request admin-tech	Collect system status information in a compressed tar file to aid in troubleshooting and diagnostics.
request nms all	Start, stop, and perform other operations on all Cisco SD-WAN Manager cluster services.
request nms application-server	Start, stop, and perform other operations on a Cisco SD-WAN Manager HTTP web server.
request nms configuration-db	Start, stop, and perform other operations on the localCisco SD-WAN Manager configuration database.
request nms coordination-server	Start, stop, and perform other operations on the local Cisco SD-WAN Manager coordination server.
request nms messaging-server	Start, stop, and perform other operations on the local Cisco SD-WAN Manager messaging server.
request nms statistics-db	Start, stop, and perform other operations on the local Cisco SD-WAN Manager statistics database.
request nms-server	Start and stop a Cisco SD-WAN Manager server and display the status of the server.
request nms server-proxy	Display the status of the Cisco SD-WAN Manager server-proxy for the configured management IP address and port.

request nms cluster-orchestrator

Use the **request nms cluster-orchestrator** command in privileged EXEC mode on a Cisco SD-WAN Manager instance to start, stop, or restart the cluster-orchestrator service, or to display the status or diagnostics information for the service.

request nms cluster-orchestrator
start | **stop** | **restart** | **status** | **diagnostics**

Syntax Description

start	Start the cluster-orchestrator service.
stop	Stop the cluster-orchestrator service.
restart	Restart the cluster-orchestrator service.
status	Display status information for the cluster-orchestrator service.
diagnostics	Display diagnostics information for the cluster-orchestrator service.

Command Default

None

Command Modes privileged EXEC (#)

Command History

Release	Modification
Cisco Catalyst SD-WAN Control Components Release 20.18.1	The **cluster-orchestrator** keyword was introduced to the **request nms** command.

Usage Guidelines

Example

The following example command stops the cluster-orchestrator service.

```
sdwan-manager#request nms cluster-orchestrator stop
Successfully stopped NMS cluster orchestrator
```

Example

The following example command displays the status of the cluster-orchestrator service.

```
sdwan-manager#request nms cluster-orchestrator status
NMS cluster orchestrator
 Enabled: true
 Status: running PID:5308 for 75s
```

Example

The following example command displays diagnostics for the cluster-orchestrator service. The output is abbreviated here.

```
sdwan-manager#request nms cluster-orchestrator diagnostics
NMS cluster orchestrator
Checking cluster connectivity for ports 9099 ...
Pinging vManage node 0 on 10.0.1.1:9099...

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2025-03-05 23:02 UTC
SENT (0.0020s) Starting TCP Handshake > 10.0.1.1:9099
RCVD (0.0024s) Handshake with 10.0.1.1:9099 completed
SENT (1.0036s) Starting TCP Handshake > 10.0.1.1:9099
RCVD (1.0041s) Handshake with 10.0.1.1:9099 completed
SENT (2.0051s) Starting TCP Handshake > 10.0.1.1:9099
RCVD (2.0055s) Handshake with 10.0.1.1:9099 completed

Max rtt: 0.479ms | Min rtt: 0.421ms | Avg rtt: 0.442ms
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 10.0.2.1:9099...
...
Server network connections
--------------------------
tcp        0      0 10.0.2.1:9099        10.0.4.1:37470       ESTABLISHED 5416/python3
tcp        0      0 10.0.3.1:38762       10.0.3.1:9099        ESTABLISHED 5409/java
tcp        0      0 10.0.2.1:9099        10.0.5.1:45988       ESTABLISHED 5416/python3
tcp        0      0 10.0.3.1:9099        10.0.3.1:38762       ESTABLISHED 5416/python3
tcp        0      0 10.0.2.1:9099        10.0.5.1:45980       ESTABLISHED 5416/python3

Checking cluster connectivity for ports 9090 ...
Pinging vManage node 0 on 10.0.1.1:9090...
...
```

request nms configuration-db

To start, stop, and perform other operations on the local Cisco SD-WAN Manager configuration database use the **request nms configuration-db** in privileged EXEC mode. The Cisco SD-WAN Manager configuration database stores device and feature templates and configurations created on the local device.

request nms configuration-db { **backup path** *path* | **configure** | **diagnostics** | **disable-daily-backup** | **enable-daily-backup** | **jcmd** | **restart** | **restore path** *path* | **start** | **status** | **stop** | **update-admin-user** | **upgrade** }

Syntax Description

backup path *path*	Performs back up of the configuration database to the specified file location.
configure	Configures the local Cisco SD-WAN Manager configuration database.
diagnostics	Runs diagnostics on local Cisco SD-WAN Manager configuration database.
disable-daily-backup	Disables local Cisco SD-WAN Manager configuration database daily backup cronjob.
enable-daily-backup	Enables local Cisco SD-WAN Manager configuration database daily backup cronjob. Up to three backups files are stored in the location that you specify with the **backup path** *path* keyword. A back up file is named configdb-daily.*x*.tar.gz, where *x* is 1, 2, or 3. After three backup files are stored, the oldest file is overwritten when the next backup is performed.
jcmd *option*	Displays information from the Java processes running on the local Cisco SD-WAN Manager configuration database. *option* can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **thread-print**—Information about the Java threads running on the vManage web server. • **vm-cmd**—Java virtual machine commands on the vManage web server. • **vm-flags**—Java virtual machine flags on the vManage web server. • **vm-sys-props**—Java virtual machine system properties on the vManage web server. • **vm-uptime**—Java virtual machine uptime on the vManage web server. • **vm-ver**—Java virtual machine version on the vManage web server.
restart	Restarts the Cisco SD-WAN Manager configuration database.
restore path *path*	Restores Cisco SD-WAN Manager configuration database from the file located at a specified path.

start	Starts the local Cisco SD-WAN Manager configuration database.
status	Determines the status of the local Cisco SD-WAN Manager configuration database.
stop	Stops the Cisco SD-WAN Manager Configuration Database: Stop the local vManage configuration database.
update-admin-user	Updates configuration database admin user information.
upgrade	Upgrades the configuration database on any one node in the cluster.

Command History

Release	Modification
16.1	Command introduced.
16.2.3	This command was modified. The **diagnostics** keyword is added.
20.3.1	This command was modified. The following keywords were added: **disable-daily-backup**, **enable-daily-backup**, **upgrade**

Examples

Perform various operations on the localCisco SD-WAN Manager configuration database

```
vManage# request nms configuration-db status
NMS configuration database
    Enabled: true
    Status:  running PID:25778 for 10601s


vManage# request nms configuration-db stop
Successfully stopped NMS configuration database


vManage# request nms configuration-db restart
Successfully restarted NMS configuration database
vManage# vManage
NMS configuration database
    Enabled: true
    Status:  running PID:9132 for 5s
```

```
vManage# request nms configuration-db jcmd vm-ver
NMS configuration database
9132:
Java HotSpot(TM) 64-Bit Server VM version 25.72-b15
JDK 8.0_72
```

Verify if the daily backup is enabled:

```
vmanage# request nms configuration-db status

NMS configuration database
       Enabled: true
       Status:  running PID:25778 for 10601s
       Daily Backup: Enabled
```

Related Topics

request nms all, on page 672
request nms application-server, on page 674
request nms coordination-server, on page 683
request nms messaging-server, on page 684
request nms statistics-db, on page 687

request nms coordination-server

request nms coordination-server—Start, stop, and perform other operations on the local vManage coordination server (on vManage NMSs only). The vManage coordination and messaging server work together to distribute messages and share state among all the vManage NMSs in a vMange cluster.

request nms coordination-server (**diagnostics** | **jcmd** *option* | **restart** | **start** | **status** | **stop**)

Syntax Description

status	Determine the Status of the Coordination Server: Determine the status of the local coordination server.
jcmd *option*	Display Java Process Information: Display information from Java processes running on the coordination server. *option* can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **thread-print**—Information about the Java threads running on the vManage web server. • **vm-cmd**—Java virtual machine commands on the vManage web server. • **vm-flags**—Java virtual machine flags on the vManage web server. • **vm-sys-props**—Java virtual machine system properties on the vManage web server. • **vm-uptime**—Java virtual machine uptime on the vManage web server. • **vm-ver**—Java virtual machine version on the vManage web server.
restart	Restart the Coordination Server: Restart the local coordination server.
diagnostics	Run Diagnostics on the Coordination Server: Run diagnostics on the local vManage coordination server.
start	Start the Coordination Server: Start the local coordination server.
stop	Stop the Coordination Server: Stop the local coordination server.

Command History

Release	Modification
16.1	Command introduced.
16.2.3	Added the **diagnostics** option.

Examples

Perform various operations on the local vManage coordination server

```
vManage# request nms coordination-server status
NMS coordination server
    Enabled: true
    Status:  running PID:28143 for 11160s
vManage#
```

Related Topics

request nms all, on page 672
request nms application-server, on page 674
request nms configuration-db, on page 681
request nms messaging-server, on page 684
request nms statistics-db, on page 687

request nms messaging-server

request nms messaging-server—Start, stop, and perform other operations on the local vManage messaging server (on vManage NMSs only). The vManage coordination and messaging server work together to distribute messages and share state among all the vManage NMSs in a vManage cluster.

request nms messaging-server (**diagnostics** | **jcmd** *option* | **restart** | **start** | **status** | **stop**)

Syntax Description

status	Determine the Status of the Messaging Server: Determine the status of the local messaging server.

jcmd *option*	Display Java Process Information: Display information from Java processes running on the messaging server. *option* can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **thread-print**—Information about the Java threads running on the vManage web server. • **vm-cmd**—Java virtual machine commands on the vManage web server. • **vm-flags**—Java virtual machine flags on the vManage web server. • **vm-sys-props**—Java virtual machine system properties on the vManage web server. • **vm-uptime**—Java virtual machine uptime on the vManage web server. • **vm-ver**—Java virtual machine version on the vManage web server.
restart	Restart the Messaging Server: Restart the local messaging server.
diagnostics	Run Diagnostics on the Message Server: Run diagnostics on the local vManage message server.
start	Start the Messaging Server: Start the local messaging server.
stop	Stop the Messaging Server: Stop the local messaging server.

Command History

Release	Modification
16.1	Command introduced.
16.2.3	Added the **diagnostics** option.

Examples

Perform various operations on local vManage messaging server

```
vManage# request nms messaging-server status
NMS messaging server
    Enabled: true
    Status:  running PID:22267 for 13679s
vManage#
```

Related Topics

request nms all, on page 672
request nms application-server, on page 674
request nms coordination-server, on page 683
request nms statistics-db, on page 687

request nms olap-db

To start, stop, or restart the Cisco vManage online analytical processing (OLAP) database, or to view the status of the database, use the **request nms olap-db** command in privileged EXEC mode.

request nms olap-db [**start** | **stop** | **restart** | **status**]

Syntax Description

start	Start the OLAP database.
stop	Stop the OLAP database.
restart	Restart the OLAP database.
status	Display the status of the OLAP database.

Command Default

The OLAP database service is started by default, and you don't have to manually start it.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
Cisco vManage Release 20.11.1	This command was introduced.

Example

The following example shows how to start the OLAP database:

```
vmanage# request nms olap-db start

Successfully started NMS OLAP database
```

The following example shows how to stop the OLAP database:

```
vmanage# request nms olap-db stop

Successfully stopped NMS OLAP database
```

The following example shows how to restart the OLAP database:

```
vmanage# request nms olap-db restart

Successfully restarted NMS OLAP database
```

The following example displays the status of the OLAP database:

```
vmanage# request nms olap-db status

NMS OLAP database

        Enabled: true

        Status: running PID:65218 for 2981335s
```

request nms statistics-db

Start, stop, and perform other operations on the local vManage statistics database (on vManage NMSs only). The vManage statistics database stores all real-time statistics from the local vManage NMS.

request nms statistics-db (**allocate-shards** | **diagnostics** | **jcmd** *option* | **restart** | **start** | **status** | **stop**)

Syntax Description

allocate-shards	Allocate Unassigned Database Shards. Check for unassigned shards in the vManage statistics database, and assign them.
diagnostics	Run diagnostics on the local vManage statistics database.
jcmd *option*	Display information from a Java process running on the vManage web server. Option can be one of the following: • **gc-class-histo**—Histogram of the Java garbage collector. Garbage collection identifies which objects are being used in heap memory. • **gc-class-stats**—Statistics of the Java garbage collector. • **thread-print**—Information about the Java threads running on the vManage web server. • **vm-cmd**—Java virtual machine commands on the vManage web server. • **vm-flags**—Java virtual machine flags on the vManage web server. • **vm-sys-props**—Java virtual machine system properties on the vManage web server. • **vm-uptime**—Java virtual machine uptime on the vManage web server. • **vm-ver**—Java virtual machine version on the vManage web server.
restart	Restart the local vManage statistics database.
start	Start the local vManage statistics database.
status	Determine the status of the local vManage statistics database.
stop	Stop the local vManage statistics database.

Command History

Release	Modification
16.1	Command introduced.
16.2.3	Command modified. Diagnostics option added.
16.3	Command modified. allocate-shards option added

Example

Perform various operations on local vManage statistics database:

```
vManage# request nms statistics-db status
NMS statistics database
 Enabled: true
 Status:  running PID:472 for 48607s
vManage# request nms statistics-db stop
Successfully stopped NMS statistics database
vManage# request nms statistics-db restart
Successfully restarted NMS statistics database
vManage# request nms statistics-db status
NMS statistics database
    Enabled: true
    Status:  running PID:10353 for 4s
vManage# request nms statistics-db jcmd vm-sys-props
NMS statistics database
10353:
#Mon Mar 21 18:45:06 PDT 2016
jna.platform.library.path=/lib64\:/usr/lib\:/lib
java.runtime.name=Java(TM) SE Runtime Environment
sun.boot.library.path=/usr/lib/jvm/jdk1.8.0_72/jre/lib/amd64
java.vm.version=25.72-b15
es.path.home=/var/lib/elasticsearch
java.vm.vendor=Oracle Corporation
java.vendor.url=http\://java.oracle.com/
path.separator=\:
java.vm.name=Java HotSpot(TM) 64-Bit Server VM
file.encoding.pkg=sun.io
user.country=US
sun.java.launcher=SUN_STANDARD
sun.os.patch.level=unknown
jna.nosys=true
java.vm.specification.name=Java Virtual Machine Specification
user.dir=/var/lib/elasticsearch/bin
java.runtime.version=1.8.0_72-b15
java.awt.graphicsenv=sun.awt.X11GraphicsEnvironment
java.endorsed.dirs=/usr/lib/jvm/jdk1.8.0_72/jre/lib/endorsed
os.arch=amd64
java.io.tmpdir=/tmp
line.separator=\n
java.vm.specification.vendor=Oracle Corporation
os.name=Linux
sun.jnu.encoding=ANSI_X3.4-1968
jnidispatch.path=/tmp/jna-564784475/jna988152057480690449.tmp
java.library.path=/usr/java/packages/lib/amd64\:/usr/lib64\:/lib64\:/lib\:/usr/lib
sun.nio.ch.bugLevel=
java.specification.name=Java Platform API Specification
java.class.version=52.0
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
```

```
os.version=3.10.62-ltsi
user.home=/home/vmanage
user.timezone=America/Los_Angeles
java.awt.printerjob=sun.print.PSPrinterJob
file.encoding=UTF-8
java.specification.version=1.8
es.logger.prefix=
user.name=vmanage
java.class.path=/var/lib/elasticsearch/lib/elasticsearch-2.2.0.jar\
:/var/lib/elasticsearch/lib/HdrHistogram-2.1.6.jar\
:/var/lib/elasticsearch/lib/apache-log4j-extras-1.2.17.jar\
:/var/lib/elasticsearch/lib/commons-cli-1.3.1.jar\
:/var/lib/elasticsearch/lib/compiler-0.8.13.jar\
:/var/lib/elasticsearch/lib/compress-lzf-1.0.2.jar\
:/var/lib/elasticsearch/lib/elasticsearch-2.2.0.jar\
:/var/lib/elasticsearch/lib/guava-18.0.jar\
:/var/lib/elasticsearch/lib/hppc-0.7.1.jar\
:/var/lib/elasticsearch/lib/jackson-core-2.6.2.jar\
:/var/lib/elasticsearch/lib/jackson-dataformat-cbor-2.6.2.jar\
:/var/lib/elasticsearch/lib/jackson-dataformat-smile-2.6.2.jar\
:/var/lib/elasticsearch/lib/jackson-dataformat-yaml-2.6.2.jar\
:/var/lib/elasticsearch/lib/jna-4.1.0.jar\
:/var/lib/elasticsearch/lib/joda-convert-1.2.jar\
:/var/lib/elasticsearch/lib/joda-time-2.8.2.jar\
:/var/lib/elasticsearch/lib/jsr166e-1.1.0.jar\
:/var/lib/elasticsearch/lib/jts-1.13.jar\
:/var/lib/elasticsearch/lib/log4j-1.2.17.jar\
:/var/lib/elasticsearch/lib/lucene-analyzers-common-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-backward-codecs-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-core-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-grouping-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-highlighter-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-join-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-memory-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-misc-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-queries-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-queryparser-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-sandbox-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-spatial-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-spatial3d-5.4.1.jar\
:/var/lib/elasticsearch/lib/lucene-suggest-5.4.1.jar\
:/var/lib/elasticsearch/lib/netty-3.10.5.Final.jar\
:/var/lib/elasticsearch/lib/securesm-1.0.jar\
:/var/lib/elasticsearch/lib/snakeyaml-1.15.jar\
:/var/lib/elasticsearch/lib/spatial4j-0.5.jar\
:/var/lib/elasticsearch/lib/t-digest-3.0.jar
java.vm.specification.version=1.8
java.home=/usr/lib/jvm/jdk1.8.0_72/jre
sun.arch.data.model=64
sun.java.command=org.elasticsearch.bootstrap.Elasticsearch start
user.language=en
java.specification.vendor=Oracle Corporation
awt.toolkit=sun.awt.X11.XToolkit
java.vm.info=mixed mode
java.version=1.8.0_72
java.ext.dirs=/usr/lib/jvm/jdk1.8.0_72/jre/lib/ext\
:/usr/java/packages/lib/ext
sun.boot.class.path=/usr/lib/jvm/jdk1.8.0_72/jre/lib/resources.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/rt.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/sunrsasign.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/jsse.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/jce.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/charsets.jar\
:/usr/lib/jvm/jdk1.8.0_72/jre/lib/jfr.jar\
```

```
:/usr/lib/jvm/jdk1.8.0_72/jre/classes
java.vendor=Oracle Corporation
java.awt.headless=true
file.separator=/
java.vendor.url.bug=http\://bugreport.sun.com/bugreport/
sun.io.unicode.encoding=UnicodeLittle
sun.cpu.endian=little
sun.cpu.isalist=
vSmart#
```

Related Topics

request nms all, on page 672
request nms application-server, on page 674
request nms configuration-db, on page 681
request nms coordination-server, on page 683
request nms statistics-db, on page 687

request nms server-proxy

To display the status of the NMS server-proxy for the configured management IP address and port, use the **request nms server-proxy** command.

request nms server-proxy set management-ip *ip-address port*

Syntax Description

set	Set NMS component.
management-ip	Update service proxy management IP configuration.
ip-address	Enter the Cisco SD-WAN Manager management IP address. Default: 127.0.0.1
port	Enter the Cisco SD-WAN Manager management IP port. Default: 8443

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command was introduced.

The following sample output shows the Cisco SD-WAN Manager management IP address and port configurations:

```
Device# request nms server-proxy set management-ip
Enter the vmanage management ip address[127.0.0.1]:127.0.0.1
Enter the vmanage management ip port[8443]:8443
/usr/bin/vconfd_serviceproxy_config.py:177: YAMLLoadWarning: calling yaml.load() without
Loader=... is deprecated, a
s the default Loader is unsafe. Please read https://msg.pyyaml.org/load for full details.
data = yaml.load(fread)
Restarted service proxy for management ip address update
```

request nms server-proxy set ratelimit

To configure rate limits for bulk and non-bulk APIs for a Cisco vManage node or cluster, use the **request nms server-proxy set ratelimit** command in the operational mode.

request nms server-proxy set ratelimit

Syntax Description

This command has no arguments or keywords.

Command Default

The rate limit per node for non-bulk APIs is 100 requests per second.

The rate limit per node for bulk APIs is 48 requests per minute.

For a Cisco vManage cluster, the default rate limit per node is multiplied by the number of nodes. For example, for a three-node cluster, the default rate limit is 144 (48*3) requests per minute across all three nodes.

Command Modes

Operational mode (#)

Command History

Release	Modification
Cisco vManage Release 20.10.1	This command is introduced.

Before you configure the rate limit, consider its effect on Cisco vManage resources.

Examples

The following example shows how you can configure the bulk API rate limit for a node. In this example, the rate limit is changed from 48 requests per minute to 50 requests per minute.

```
vManage# request nms server-proxy set ratelimit

Do you want to reconfigure rate limit for URL non bulk api [y/n] : n
Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics
 [y/n] : y
Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [48 load
 balanced across all nodes at present] : 50

Enter the rate limit unit (second, minute, hour, day) for URL bulk api
/dataservice/data/device/statistics [minute] : minute

Propagating rate limit update across all nodes. Please wait.
vmanage#
```

The following example shows how you can configure the bulk API rate limit for a cluster from one of the nodes in the cluster. This example shows the configuration of the bulk API rate limit on one of the nodes on a three-node cluster. The existing bulk API rate limit per node is 48 requests per minute, and the bulk API rate limit for the cluster is 144 (48*3) requests per minute. The configuration changes the bulk API rate limit per node to 50 requests per minute and the bulk API rate limit for the cluster to 150 requests per minute.

```
vManage# request nms server-proxy set ratelimit
Do you want to reconfigure rate limit for URL non bulk api [y/n] : n
Do you want to reconfigure rate limit for URL bulk api /dataservice/data/device/statistics
 [y/n] : y
Enter the PER NODE rate limit for URL bulk api /dataservice/data/device/statistics [144
load balanced across all nodes at present] : 50
Enter the rate limit unit (second, minute, hour, day) for URL bulk api
/dataservice/data/device/statistics [minute] : minute
```

```
Propagating rate limit update across all nodes. Please wait.
Done. Please restart server-proxy on all nodes using "request nms server-proxy restart"
command.
```

Related Commands

Command	Description
show nms server-proxy ratelimit	Displays rate limits configured on the Cisco vManage server-proxy for bulk and non-bulk APIs.

request on-vbond-controller

Delete the serial number of a vEdge router (on vBond orchestrators only).

request on-vbond-controller delete serial-number *serial-number*

Syntax Description

serial-number	vEdge router serial number to delete.

Command History

Release	Modification
14.1	Command introduced.
16.1	Command modified. on-vbond-vsmart to request on-vbond-controller option added.

request on-vbond-vsmart

Delete the serial number of a vEdge router (on vBond orchestrators only).

Starting with Release 16.1, this command has been renamed to **request on-vbond-controller**.

request on-vbond-vsmart delete serial-number *serial-number*

Syntax Description

serial-number	vEdge router serial number to delete.

Command History

Release	Modification
14.1	Command introduced.

request platform software sdwan bootstrap-config save

To save a bootstrap file to the device bootflash, on Cisco IOS XE Catalyst SD-WAN devices, use **request platform software sdwan bootstrap-config save** in EXEC mode.

request platform software sdwan bootstrap-config save

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	The command was introduced.

Usage Guidelines

To establish connectivity with the Cisco Catalyst SD-WAN controller, a device requires a minimum configuration. In most situations, this minimum bootstrap configuration (MBC) can be provided initially by plug-and-play (PnP). But in some situations, such as in remote sites where it may be preferable not to use PnP, it is helpful to have a saved bootstrap configuration that can connect the device to the controller.

The **request platform software sdwan bootstrap-config save** command saves the device configuration to the bootflash. The command can be used to save the configuration at any time, but it is intended for saving a minimum bootstrap configuration (MBC) file that enables the device to reconnect to the controller in case the full configuration is ever lost or removed.

When setting up a device, add to the configuration the details that are required to connect to the controller, and use this command to save the MBC. The file is saved to this location:

bootflash:/ciscosdwan.cfg

Example

The following example shows the command execution and output.

```
Device#request platform software sdwan bootstrap-config save
Saving bootstrap file 'bootflash:/ciscosdwan.cfg'...
Done
```

request port-hop

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 (on vEdge routers only). Each connection attempt times out in about 60 seconds.

One case to issue this command is when NAT entries become stale.

request 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 History

Release	Modification
15.3.1	Command introduced.

Example

Request port hopping on TLOCs whose color is **lte**:

```
vEdge# request port-hop color lte vEdge#
```

Related Topics

port-hop, on page 391
port-offset, on page 393
show omp tlocs, on page 924

request reset configuration

Reset the device configuration to the factory-default configuration. This command reboots the device.

The configuration reset is reported in the output of the **show reboot history** command.

Command Hierarchy

request reset configuration

Command History

Release	Modification
15.4	Command introduced.

Examples

The following example shows the running configuration on vEdge:

```
vEdge# show running-config
system
 host-name         ve100
 system-ip         172.16.255.30
 site-id           102
 organization-name "Cisco, Inc."
 no track-transport
 clock timezone America/Los_Angeles
 vbond 10.1.14.14
 aaa
  auth-order local radius tacacs
  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 $1$ufgUundA$0D2MxOsGlNqp/hcGPQ.51.
  !
 !
 logging
  disk
   enable
  !
 !
 archive
  path     scp://user@192.168.15.1:~/user/ve100
  interval 1440
  vpn      512
 !
!
bridge 1
 interface ge0/0
  no native-vlan
  no shutdown
 !
 interface ge0/2
  no native-vlan
  no shutdown
 !
 interface ge0/3
  no native-vlan
  no shutdown
 !
!
omp
 no shutdown
 graceful-restart
 advertise connected
!
security
 ipsec
  rekey               172800
  replay-window       4096
  authentication-type none ah-sha1-hmac sha1-hmac
 !
!
vpn 0
 interface ge0/0
  no poe
  autonegotiate
  no shutdown
 !
 interface ge0/1
  ip address 10.1.30.15/24
  tunnel-interface
   encapsulation ipsec
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service ntp
   no allow-service stun
```

```
  !
  mtu           1600
  autonegotiate
  no shutdown
 !
 interface ge0/2
  autonegotiate
  no shutdown
 !
 interface ge0/3
  autonegotiate
  no shutdown
 !
 interface ge0/4
  ip address 1.0.4.1/24
  autonegotiate
  no shutdown
 !
 ip route 0.0.0.0/0 10.1.30.113
!
vpn 1
 interface irb1
  ip address 20.1.1.15/24
  autonegotiate
  no shutdown
 !
!
vpn 512
 interface mgmt0
  ip address 192.168.15.78/24
  autonegotiate
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.15.1
!

vEdge# request reset configuration
Are you sure you want to reset to default configuration? [yes,NO] yes

Broadcast message from root@vEdge (console) (Mon Apr 24 17:52:33 2017):

Mon Apr 24 17:52:33 PDT 2017: The system is going down for reboot NOW!

shell# ssh vEdge
Last login: Tue Apr 25 00:52:16 2017 from 10.0.1.1
Welcome to Cisco SD-WAN CLI
admin connected from 10.0.1.1 using ssh on vEdge
vEdge# show running-config
omp
 no shutdown
!
system
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 $1$OFJrA0HM$IFekE/.08fNJzhJdJHSqt0
  !
!
logging
  disk
   enable
  !
 !
!
vpn 0
 interface ge0/0
  shutdown
 !
 interface ge0/1
  shutdown
 !
 interface ge0/2
  shutdown
 !
 interface ge0/3
  shutdown
 !
 interface ge0/4
  shutdown
 !
 interface ge0/5
  shutdown
 !
 interface ge0/6
  shutdown
 !
 interface ge0/7
  shutdown
 !
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

Related Topics

show reboot history, on page 983

request reset logs

Clear the contents of all syslog logging files on the local device (on vEdge routers and vSmart controllers only). This operation also clears the contents of the WTMP file, which records all login and logout events that have occurred on the device. Resetting the logs does not require the device to be rebooted.

Command Hierarchy

request reset logs

Command History

Release	Modification
15.4	Command introduced.

Examples

The following example clears the syslog logging files on the vEdge device:

```
vEdge# file show /var/log/console-log
No license at startup, please load a valid licence.
licence error, could not read hardware identifier v4
licence error, could not read hardware identifier v5
...
vEdge# request reset logs
vEdge# show /var/log/console-log
vEdge#
```

Related Topics

file list, on page 637
file show, on page 637
job stop, on page 640
logging disk, on page 298
logging server, on page 305
monitor start, on page 643
monitor stop, on page 643
show jobs, on page 887
show logging, on page 891

request sla-dampening-reset color

To reset dampening on a tunnel for a color, use the **request sla-dampening-reset color** command in privileged EXEC mode.

Syntax

request sla-dampening-reset color *color*

Syntax Description

color *color*	Specifies an identifier for the transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider. The following are the color 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 History

Release	Modification
20.5.1	This command is introduced.

Example

The following example resets dampening on a tunnel for the public-internet color:

```
vEdge (config)# bfd app-route
vEdge (config)# bfd app-route poll-interval 60000
vEdge (config-bfd)# bfd app-route multiplier 3
vEdge (config)# bfd app-route color public-internet
vEdge (config-color-public-internet)# sla-damp-multipler 60
vEdge (config-color-public-internet)# exit
vEdge (config-color-public-internet)# exit
vEdge# request sla-dampening-reset color public-internet
```

request root-ca-crl

To install a file that contains the root certificate authority Certificate Revocation List (CRL), use the **request root-ca-crl install** command in privileged EXEC mode.

To uninstall a file that contains the root certificate authority CRL, use the **request root-ca-crl uninstall** command in privileged EXEC mode.

request root-ca-crl install *filename* [**vpn** *vpn-id*]

request root-ca-crl uninstall

Syntax Description

install *filename*	Installs the specified file that contains the root certificate authority CRL.
vpn *vpn-id*	Specifies the VPN in which the CRL file is located.
uninstall	Uinstalls the file that contains the root certificate authority CRL from the device.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command was introduced.

Usage Guidelines

- The file that contains the root certificate authority CRL is installed in the /usr/share/viptela/root-ca.crl directory in the device. The file can be in the home directory in your local device, or in a remote device that can be reached through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided.
- When you include the VPN option, one of the interfaces in the specified VPN is used to retrieve the file that contains the root certificate authority CRL. You can omit this option for a Cisco Catalyst SD-WAN

Controller because its interfaces are only in VPN 0, which is the VPN that is reserved for the control plane, and Cisco Catalyst SD-WAN Controller images are always retrieved from VPN 0.

Examples

The following example shows how to install the master_root.crl file:

```
vEdge # request root-ca-crl install /home/admin/master_root.crl
Uploading root-ca-crl via VPN 0
Copying /home/admin/master_root.crl to /tmp/vconfd/root-ca.crl.tmp via VPN 0
install_crl new_crl /tmp/vconfd/root-ca.crl.tmp destination_crl /usr/share/viptela/root-ca.crl
send_install_crl_notification
```

The following example shows how to uninstall installs the master_root.crl file:

```
vEdge # request root-ca-crl uninstall
Setting root-ca-crl-installed to false
send_uninstall_crl_notification
Successfully uninstalled the root CA CRL
```

request root-cert-chain

Install or uninstall a file containing the root certificate key chain.

Command Hierarchy

request root-cert-chain install *filename* [**vpn** *vpn-id*]

request root-cert-chain uninstall

Syntax Description

install *filename*	Install the specified file containing the root certificate chain The file can be in a your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided.
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. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrieved from VPN 0.
uninstall	Uninstall the file containing the root certificate key chain from the Cisco vEdge device.

Command History

Release	Modification
14.1	Command introduced.

request security ipsec-rekey

Force IPsec to generate new keys (on vEdge routers only). Use this command when the IPsec keys have been compromised. After you issue this command, the old key continues to be used until it times out.

Command Hierarchy

request security ipsec-rekey

Command History

Release	Modification
14.2	Command introduced.

Examples

In this example, the SPIs (keys) for TLOC 172.16.255.15 change from 256 and 257 to 257 and 258:

```
vEdge# show tunnel local-sa
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              256     10.1.15.15       12346   *****b93a
172.16.255.15    lte              257     10.1.15.15       12346   *****b93a

vEdge# request security ipsec-rekey

vEdge# show tunnel local-sa
TLOC ADDRESS     TLOC COLOR       SPI     IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              257     10.1.15.15       12346   *****b93a
172.16.255.15    lte              258     10.1.15.15       12346   *****a19d
```

Related Topics

rekey, on page 419
show bfd sessions, on page 748
show ipsec inbound-connections, on page 873
show ipsec local-sa, on page 874
show ipsec outbound-connections, on page 875

request software activate

Activate a software image on the local Cisco SD-WAN device (on vEdge routers and vSmart controllers only). Starting from Release 15.4, this command replaces the **reboot other-boot-partition** command.

Command Hierarchy

request software activate *software-image* [**clean**] [**now**]

Syntax Description

now	Activate 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.

clean	Activate 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.
software-image	Name of the software image to activate on the device.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers.
15.4	Command supported on all vEdge routers and vSmart controllers.
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.

Examples

The following example activates a software image:

```
vEdge# request software activate 15.3.3
This will reboot the node with the activated version.
Are you sure you want to proceed? [yes,NO]
```

Related Topics

request download, on page 668
request software install-image, on page 704
request software remove, on page 705
request software reset, on page 706
request software secure-boot, on page 707
request software set-default, on page 708
request software verify-image, on page 710
show software, on page 1006
show version, on page 1036

request software install

Download, install, and activate a software image on the Cisco SD-WAN device (on all devices except vEdge 100 routers). 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.

Command Hierarchy

request software install *filename* [**download-timeout** *minutes*] [**reboot** [**no-sync**]] [**vpn** *vpn-id*]

Syntax Description

download-timeout*minutes*	Specifies the installation timeout value. How long to wait before canceling requests to install software. The duration ranges from 1 through 1440 minutes (24 hours). The default time is 60 minutes.
filename	Install the software image in specified filename. The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided. For a vEdge router, filename has the format `SD-WAN-release-number-mips64.tar.bz2` (this image includes both the vEdge and the software for a hardware-based vBond orchestrator). For a vSmart controller and software-based vBond orchestrator, filename has the format `SD-WAN-release-number-x86_64.tar.bz2`. For a vManage NMS, filename has the format `vmanage-release-number-x86_64.tar.bz2`. In all the image names, the release number consists of the last two digits of the release year and a number that indicates which release it is in that year. An example of a vEdge image name is `SD-WAN-16.1-mips64.tar.bz2`, for the first image released in 2016. When you upgrade the software on a vManage NMS, you should back up the vManage storage partition before performing the upgrade. See Restore the vManage NMS .
rebootno-sync	Reboot 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.
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. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrived from VPN 0.

Command History

Release	Modification
14.1	Command introduced.
14.2	**no-sync** option added.

Release	Modification
15.3.5	**download-timeout** option and prompt for backing up vManage database are added.
16.1	Support for signed images and image verification added.

Examples

To upgrade the software on a vManage NMS:

```
vEdge# request software install /home/admin/vmanage-15.2.0-x86_64.tar.bz2 reboot
It is recommended that you back up the vManage storage partition before upgrade. Proceed
with upgrade? [y/n]: n
vManage storage partition not backed up. Stopping upgrade.
vManage# request software install /home/admin/vmanage-15.2.0-x86_64.tar.bz2 reboot
It is recommended that you back up the vManage storage partition before upgrade. Proceed
with upgrade? [y/n]: Y
Prompted for vManage storage backup. Proceeding with upgrade
Starting download of image..
Copying file:///home/admin/vmanage-15.2.0-x86_64.tar.bz2via VPN 0
Successfully downloaded /home/admin/vmanage-15.2.0-x86_64.tar.bz2
Validating image /home/admin/vmanage-15.2.0-x86_64.tar.bz2..
Preparing filesystem
Extracting firmware
Creating recovery backup for factory reset
configuring boot-loader
Installation complete
preparing for reboot
```

Related Topics

reboot, on page 652
request software install-image, on page 704
request software secure-boot, on page 707
request software verify-image, on page 710
show boot-partition, on page 759
show software, on page 1006

request software install-image

Install a software image on the SD-WAN device (on vEdge routers and vSmart controllers only). 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.

Command Hierarchy

request software install-image *file-system-name*

Syntax Description

Table 14: Syntax Description

file-system-name	Install the software image in the specified file system. The file system must be located on the local device. Use the **request download** command to transfer the image file to the local device.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers.
15.4	Support extended on all routers and on vSmart controllers.
16.1	Support for signed images and image verification added.

Related Topics

request download, on page 668
request software activate, on page 701
request software install, on page 702
request software remove, on page 705
request software reset, on page 706
request software secure-boot, on page 707
request software set-default, on page 708
request software verify-image, on page 710
show software, on page 1006
show version, on page 1036

request software remove

Remove a software image from the local Cisco SD-WAN device (on vEdge routers and vSmart controllers only).

Command Hierarchy

request software remove *file-system-name*

Syntax Description

file-system-name	Name of the software image to delete from the device. You cannot delete the active image.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers.
15.4	Support extended on all routers and on vSmart controllers.

Examples

Attempt to remove a software image:

```
vEdge# request software remove ?
Description: Display software versions
Possible completions:
  15.3.3
```

```
vEdge# request software remove 15.3.3
cannot remove active image
vEdge#
```

Related Topics

request download, on page 668
request software activate, on page 701
request software install-image, on page 704
request software reset, on page 706
request software secure-boot, on page 707
request software set-default, on page 708
show software, on page 1006
show version, on page 1036

request software reset

Return the Cisco SD-WAN device to the default software image and default configuration. The default is either the factory-default image and configuration or the default image set with the **request software set-default** command.

When you issue this command, all non-default software images are removed from the device. Then, the device reboots with the default image and configuration.

In Releases 15.3 and earlier, this command reformats the boot partition and installs the software image again. During this process, which is very time-consuming, all logs and the configuration are lost. It is recommended that you issue a **request admin-tech** command to collect system-wide information before issuing this command and that you use this command only when you suspect that the filesystem is corrupt.

Command Hierarchy

request software reset

Command History

Release	Modification
14.1	Command introduced.

Examples

After the command completes, you are logged out of the device. You may need to press the Return key to complete the logout process.

```
vEdge# request software reset
Are you sure you want to reset to factory defaults? [yes,NO] yes
Broadcast message from root@vEdge (console) (Mon Apr 24 17:58:08 2017):
Mon Apr 24 17:58:08 PDT 2017: The system is going down for reboot NOW!
my-computer $
```

Related Topics

reboot, on page 652

request admin-tech, on page 655
request download, on page 668
request software activate, on page 701
request software install, on page 702
request software install-image, on page 704
request software remove, on page 705
request software secure-boot, on page 707
request software set-default, on page 708
show software, on page 1006
show version, on page 1036

request software secure-boot

Check and enforce the secure boot state of the system software images and, for vEdge hardware routers, of the boot loader.

Command Hierarchy

request software secure-boot list request software secure-boot set request software secure-boot status

Syntax Description

request software secure-boot list	Check secure boot state and check whether software images on the device are secure or not secure.
request software secure-boot set	Remove insecure software images from the device and, for vEdge hardware routers, remove an insecure boot loader.
request software secure-boot status	Display the security status of the software images installed on the device.

Command History

Release	Modification
18.3.1	Command introduced.

Examples

```
vEdge# request software secure-boot list
Secure-image check found no insecure software versions
vEdge# request software secure-boot status
Secure-image status: HIGH
```

Related Topics

reboot, on page 652
request software install-image, on page 704
request software install, on page 702
request software verify-image, on page 710

show boot-partition, on page 759
show software, on page 1006

request software set-default

Set a software image to be the default image on the device (on vEdge routers and vSmart controllers only). 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 the device and in your network.

Command Hierarchy

request software set-default *image-name*

Syntax Description

image-name	Name of the software image to designate as the default image on the device.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers.
15.4	Supported on all routers and on vSmart controllers.

Examples

```
vEdge# request software set-default 15.3.3
This will change the default software version.
Are you sure you want to proceed? [yes,NO] yes
vEdge#
```

Related Topics

request download, on page 668
request software activate, on page 701
request software install, on page 702
request software remove, on page 705
request software reset, on page 706
request software secure-boot, on page 707
show software, on page 1006
show version, on page 1036

request software upgrade-confirm

Confirm that the upgrade to a new software image is successful. If the device configuration includes the **system upgrade-confirm** command, issuing the **request 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 the vManage NMS, the vManage NMS automatically issues the **request software upgrade-confirm** command when the vEdge router finishes rebooting. If you have initiated the software upgrade manually from the vEdge router, you issue this command from the CLI.

Command Hierarchy

request software upgrade-confirm

Command History

Release	Modification
15.1	Command introduced.
15.2	Command support added for vBond orchestrator, vManage NMS, and vSmart controller.
15.4	Command renamed from **request upgrade-confirm**.

Examples

Configure an upgrade confirm time limit of 5 minutes, upgrade the software manually from the vEdge router CLI, and confirm that the upgrade has been successful:

```
vEdge# config
vEdge(config)# system upgrade-confirm 5
vEdge(system)# u
vEdge# request software install viptela-15.1.mips64.tar.bz2 reboot
[Software is installed, and router reboots and restarts.]
user$ ssh -l admin vEdge
Software upgrade completed. Device will revert to previous software version in '300' seconds
 unless confirmed.
Execute "request software upgrade-confirm" to confirm the upgrade.
vEdge#
[Less than 5 minutes elapse.]
vEdge# request software upgrade-confirm
Software upgrade confirmed.
vEdge#
```

Configure an upgrade confirm time limit of 5 minutes, upgrade the software, and log back in to the router, but do not confirm that the upgrade has been successful:

```
vEdge# config
vEdge(config)# system upgrade-confirm 5
vEdge(system)# commit and-quit
vEdge# request software install viptela-15.1.mips64.tar.bz2 reboot
[Software is installed, and router reboots and restarts.]
user$ ssh -l admin vEdge
Software upgrade completed. Device will revert to previous software version in '300' seconds
 unless confirmed.
Execute "request software upgrade-confirm" to confirm the upgrade.
vEdge#
[More than 5 minutes elapse.]
Software upgrade not confirmed. Device will revert to previous software version.
vEdge#
```

Related Topics

request software install, on page 702
upgrade-confirm, on page 521

request software verify-image

Verify that a Cisco SD-WAN software image is valid and has been signed.

It is recommended that you issue a **request software install** or **request software install-image** command, or that you install device software from the vManage NMS, rather than using the request software verify-image command. Both these commands, as well as the vManage NMS image installation and upgrade processes, verify that the image is valid and has been signed before they install the software. If the verification process fails, the software image installation is not performed.

Command Hierarchy

request software verify-image *filename*

Syntax Description

filename	Name of the Cisco SD-WAN software image file. This file is a compressed tar file (`filename extension tar.gz`) on the local device. The tar file names have the following format, where x.x.x represents the release version: • `vEdge router—viptela-x.x.x-mips64.tar.gz` • `vBond and vSmart—viptela-x.x.x86_64.tar.gz` • `vManage—vmanage-x.x.x86_64.tar.gz`

Command History

Release	Modification
16.1	Command introduced.

Example

```
vManage# request software verify-image vmanage-16.1.0-x86_64.tar.gz
verify OK
Signature verified for rootfs.img
Signature verified for vmlinuz
vManage#
```

Related Topics

request download, on page 668
request software activate, on page 701
request software install, on page 702
request software install-image, on page 704
request software remove, on page 705
request software reset, on page 706

request upload, on page 712

request stream capture

To debug issues related to loss of connectivity between Cisco vEdge devices and Cisco vManage, use the **request stream capture** command in privileged EXEC mode.

request stream capture { **enable** | **disable** | **abort** } { **control** | **data** } **vpn** *vpn-id* **interface** *interface-name* **session-id** *session-id* [**dst-ip** *ip-address* | **dst-port** *port* | **src-ip** *ip-address* | **src-port** *port* | **protocol** *number*]

Syntax Description

enable	Enables capturing data stream.
disable	Disables capturing data stream.
abort	Terminates the data stream capturing process.
data	Captures data stream for the data plane.
control	Captures data stream information for the control plane.
vpn-id *vpn-id*	VPN ID to capture the data stream details for.
interface *interface-name*	Interface to capture data stream details for.
session-id*session-id*	Session ID to capture the data stream details for.
dst-ip *ip-address*	(Optional) Destination IP address to capture the data stream details for.
dst-port *port*	(Optional) Destination port to capture the data stream details for.
src-ip *ip-address*	(Optional) Source IP address to capture the data stream details for.
src-port *port*	(Optional) Source port to capture the data stream details for.
protocol *number*	(Optional) Valid protocol number Range: 0 to 255

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.6.1	This command was introduced.

Usage Guidelines

The parameters in this command syntax can be configured in any order.

Example

The following example shows how to enable stream capture for the specified details.

```
Device# request stream capture enable vpn1 interface ipsec1 data session-id s123
```

request upload

Upload a file from the Cisco SD-WAN device to another device in the network (on vEdge routers and vSmart controllers only).

Command Hierarchy

request upload [**vpn** *vpn-id*] *destination filename*

Syntax Description

filename	Name of file on the local SD-WAN device to upload to a remote device. If the file is not in your home directory, specify the full path.
destination	Remote device. It must be reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided.
vpn *vpn-id*	VPN in which the remote device containing the file to be downloaded is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers only.
15.4	Command supported on all vEdge routers and on vSmart controllers.

Related Topics

request download, on page 668
request software activate, on page 701
request software install, on page 702
request software install-image, on page 704
request software remove, on page 705
request software reset, on page 706
show software, on page 1006

request vedge

Add a vEdge serial number–chassis number pair to or delete a vEdge serial number-chassis number pair from the vEdge authorized serial number file on the local device.

Comamnd Hierarchy

request vedge [**add** | **delete**] **serial-num** *number* **chassis-num** *number*

Syntax Description

addserial-num *number* **chassis-num** *number*	Add vEdge Serial and Chassis Numbers. Add the specified vEdge serial and chassis number pair to the vEdge authorized serial number file on the local device.
deleteserial-num *number* **chassis-num** *number*	Delete vEdge Serial and Chassis Number. Remove the specified vEdge serial and chassis number from the vEdge authorized serial number file on the local device.

Command History

Release	Modification
14.1	Command introduced.

Related Topics

request vsmart add serial-num, on page 714
request vsmart-upload serial-file, on page 715
show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

request vedge-cloud activate

Activate a vEdge Cloud router in the overlay network (on vEdge Cloud routers only). Before you can use this command, you must configure the organization name and the vBond orchestrator's IP address or DNS name on the vEdge Cloud router.

Command Hierarchy

request vedge-cloud activate chassis-number *number* **token** *token*

Syntax Description

chassis-number *number*	Chassis number of the vEdge Cloud router. To obtain the chassis number (UUID) in vManage NMS, select the Configuration > Devices screen. In the vEdge List, locate the Chassis Number column. If the router is not listed in the vEdge List, click Upload vEdge List to upload the serial number file that contains the vEdge Cloud router's information.
token *token*	Token identifier of the vEdge Cloud router. To obtain the token in vManage NMS, select the Configuration > Devices screen. In the vEdge List, locate the Serial No./Token column. If the router is not listed in the vEdge List, click Upload vEdge List to upload the serial number file that contains the vEdge Cloud router's information.

Command History

Release	Modification
17.1	Command introduced.

request vsmart add serial-num

Send the certificate serial number of a vManage NMS or a vSmart controller to the vBond orchestrator. If your network does not have a vManage NMS and you reboot the vSmart controller, the serial numbers sent with this command are lost. To have the vSmart controller retain the certificate serial numbers, use the **request vsmart-upload** command instead.

Starting in Release 15.4, this command is replaced by the **request controller add** command.

Command Hierarchy

request vsmart add serial-num *number*

Syntax Description

serial-num *number*	Certificate serial number to send to the vManage or vSmart controller.

Command History

Release	Modification
14.1	Command introduced.
15.4	Command is replaced by the **request controller add**.

Related Topics

request vedge, on page 712
request vsmart delete serial-num, on page 714
request vsmart-upload serial-file, on page 715
show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

request vsmart delete serial-num

Delete a vSmart serial number from the vSmart controller serial number file on the local device. Starting in Release 15.4, this command is replaced by the **request controller delete serial-num** command.

Command Hierarchy

request vsmart delete serial-num *number*

Syntax Description

Table 15: Syntax Description

number	vSmart serial number to delete from the vSmart serial number file on the local device.

Command History

Release	Modification
14.1	Command introduced.
15.4	Command replaced by **request controller delete serial-num** command.

Related Topics

request vedge, on page 712
request vsmart add serial-num, on page 714
request vsmart-upload serial-file, on page 715
show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

request vsmart-upload serial-file

Upload the certificate serial number file to the local device (on vBond orchestrators and vManage NMSs only). The local device retains these serial numbers even after you reboot it. Starting in Release 15.4, this command is replaced by **request controller-upload serial-file** command.

Command Hierarchy

request vsmart-upload serial-file *filename* [**vpn** *vpn-id*]

Syntax Description

request vsmart-upload serial-file *filename*	Name of Certificate File. Install the specified file containing the list of serial numbers for the vSmart controllers and the vManage NMSs in the network. The file can be in a your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename. No file path name is provided.
vpn *vpn-id*	Specific VPN in which the file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file. The interfaces on a vSmart controller are only in VPN 0, the VPN reserved for the control plane, so you can omit this option because vSmart images are always retrieved from VPN 0.

Command History

Release	Modification
14.1	Command introduced.
15.4	Command replaced by **request controller-upload serial-file** command.

Related Topics

request vsmart add serial-num, on page 714
request vsmart delete serial-num, on page 714

screen-length

Set the length of the terminal window. For most Cisco SD-WAN software commands, the output is rendered automatically either by the CLI or by templates that format the output. For these commands, any value that you set for screen-length command has no effect. Use the **more** and **nomore** command filters to control the length of the output.

Command Hierarchy

screen-length *number*

Syntax Description

screen-length *number*	Set the length of the terminal screen. Number can be a value from 0 through 256. When you set the screen length to 0, the CLI does not paginate command output.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# screen-length 24
vEdge#
```

Related Topics

screen-width, on page 716
show cli, on page 778

screen-width

Set the width of the terminal window. For most Cisco SD-WAN software commands, the output is rendered automatically either by the CLI or by templates that format the output. For these commands, any value that you set for **screen-width** command has no effect. Use the **tab** and **notab** command filters to control the width of the output.

Command Hierarchy

screen-width *number*

Syntax Description

screen-width *number*	Set the width of the terminal screen. Number can be a value from 20 through 256.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# screen-width 80
vEdge#
```

Related Topics

screen-length, on page 716
show cli, on page 778

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 16: 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
```

show aaa usergroup

show aaa usergroup—List the groups configured for AAA role-based access to a Cisco vEdge device.

Command Syntax

show aaa usergroup

show aaa usergroup task [**permission** (**read** | **write**)]

show aaa usergroup users *username*

vManage Equivalent

For all Cisco vEdge devices:

Administration ► Manage Users

Syntax Description

show aaa usergroup	All Usergroups, Users, Tasks, and Permissions: List all configured usergroups, the users in those groups, and the task permissions that each group has.
show aaa usergroup task [permission (**read** | **write**)]	All Usergroups, Tasks, and Permissions: List all configured usergroups and the task permissions that each group has.
show aaa usergroup users *username*	Usergroup Information for a User: For the specified user, list the group they are in and that group's task permissions.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show aaa usergroup

```
vEdge# show aaa usergroup
GROUP     USERS  TASK       PERMISSION
----------------------------------------
basic     -      system     read write
                 interface  read write
admin     admin  system     read write
                 interface  read write
                 policy     read write
                 routing    read write
                 security   read write
operator  eve    system     read
                 interface  read
                 policy     read
                 routing    read
                 security   read

vEdge# show aaa usergroup task
GROUP     TASK       PERMISSION
---------------------------------
basic     system     read write
          interface  read write
admin     system     read write
          interface  read write
          policy     read write
          routing    read write
          security   read write
operator  system     read
          interface  read
          policy     read
          routing    read
          security   read
```

```
vEdge# show aaa usergroup users eve
GROUP     USERS  TASK       PERMISSION
-----------------------------------------
operator  eve    system     read
                 interface  read
                 policy     read
                 routing    read
                 security   read
```

Related Topics

aaa, on page 24

show alarms

To view alarms history and view the watermarks configured for CPU, memory, and disk usage, and the disk read and write speeds, use the **show alarms** command in the operational mode.

show alarms { **cpu-usage** | **history** | **memory-usage** | **disk-usage** | **disk-speed** }

Syntax Description

cpu-usage	Shows configured CPU-usage watermarks.
history	Shows the history of alarms. The following options are available: • **from**: Displays alarms from timestamp (YYYY-MM-DDTHH:MM:SS) • **last-n**: Displays last-n alarms (default: 25) • **severity**: Shows alarms matching severity • **skip-type**: Skips displaying alarms matching type • **to**: Displays alarms till timestamp (YYYY-MM-DDTHH:MM:SS) • **type**: Shows alarms matching type
memory-usage	Shows configured memory-usage watermarks.
disk-usage	Shows configured disk-usage watermarks.
disk-speed	Shows configured watermarks for disk read and write speeds. **Note** Watermarks for disk read and write speeds can only be configured in a Cisco vManage server.

Command Modes

Operational mode (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command is introduced.

Examples

The following is a sample output of the **show alarms cpu-usage** command:

```
Device# show alarms cpu-usage

            HIGH        MEDIUM      LOW
            WATERMARK   WATERMARK   WATERMARK
CPU USAGE   PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-----------------------------------------------------------------
cpu-usage   80          70          50          10
```

The following is a sample output of the **show alarms history** command:

```
Device# show alarms history
DATE  TIME       TYPE                                SEVERITY   DETAILS

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

03/10 11:01:35   cpu-usage                           minor      warning:System cpu usage
back to normal level cpu-user-percentage:6.50 cpu-system-pe
rcentage:47.50 cpu-idle-percentage:46.00

03/10 11:01:33   system-reboot-issued                major      reboot-reason:Initiated by
 user - activate 10.8.0-71
03/10 11:01:27   control-connection-state-change     major      personality:vedge
peer-type:vmanage peer-system-ip:10.168.1.197 peer-vmanage-system
-ip:0.0.0.0 public-ip:10.130.130.4 public-port:23756 src-color:biz-internet
remote-color:default uptime:0:00:00:35 new-state:down
03/10 11:01:27   control-connection-state-change     major      personality:vedge
peer-type:vsmart peer-system-ip:10.168.1.195 peer-vmanage-system-
ip:0.0.0.0 public-ip:10.130.130.3 public-port:12446 src-color:biz-internet
remote-color:biz-internet uptime:0:00:00:34 new-state:down
03/10 11:01:27   control-no-active-vsmart            critical   personality:vedge
```

The following is a sample output of the **show alarms memory-usage** command:

```
Device# show alarms memory-usage

              HIGH        MEDIUM      LOW
              WATERMARK   WATERMARK   WATERMARK
MEMORY USAGE  PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-----------------------------------------------------------------
memory-usage  80          70          50          10
```

The following is a sample output of the **show alarms disk-usage** command:

```
Device# show alarms disk-usage

             HIGH         MEDIUM       LOW
FILESYSTEM   WATERMARK    WATERMARK    WATERMARK
PATH         PERCENTAGE   PERCENTAGE   PERCENTAGE  INTERVAL
-------------------------------------------------------------------
/rootfs.rw    90           75           60          5
/tmp          90           75           60          5
/opt/data     80           70           50          10
```

The following is a sample output of the **show alarms disk-speed** command:

```
vManage# show alarms disk-speed

                        READ                    WRITE       WRITE
             READ HIGH  MEDIUM      READ LOW    HIGH        MEDIUM      WRITE LOW
             WATERMARK  WATERMARK   WATERMARK   WATERMARK   WATERMARK   WATERMARK
DISK PATH    K BPS      K BPS       K BPS       K BPS       K BPS       K BPS       INTERVAL
```

```
-------------------------------------------------------------------------------------
/dev/sda2   1000       500        100        1000       500        100        100
```

Related Commands

Command	Description
cpu-usage	Configures CPU-usage watermarks and polling interval.
memory-usage	Configures memory-usage watermarks and polling interval.
disk-usage	Configures disk-usage watermarks and polling interval.
disk-speed	Configures watermarks for the disk read and write speeds for disk partitions on a Cisco vManage server.

show app cflowd collector

show app cflowd collector—Display information about the configured cflowd collectors that the vEdge router has learned from a vSmart controller (on vEdge routers only).

Command Syntax

show app cflowd collector

vManage Equivalent

For vEdge routers only:

Monitor ► Network ► Application ► Flows

Syntax Description

None

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show app cflowd collector

```
vEdge# show app cflowd collector

      COLLECTOR
VPN   IP          COLLECTOR  CONNECTION            IPFIX    CONNECTION  TEMPLATE  DATA
ID    ADDRESS     PORT       STATE       PROTOCOL  VERSION  RETRY       PACKETS   PACKETS
-------------------------------------------------------------------------------------
1024  10.20.7.1   18004      true        TCP       10       1           2         0
1024  10.20.7.1   18003      true        TCP       10       1           2         0
```

```
1024  10.20.7.1  18002      true        TCP       10       1           2          0
1024  10.20.7.1  18001      true        TCP       10       1           2          0
```

Related Topics

cflowd-template, on page 121
clear app cflowd flows, on page 568
clear app cflowd statistics, on page 570
show app cflowd flow-count, on page 723
show app cflowd flows, on page 724
show app cflowd statistics, on page 726
show app cflowd template, on page 727
show policy from-vsmart, on page 971

show app cflowd flow-count

show app cflowd flow-count—Display the number of current cflowd traffic flows (on vEdge routers only).

Command Syntax

show app cflowd flow-count

vManage Equivalent

For vEdge routers only:

Monitor ► Network ► Real Time ► App Log Flow Count

Syntax Description

Syntax Description

None

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show app cflowd flow-count

```
vEdge# show app cflowd flow-count

VPN  count
------------
1    502
2    452
3    502
4    502
5    502
6    502
```

```
7     502
8     502
9     502
10    502
```

Related Topics

cflowd-template, on page 121
clear app cflowd flows, on page 568
clear app cflowd statistics, on page 570
show app cflowd collector, on page 722
show app cflowd flows, on page 724
show app cflowd statistics, on page 726
show app cflowd template, on page 727
show policy from-vsmart, on page 971

show app cflowd flows

show app cflowd flows—Display cflowd flow information (on vEdge routers only).

Command Syntax

show app cflowd flows [**vpn** *vpn-id*]

show app cflowd flows [**vpn** *vpn-id*] [*flow-parameter*]

show app cflowd flows vpn *vpn-id* **src-ip** *ip-address* **dest-ip** *ip-address* **src-port** *port-number* **dest-port** *port-number* **dscp** *value*

ip-proto *protocol-number*

vManage Equivalent

For vEdge routers only:

Monitor ► Network ► Real Time ► App Log Flows

Syntax Description

None	None Display cflowd flow information for all flows.
vpn *vpn-id* **src-ip** *ip-address* **dest-ip** *ip-address* **src-port** *port-number* **dest-port** *port-number* **dscp** *value* **ip-proto** *protocol-number*	Flow Key Elements Display cflowd flow information for a specific flow key element. You must specify all the key elements as shown in the syntax and in the order shown in the syntax. You can also just specify all the key elements until the last one that you are interested in, and again you must specify them in the order shown. For example, if you are interested only in filtering on the source and destination ports, you include only the VPN, source and destination addresses, and source and destination ports in the command; you can omit the last two key elements (DSCP and IP protocol). To select all values for a key elements, specify an asterisk (*) as a wildcard in place of the variable; for example, **src-ip ***.

flow-parameter	Flow Parameter: Display the flow that matches the specified flow parameter. These parameters correspond to a number of the column headers in the output of the plain **show app cflowd flows** command. *flow-parameter* can be one of the following: • **egress-intf-name** *interface-name*—Flow's outgoing interface. • **icmp-opcode** *value*—Flow's ICMP operational code. • **ingress-intf-name** *interface-name*—Flow's incoming interface. • **max-length** *bytes*—Maximum IP packet length in the flow. • **min-length** *bytes*—Minimum IP packet length in the flow. • **nhop-ip** *ip-address*—IP address of the flow's next hop. • **start-time** *time*—Flow's start time. • **tcp-cntrl-bits** *bit*—Flow's TCP control bit value. • **time-to-expire** *seconds*—Time until the flow expires. • **total-bytes** *number*—Total number of bytes in the flow. • **total-packets** *number*—Total number of packets in the flow.
vpn *vpn-id*	VPN Display cflowd information for flows in a specific VPN.

Command History

Release	Modification
14.3.	Command introduced.
15.4.	Options for flow parameters and IP address, ports, DSCP, and protocol added.

Examples

Show app cflowd flows

```
vEdge# show app cflowd flows
                                                                    TCP                                                                                     TIME
                                    SRC     DEST           IP       CNTRL  ICMP                          TOTAL   TOTAL     MIN  MAX                              TO       EGRESS     INGRESS
    APP
VPN  SRC IP           DEST IP           PORT    PORT   DSCP  PROTO  BITS   OPCODE  NHOP IP          PKTS    BYTES     LEN  LEN   START TIME                  EXPIRE  INTF NAME  INTF
NAME  ID
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
100  10.1.111.2      18.100.44.4       12345  6789  0      6       24      0       192.168.10.9    23      1902      70   155   Fri Sep 28 17:44:36 2018   45       ipsec1     ge0/3
     1118
100  18.100.44.4     10.1.111.2        6789   12345 0      6       16      0       10.1.111.2      41      5914      40   1340  Fri Sep 28 17:39:56 2018   43       ge0/3      ipsec1
     1118

vEdge# show app dpi supported-applications | tab | include 1118
apns           application_service  Apple Push Notification Service            Application Service 1118
```

Related Topics

cflowd-template, on page 121

clear app cflowd flows, on page 568
clear app cflowd statistics, on page 570
show app cflowd collector, on page 722
show app cflowd flow-count, on page 723
show app cflowd statistics, on page 726
show app cflowd template, on page 727
show policy from-vsmart, on page 971

show app cflowd statistics

show app cflowd statistics—Display cflowd packet statistics (on vEdge routers only).

Command Syntax

show app cflowd statistics

Syntax Description

Syntax Description None

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show app cflowd statistics

```
vEdge# show app cflowd statistics

      data_packets             :      47243
      template_packets         :      77
      total-packets            :      47320
      flow-refresh             :      271395
      flow-ageout              :      24203
      flow-end-detected        :      58
      flow-end-forced          :      0
Release Information
```

Related Topics

cflowd-template, on page 121
clear app cflowd flows, on page 568
clear app cflowd statistics, on page 570
show app cflowd flow-count, on page 723
show app cflowd flows, on page 724
show app cflowd template, on page 727
show policy from-vsmart, on page 971

show app cflowd template

show app cflowd template—Display the cflowd template information that the vEdge router transmits periodically to the cflowd collector (on vEdge routers only).

Command Syntax

show app cflowd template [**name** *template-name*] [**flow-active-timeout**] [**flow-inactive-timeout**] [**template-refresh**]

Syntax Description

None	Options Display information about all the cflowd templates that the vEdge router has learned from a vSmart controller.
nametemplate-name	Specific Template Display information about the named cflowd template.
template-refresh	Template Refresh Values Display the template refresh values for the cflowd templates learned from a vSmart controller.
flow-active-timeout **flow-inactive-timeout**	Timeout Values Display the active or inactive flow timeout values for the cflowd templates learned from a vSmart controller.

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show app cflowd template

```
vEdge# show app cflowd template

app cflowd template name cflowd-server-10
app cflowd template flow-active-timeout 30
app cflowd template flow-inactive-timeout 30
app cflowd template template-refresh 600
```

Related Topics

cflowd-template, on page 121
clear app cflowd flows, on page 568
clear app cflowd statistics, on page 570

show app cflowd collector, on page 722
show app cflowd flow-count, on page 723
show app cflowd flows, on page 724
show app cflowd statistics, on page 726
show policy from-vsmart, on page 971

show app dpi applications

show app dpi applications—Display application-aware applications running on the vEdge router (on vEdge routers only).

Command Syntax

show app dpi applications [**vpn** *vpn-id*]

Syntax Description

None	List all applications running on the subnets connected to the vEdge router.
vpnvpn-id	Specific VPN List all applications running in the subnets in the specific VPN.

Command History

Release	Modification
15.2.	Command introduced.
17.1.2.	Removed Source IP and Total Flows fields from command output.

Examples

Show app dpi applications

```
vEdge# show app dpi applications
                                                        EXPIRED
VPN  APPLICATION             FAMILY               FLOWS  LAST SEEN                PACKETS
  OCTETS
-------------------------------------------------------------------------------------------
1    dns                      Network Service       25     2017-05-15T14:05:23+00:00  100
     10326
1    google_accounts          Web                   2      2017-05-15T14:04:43+00:00  28
     6520
1    https                    Web                   35     2017-05-15T14:04:43+00:00  1282
     191073
```

Related Topics

app-visibility, on page 69
clear app dpi all, on page 570
clear app dpi apps, on page 571

clear app dpi flows, on page 573
show app dpi flows, on page 729
show app dpi supported-applications, on page 732

show app dpi flows

show app dpi flows—Display flow information for the application-aware applications running on the vEdge router (on vEdge routers only).

show app dpi flows [**vpn** *vpn-id*] [**detail**]

Syntax Description

None	List all application flows running on the subnets connected to the vEdge router.
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. Tunnels-in refers to packets sent from the device into a tunnel towards remote edge. Tunnels-out refers to packets received on the device from a remote edge. **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.
source-ip-address	Source IP Address Within a specific VPN, list the applications flows with the specified source IP address.
vpn *vpn-id*	Specific VPN List all application flows running in the subnets in the specific VPN.

Command History

Release	Modification
15.2.	Command introduced.
16.2.	Added **detail** option.

Examples

Show app dpi flows

```
vEdge# show app dpi flows
                                        SOURCE   DEST
```

```
VPN  SRC IP         DST IP         PORT    PORT   PROTOCOL  APPLICATION  FAMILY
  ACTIVE SINCE
-------------------------------------------------------------------------------------------------------------
1    10.0.0.1    10.255.255.254   20581   443    udp       unknown      Standard
 2015-05-04T14:07:46+00:00
1    10.0.0.1    10.255.255.254  55742   5228   tcp       gtalk        Instant Messaging
2015-05-03T21:06:57+00:00
1    10.0.0.1    10.255.255.254   36597   443    tcp       google       Web
 2015-05-04T14:12:43+00:00
1    10.0.0.1    10.255.255.254   36598   443    tcp       google       Web
 2015-05-04T14:12:45+00:00
1    10.0.0.1    10.255.255.254   63665   53     udp       dns          Network Service
 2015-05-04T14:14:40+00:00
1    10.0.0.1    10.255.255.254  40616   443    tcp       https        Web
2015-05-04T14:12:02+00:00
1    10.0.0.1    10.255.255.254  45889   443    tcp       https        Web
2015-05-04T14:14:40+00:00
1    10.0.0.1    10.255.255.254  45903   443    tcp       https        Web
2015-05-04T14:14:40+00:00
1    10.0.0.1    10.255.255.254  10000   10000  udp       sip          Audio/Video
2015-05-03T08:22:51+00:00
1    10.0.0.1    10.255.255.254  51586   22     tcp       ssh          Encrypted
2015-05-04T13:28:03+00:00
```

```
vEdge# show app dpi flows detail
app dpi flows vpn 1 10.0.0.1 10.255.255.254 38967 8002 tcp
application  iperf
family       "Network Management"
starting-application unknown
 starting-family network-service
 sticky false
active-since 2016-05-16T07:52:38+00:00
packets      14500
octets       14321048
tunnels-in 1
  local-tloc 2001:DB8:1::1
  local-tloc color default
  local-tloc encap dtls
  remote-tloc 2001:DB8:1::1
  remote-tloc color default
  remote-tloc encap dtls
  packets    14500
  octets     14321048
  start-time 2016-05-16T07:52:38+00:00
tunnels-out 1
  local-tloc ip ::23
  local-tloc color default
  local-tloc encap dtls
  remote-tloc 2001:DB8:1::1
  remote-tloc color default
  remote-tloc encap dtls
  packets    0
  octets     0
  start-time 2016-05-16T07:52:38+00:00
```

```
Device# show app dpi flows detail
app dpi flows vpn 1 10.0.0.1 10.255.255.254 47011 443 tcp
 application whatsapp
 family instant-messaging
 starting-application unknown
 starting-family network-service
```

```
sticky false
active-since 2021-07-01T18:04:24+00:00
packets 55
octets 9027
tunnels-in 1
 local-tloc TLOC IP 172.31.255.254
 local-tloc color lte
 local-tloc encap ipsec
 remote-tloc TLOC IP 172.31.255.254
 remote-tloc color lte
 remote-tloc encap ipsec
 packets 32
 octets 7140
 start-time 2021-07-01T18:04:24+00:00
tunnels-out 1
 local-tloc ip 172.31.255.254
 local-tloc color lte
 local-tloc encap ipsec
 remote-tloc TLOC IP 172.31.255.254
 remote-tloc color lte
 remote-tloc encap ipsec
 packets 23
 octets 1887
 start-time 2021-07-01T18:04:24+00:00
```

Related Topics

app-visibility, on page 69
clear app dpi all, on page 570
clear app dpi apps, on page 571
clear app dpi flows, on page 573
show app dpi applications, on page 728
show app dpi supported-applications, on page 732

show app dpi summary statistics

show app dpi summary statistics—Display summary statistics for DPI flows on the vEdge router.

show app dpi summary statistics

Syntax Description

Syntax Description

None

Command History

Release	Modification
15.3.	Command introduced.

Examples

Show app dpi summary statistics

```
vEdge# show app dpi summary statistics
Dpi status               enable
Flows created            16
Flows expired            2
Current flows            11
Peak flows               13
Current rate             7
Peak rate                10
```

Dpi status	Indicates whether **DPI** is enabled or disabled on the vEdge router. DPI must be **enabled** for application-aware routing and traffic classification to function.
Flows created	Total number of flows created since the vEdge router started or since the DPI statistics were last cleared. A flow represents a stream of packets with the same 5-tuple (source IP, destination IP, source port, destination port, and protocol).
Flows expired	Number of flows that have expired and are no longer active. A flow can expire due to: • Timeout (no traffic seen for a specific period) • Normal flow termination (for example, TCP session closure)
Current flows	Number of active flows currently being tracked by the DPI engine and the number of concurrent active sessions on the router.
Peak flows	Highest number of concurrent flows observed on the router and the number of concurrent active sessions handled by vEdge.
Current rate	Number of flows being processed per second.
Peak rate	Highest rate of flow creation observed since the DPI engine started.

Related Topics

app-visibility, on page 69
clear app dpi apps, on page 571
clear app dpi flows, on page 573
show app dpi applications, on page 728
show app dpi flows, on page 729
show app dpi supported-applications, on page 732

show app dpi supported-applications

show app dpi supported-applications—List all the application-aware applications supported by the SD-WAN software on the vEdge router (on vEdge routers only) .

Command Syntax

show app dpi supported-applications

show app dpi supported-applications | tab

Syntax Description

None	List the application name and its family.
Pipe Output To Tabular Format	Pipe Output To Tabular Format List full information about the application, including its shortened and long name, family shortened and long name, and application identifier number.

Command History

Release	Modification
15.2.	Command introduced.

Usage Guidelines

To understand the applications available for each family, you can use command: **show app dpi supported-applications | inc <app_family>**.

The following example shows the supported application for Web family:

```
vEdge# show app dpi supported-applications | <web>

      APP
APPLICATION  FAMILY              APPLICATION LONG NAME                    FAMILY LONG NAME
     ID
-------------------------------------------------------------------------------------------------

dr           web                 Dr.dk                                    Web
      2043
dv           web                 DV.is                                    Web
      1861
hs           web                 Hs.fi (Helsingin Sanomat)                Web
      2097
ja           web                 Ja.is                                    Web
      1897
mk           web                 Mk.co.kr                                 Web
      1213
mt           web                 mt                                       Web
      1214
nu           web                 Nu.nl                                    Web
      2119
rt           web                 Rt.com                                   Web
      2064
ss           web                 Ss.lv                                    Web
      1943
ts           web                 Ts                                       Web
      2427
tv           web                 Tv.com                                   Web
      1062
vg           web                 Vg.no                                    Web
      2076
wp           web                 Wp.pl                                    Web
      2078
xl           web                 Xl                                       Web
```

```
      2190
y8            web                 Y8.com                                  Web
      1758
yr            web                 Yr                                      Web
      2579
17u           web                 17u.com                                 Web
      1341
24h           web                 24h.com.vn                              Web
      1820
2ch           web                 2ch.net                                 Web
      1316
```

Examples

Display abbreviated application information:

Show app dpi supported-applications

```
vEdge# show app dpi supported-applications

APPLICATION                FAMILY
-------------------------------------------------------
ah                         network_service
dr                         web
dv                         web
hs                         web
il                         network_service
ip                         network_service
ja                         web
mk                         web
mq                         application_service
mt                         web
nu                         web
pp                         network_service
qq                         instant_messaging
rt                         web
sm                         network_service
sp                         network_service
ss                         web
st                         network_service
ts                         web
tu                         audio_video
tv                         web
...
unassigned_ip_prot_251     network_service
unassigned_ip_prot_252     network_service
the_simpsons_tapped_out    game
wallstreetjournal_china    web

vEdge# show app dpi supported-applications bi?

APPLICATION             FAMILY
---------------------------------------
biip                    Web
bild                    Web
bing                    Web
bits                    File Transfer
bithq                   Peer to Peer
bitme                   Peer to Peer
bigeye                  Web
bikhir                  Web
bigadda                 Web
```

```
bigtent                 Web
bitcoin                 Peer to Peer
bitlord                 Peer to Peer
bitmetv                 Peer to Peer
bitsoup                 Peer to Peer
bidorbuy                Web
bitenova                Peer to Peer
bitshock                Peer to Peer
bitworld                Peer to Peer
bigupload               Web
bitseduce               Peer to Peer
bitstrips               Game
biglobe_ne              Web
bittorrent              Peer to Peer
bitvaulttorrent         Peer to Peer
bitdefender_update      Web
bittorrent_application  Peer to Peer
vEdge#
```

Examples

Display full application information:

```
vEdge# show app dpi supported-applications | tab

      APP
APPLICATION  FAMILY               APPLICATION LONG NAME                    FAMILY LONG NAME
     ID
-------------------------------------------------------------------------------------------------

ah           network_service      Authentication Header                     Network Service
      720
dr           web                  Dr.dk                                     Web
      2043
dv           web                  DV.is                                     Web
      1861
hs           web                  Hs.fi (Helsingin Sanomat)                 Web
      2097
il           network_service      Internet Link (Transport protocol)        Network Service
      637
ip           network_service      Internet Protocol                         Network Service
      81
ja           web                  Ja.is                                     Web
      1897
mk           web                  Mk.co.kr                                  Web
      1213
mq           application_service  IBM Websphere MQ                          Application
Service  312
mt           web                  mt                                        Web
      1214
nu           web                  Nu.nl                                     Web
      2119
pp           network_service      ISO 8823 Presentation Protocol            Network Service
      938
qq          instant_messaging    QQ                                       Instant Messaging
    156
rt           web                  Rt.com                                    Web
      2064
sm           network_service      Sparse Mode                               Network Service
      678
sp           network_service      ISO 8327 Session Protocol                 Network Service
      937
```

```
ss            web                  Ss.lv                                    Web
      1943
st            network_service      Stream protocol                          Network Service
      685
ts            web                  Ts                                       Web
      2427
tu            audio_video          Tu.tv                                    Audio/Video
      1060
tv            web                  Tv.com                                   Web
      1062
vg            web                  Vg.no                                    Web
      2076
wp            web                  Wp.pl                                    Web
      2078
xl            web                  Xl                                       Web
      2190
y8            web                  Y8.com                                   Web
      1758
yr            web                  Yr                                       Web
      2579
17u           web                  17u.com                                  Web
      1341
24h           web                  24h.com.vn                               Web
      1820
2ch           web                  2ch.net                                  Web
      1316
3pc           network_service      Third Party Connect                      Network Service
      606
abc           peer_to_peer         ABC Bittorrent client                    Peer to Peer
      1690
abv           web                  Abv.bg                                   Web
      1826
adc           peer_to_peer         Advanced Direct Connect                  Peer to Peer
      1438
adf           web                  AdF.ly                                   Web
      2824
adp           web                  Automatic Data Processing (ADP)          Web
      3275
afl           web                  AFL                                      Web
      2538
afp           file_server          Apple Filing Protocol                    File Server
      2645
aib           web                  Aib                                      Web
      2185
aim          instant_messaging    AOL Instant Messenger (formerly OSCAR)   Instant Messaging
    8
--More--
```

```
vEdge# show app dpi supported-applications m* | tab


APPLICATION  FAMILY               APPLICATION LONG NAME                        FAMILY LONG
 NAME     ID
-----------------------------------------------------------------------------------------------

mk           web                  Mk.co.kr                                     Web
          1213
mq           application_service  IBM Websphere MQ                             Application
 Service  312
mt           web                  mt                                           Web
          1214
mbc          web                  MBC (Munhwa Broadcasting Corp)               Web
          1231
```

```
mbl          web                 Mbl.is                                    Web
          2110
mbn          web                 MBN.co.kr                                 Web
          1212
mcs          network_service     Multipoint Communication Service          Network
Service      112
mms          audio_video         Microsoft Multimedia Streaming            Audio/Video
          115
mog          audio_video         MOG.com                                   Audio/Video
          447
mop          web                 Mop.com                                   Web
          1276
msn          instant_messaging   MSN Messenger                             Instant
Messaging    120
mtn          web                 MTN Group                                 Web
          3023
mtp          network_service     Multicast Transport Protocol              Network
Service      656
mtv          web                 MTV                                       Web
          1021
mux          network_service     Multiplexing                              Network
Service      657
m2pa         network_service     MTP2 User Peer-to-Peer Adaptation Layer    Network
Service      1304
m2ua         network_service     MTP2 User Adaptation Layer                Network
Service      1302
m3ua         network_service     MTP3 User Adaptation Layer                Network
Service      1301
mako         web                 Mako.co.il                                Web
          2107
mana         web                 Mana.pf                                   Web
          1919
manx         web                 Manx Telecom                              Web
          2874
mapi         mail                MS Exchange Message API                   Mail
          110
mapy         web                 Mapy                                      Web
          2367
mebc         web                 Middle East Broadcasting Center (MBC Group)  Web
          2902
mega         web                 MEGA                                      Web
          1299
mgcp         audio_video         Media Gateway Control Protocol            Audio/Video
          113
mgid         web                 MGID                                      Web
          3203
micp         network_service     Mobile Internetworking Control Protocol   Network
Service      724
mimp         webmail             IMP mobile version                        Webmail
          326
miro         peer_to_peer        Miro (getmiro.com)                        Peer to Peer
         1548
mixi         web                 Mixi.jp                                   Web
          444
mmse         wap                 MultiMedia Messages Encapsulation         Wap
          116
moat         web                 Moat                                      Web
          2704
moov         web                 Moov.mg                                   Web
          1922
mpls         routing             Multiprotocol Packet Label Switching      Routing
          119
mqtt         middleware          MQ Telemetry Transport                    Middleware
          2900
```

```
msrp          audio_video          Message Session Relay Protocol               Audio/Video
          919
mubi          audio_video          Mubi                                         Audio/Video
          2412
mute          peer_to_peer         Mute                                       Peer to Peer
         124
--More--
```

Related Topics

app-visibility, on page 69
clear app dpi all, on page 570
clear app dpi apps, on page 571
clear app dpi flows, on page 573
show app dpi applications, on page 728
show app cflowd flows, on page 724
show app dpi flows, on page 729

show app log flow-count

show app log flow-count—Display the count of packet flows that are being logged (on vEdge routers only). Packet flows include a flow that matches an access list (ACL), a cflowd flow, or a DPI flow.

Command Syntax

show app log flow-count[**vpn** *vpn-id*]

Syntax Description

None	Display the count of all packet flows that are being logged.
vpn*vpn-id*	Specific VPN Display the count of packet flows in the specified VPN.

Command History

Release	Modification
16.3..	Command introduced.

Examples

Show app log flow-count

```
vEdge# show app log flow-count

VPN   COUNT
------------
1     20
```

Related Topics

clear app log flow-all, on page 574
clear app log flows, on page 575
log-frequency, on page 295
show app log flows, on page 739
show system statistics, on page 1015

show app log flows

show app log flows—Display logging information for packet flows (on vEdge routers only). Packet flows include flows that match an access list (ACL), a cflowd flow, and a DPI flow. Packet flows are logged when you configure a **log** action in a localized data policy (ACL), data policy for cflowd traffic monitoring, or an application-aware routing policy

Command Syntax

show app log flows [**vpn** *vpn-id*] [*flow-parameter*]

vManage Screen

Monitor ► Network ► ACL Logs

Syntax Description

None	Display all flow logging information.
flow-parameter	Flow Parameter Display flow logging information for a specific parameter. *flow-parameter* can be one of **egress-intf-name**, **icmp-opcode**, **ingress-intf-name**, **nhop-ip**, **policy-action**, **policy-direction**, **policy-name**, **start-time**, **tcp-cntrl-bits**, **time-to-expire**, **total-bytes**, and **total-pkts**. These parameters correspond to the column headings in the output of the **show app log flows** command.
vpn*vpn-id*	Specific VPN Display the flow logging information in the specified VPN.

Command History

Release	Modification
16.3.	Command introduced.

Examples

show app log flows

```
vEdge# show app log flows
```

```
                                                                  TCP
                                    TIME    EGRESS  INGRESS
                                SRC DEST        IP     CNTRL  ICMP                TOTAL
TOTAL                             TO    INTF    INTF                       POLICY  POLICY
VPN  SRC IP      DEST IP     PORT   PORT  DSCP  PROTO  BITS   OPCODE  NHOP IP     PKTS
BYTES     START TIME                EXPIRE  NAME    NAME     POLICY NAME      ACTION
DIRECTION
-------------------------------------------------------------------------------------------------------------------------------
0    10.0.5.19   10.1.15.15  23556  34576  0     6      16     0       10.1.15.15  8531
1200071   Tue Aug  2 10:32:52 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.12.20  10.1.15.15  23556  39482  0     6      24     0       10.1.15.15  8459
1195449   Tue Aug  2 10:32:52 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.12.26  10.1.15.15  0      0      0     1      0      0       10.1.15.15  1127
110446    Tue Aug  2 10:00:43 2016  54      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.101.1  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  8983
2246402   Tue Aug  2 10:48:41 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.101.2  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  8983
2246402   Tue Aug  2 10:48:41 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.101.3  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  8983
2246402   Tue Aug  2 10:48:41 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.101.4  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  8983
2246402   Tue Aug  2 10:48:41 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.111.1  10.1.15.15  12366  12346  48    17     0      0       10.1.15.15  21157
11852774  Tue Aug  2 10:00:38 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.0.111.2  10.1.15.15  12366  12346  48    17     0      0       10.1.15.15  21305
12021134  Tue Aug  2 10:00:38 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.1.14.14  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  15566
3879908   Tue Aug  2 10:00:39 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
0    10.1.15.15  10.0.5.19   34576  23556  48    6      24     0       0.0.0.0     8450
1170516   Tue Aug  2 10:32:52 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.12.20  39482  23556  48    6      24     0       0.0.0.0     8324
1162324   Tue Aug  2 10:32:52 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.12.26  0      0      0     1      0      2048    0.0.0.0     1127
110446    Tue Aug  2 10:00:43 2016  54      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.101.1  12346  12346  48    17     0      0       0.0.0.0     8984
2120800   Tue Aug  2 10:48:41 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.101.2  12346  12346  48    17     0      0       0.0.0.0     8984
2120800   Tue Aug  2 10:48:41 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.101.3  12346  12346  48    17     0      0       0.0.0.0     8984
2120800   Tue Aug  2 10:48:41 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.101.4  12346  12346  48    17     0      0       0.0.0.0     8984
```

```
2120800   Tue Aug  2 10:48:41 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.111.1  12346  12366  48    17     0      0       0.0.0.0     14780
3055280   Tue Aug  2 10:34:08 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.0.111.2  12346  12366  48    17     0      0       0.0.0.0     15025
3107792   Tue Aug  2 10:34:08 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.1.14.14  12346  12346  48    17     0      0       0.0.0.0     15566
3674704   Tue Aug  2 10:00:39 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.15.15  10.1.16.16  12346  12346  48    17     0      0       0.0.0.0     10966
2588240   Tue Aug  2 10:34:08 2016  59      cpu     cpu      123NenokaKantri  accept
outbound-acl
0    10.1.16.16  10.1.15.15  12346  12346  48    17     0      0       10.1.15.15  15547
3876810   Tue Aug  2 10:00:39 2016  59      cpu     ge0/0    123NenokaKantri  accept
inbound-acl
```

Related Topics

action, on page 34
clear app log flow-all, on page 574
clear app log flows, on page 575
log-frequency, on page 295
policy, on page 382
show app log flow-count, on page 738
show system statistics, on page 1015

show app tcp-opt

show app tcp-opt—Display information about TCP-optimized flows (on vEdge routers only).

Command Syntax

show app tcp-opt (**active-flows** | **expired-flows**)

show app tcp-opt summary

Syntax Description

active-flows	Active Flows Display information about active TCP-optimized flows.
expired-flows	Expired Flows Display information about expired TCP-optimized flows.
summary	Flow Summary Display a summary of the TCP-optimized flows.

Command History

Release	Modification
17.2.	Command introduced.

Examples

Display information about active and expired TCP-optimized flows:

Show app tcp-opt

```
vEdge# show app tcp-opt active-flows


app tcp-opt active-flows vpn 1 src-ip 10.20.24.17 dest-ip 10.20.25.18 src-port 53723 dest-port
 22
 start-time        "Fri Mar 17 13:21:02 2017"
 egress-intf-name  loop0.3
 ingress-intf-name ge0_4
 tx-bytes          153
 rx-bytes          64
 tcp-state         "In progress"
 proxy-identity    Client-Proxy

vEdge# show app tcp-opt expired-flows
app tcp-opt expired-flows 1489781786360 vpn 1 src-ip 10.20.24.17 dest-ip 10.20.25.18 src-port
 53722 dest-port 22
 start-time     "Fri Mar 17 13:16:26 2017"
 end-time       "Fri Mar 17 13:17:51 2017"
 tx-bytes       4113
 rx-bytes       4333
 tcp-state      Optimized
 proxy-identity Client-Proxy
 del-reason     Closed
```

Related Topics

data-policy, on page 165
tcp-optimization, on page 479

show app-route sla-class

show app-route sla-class—Display information about the SLA classes operating on the vEdge router (on vEdge routers only).

Note that when the thresholds cross for one of these SLA classes, a notification and a syslog are triggered.

Command Syntax

show app-route sla-class

show app-route sla-class (**latency** [*milliseconds*] | **loss** [*percentage*] | **name** [*string*])

Syntax Description

None	Display information for all SLA classes configured and operating on the vEdge router
latency[*milliseconds*]	Packet Latency Display information for all packet latency values or for the specified latency value operating on the vEdge router.
loss[*percentage*]	Packet Loss Display information for all packet loss values or for the specified loss value operating on the vEdge router.
name[*string*]	SLA Class Name Display information for all SLA class names or for the specified class name operating on the vEdge router.

Command History

Release	Modification
15.2.	Command introduced.

Examples

The following output shows three SLA classes and the index numbers that identify these classes. The first line of the output shows the default SLA class (__all_tunnels_sc), and second and third lines show two configured SLA classes that are operating on the router (test_sla_class and test_sla_class1).

Show app-route sla-class

```
vEdge# show app-route sla-class

INDEX   NAME                    LOSS  LATENCY
-----------------------------------------------
0       __all_tunnels_sc        100   2147483647
1       test_sla_class          100   50
2       test_sla_class1         1     1
```

Related Topics

app-route-policy, on page 67
bfd color, on page 106
show app-route stats, on page 744
show bfd sessions, on page 748
show policy service-path, on page 973
show policy tunnel-path, on page 974

show app-route stats

show app-route stats—Display statistics about data traffic traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels (on vEdge routers only). The command also displays the index of the SLA classes that are dampened and the dampening left for the SLA class. You can use the information from the command output to fashion application-aware routing policy.

Command Syntax

show app-route-statsshow app-route stats local-color *color* [**remote-system-ip** *ip-address*]

show app-route stats remote-color *color* [**remote-system-ip** *ip-address*]

show app-route stats remote-system-ip *ip-address*

Syntax Description

None	Display data traffic statistics for all data plane tunnel connections.
local-color*color*	Local TLOC Color Display data traffic statistics for the specified local TLOC color.
remote-system-ip*ip-address*	Remote System IP Address Display data traffic statistics for the specified remote system.
remote-color*color*	Remote TLOC Color Display data traffic statistics for the specified remote TLOC color.

Command History

Release	Modification
14.2.	Command introduced.
15.2.	**sla-class-index** option added.
15.3.	Syntax changed and simplified.
20.5	The commands displays the index of the SLA classes that are dampened and the dampening left for the SLA class.

Examples

show app-route stats

```
vEdge# show app-route stats


app-route statistics 184.111.1.2 184.118.101.2 ipsec 12346 12346
 remote-system-ip 172.16.248.101
```

```
 local-color      mpls
 remote-color     mpls
 mean-loss        0
 mean-latency     5
 sla-class-index  0

       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      592      0     4        8        0        0
1      592      0     4        8        0        0
2      592      0     6        11       0        0
3      592      0     4        8        0        0
4      593      0     5        9        0        0
5      590      0     4        8        0        0

app-route statistics 184.111.1.2 184.116.102.2 ipsec 12346 12346
 remote-system-ip 172.16.248.102
 local-color      mpls
 remote-color     mpls
 mean-loss        1
 mean-latency     4
 sla-class-index  0

       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      591      64    4        7        0        0
1      594      0     5        8        0        0
2      590      0     5        10       0        0
3      592      0     4        8        0        0
4      593      0     4        8        0        0
5      589      0     4        8        0        0

app-route statistics 184.111.1.2 184.120.103.2 ipsec 12346 12346
 remote-system-ip 172.16.248.103
 local-color      mpls
 remote-color     mpls
 mean-loss        17
 mean-latency     5
 sla-class-index  0

       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      590      140   4        7        0        0
1      594      0     5        9        0        0
2      592      0     6        11       0        0
3      591      0     4        8        0        0
4      593      0     5        10       0        0
5      590      475   5        9        0        0
...


vEdge# show app-route stats
app-route statistics 192.168.0.1 192.168.101.2 ipsec 12346 12386
 remote-system-ip 172.16.248.101
 local-color      public-internet
 remote-color     public-internet
 mean-loss
 mean-latency     15
 sla-class-index  0, 1
 Dampening-sla-class-index 2,3
 Dampening-multiplier-left 10,20
```

```
TOTAL           AVERAGE   AVERAGE   TX DATA   RX DATA
INDEX   PACKETS   LOSS   LATENCY   JITTER    PKTS      PKTS
-------------------------------------------------------------
0       600       0      16        21        0         0
1       600       0      14        18        0         0
2       599       0      17        20        0         0
3       599       0      14        18        0         0
4       600       0      15        19        0         0
5       599       0      15        19        0         0
...
```

Related Topics

app-route-policy, on page 67
bfd color, on page 106
show app-route sla-class, on page 742
show bfd sessions, on page 748
show policy service-path, on page 973
show policy tunnel-path, on page 974

show arp

show arp—Display the IPv4 entries in the Address Resolution Protocol (ARP) table, which lists the mapping of IPv4 addresses to device MAC addresses.

To display IPv6 ARP table entries, use the **show ipv6 neighbor** command.

Command Syntax

show arp [**vpn** *vpn-id*]

Syntax Description

None	List all the IPv4 entries in the ARP table.
vpn*vpn-id*	VPN List the ARP table entries for the specified VPN.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show arp

```
Cisco vEdge# show arp
     IF
```

```
VPN  NAME   IP           MAC                STATE    IDLE TIMER  UPTIME
-------------------------------------------------------------------------------
0    ge0/0  10.0.11.1    00:0c:29:86:ea:83  static   -           0:10:10:07
0    ge0/7  10.0.100.11  00:0c:29:86:ea:c9  static   -           0:10:10:07
512  eth0   10.0.1.1     00:50:56:c0:00:01  dynamic  0:00:19:04  0:00:05:04
512  eth0   10.0.1.11    00:50:56:00:01:01  static   -           0:10:10:03
512  eth0   10.0.1.254   00:50:56:ed:b5:5e  dynamic  0:00:17:04  0:00:09:04
```

Related Topics

arp, on page 79
clear arp, on page 577
show ipv6 neighbor, on page 882

show bfd history

show bfd history—Display the history of the BFD sessions running on a vEdge router (on vEdge routers only). BFD sessions between vEdge routers start automatically, with requiring any configuring, as soon as at least two vEdge routers are running in the Cisco SD-WAN network. The sessions run over an IPsec tunnel between the two devices.

Command Syntax

show bfd history [**color** *color*] [**site-id** *site-id*] [**state** *state*] [**system-ip** *ip-address*]

Syntax Description

None	Show the history of all the BFD sessions running on the vEdge router.
state *state*	BFD State Display the history of BFD sessions in a particular state. *state* can be one of the following: **admin-down**, **down**, **init**, **invalid**, and **up**.
color *color*	Color Display the history of BFD sessions for a specific traffic flow.
site-id *site-id*	Site ID Display the history of BFD sessions to a specific Cisco SD-WAN network site.
system-ip *ip-address*	System IP Display the history of BFD sessions to a specific device in the Cisco SD-WAN network.

Command History

Release	Modification
14.1.	Command introduced.
Cisco SD-WAN Release 20.3.1	New status added to STATE column: **inactive** indicates that an on-demand tunnel is in Inactive mode on a device with on-demand tunnels enabled.

Examples

show bfd history

```
RX      TX
SYSTEM IP        SITE ID  COLOR            STATE       IP               PORT        ENCAP
 TIME                     PKTS    PKTS     DEL
-------------------------------------------------------------------------------------------
10.0.104.1       300      lte               up          192.168.10.100   12366       ipsec
 2020-07-21T16:44:54+0000 0       0        0
10.0.104.1       300      lte               down        192.168.10.100   12366       ipsec
 2020-07-21T16:46:46+0000 0       0        0
10.0.104.1       300      lte               down        192.168.10.100   12366       ipsec
 2020-07-21T16:46:46+0000 0       0        1
10.0.104.1       300      lte               inactive    192.168.10.100   12366       ipsec
 2020-07-21T16:46:46+0000 0       0        0
10.0.104.1       300      lte               down        192.168.10.100   12366       ipsec
 2020-07-21T18:39:02+0000 0       0        0
10.0.104.1       300      lte               up          192.168.10.100   12366       ipsec
 2020-07-21T18:39:04+0000 0       0        0
10.0.104.1       300      lte               down        192.168.10.100   12366       ipsec
 2020-07-21T18:40:52+0000 0       0        0
10.0.104.1       300      lte               down        192.168.10.100   12366       ipsec
 2020-07-21T18:40:52+0000 0       0        1
10.0.104.1       300      lte               inactive    192.168.10.100   12366       ipsec
 2020-07-21T18:40:52+0000 0       0        0
```

Related Topics

bfd color, on page 106
show bfd sessions, on page 748
show bfd summary, on page 750
show bfd tloc-summary-list, on page 751

show bfd sessions

show bfd sessions—Display information about the BFD sessions running on the local vEdge router (on vEdge routers only). BFD sessions between vEdge routers start automatically, without requiring any configuring, as soon as at least two vEdge routers are running in the Cisco SD-WAN network. The BFD sessions run over an IPsec connection between the two devices.

Command Syntax

show bfd sessions [**color** *color*] [**site-id** *site-id*] [**state** *state*] [**system-ip** *ip-address*]

Syntax Description

None	Show the history of all the BFD sessions running on the vEdge router.
state *state*	BFD State Display the history of BFD sessions in a particular state. *state* can be one of the following: **admin-down**, **down**, **init**, **invalid**, and **up**.

color *color*	Color Display the history of BFD sessions for a specific traffic flow.
site-id *id*	Site ID Display the history of BFD sessions to a specific Cisco SD-WAN network site.
system-ip *ip-address*	System IP Display the history of BFD sessions to a specific device in the Cisco SD-WAN network.

Command History

Release	Modification
14.1.	Command introduced.
16.3.	Added support to display IPv6 end points.

Examples

Display BFD session information for network end points:

Show bfd sessions

```
vEdge# show 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
-------------------------------------------------------------------------------------------------------
172.16.241.1     30001001 up          mpls             mpls              184.116.102.2
174.11.1.2       12346       ipsec  20          1000             0:01:46:50      0

172.16.241.1     30001001 up          private1         mpls              186.116.102.2
174.11.1.2       12346       ipsec  20          1000             0:01:46:51      0

172.16.241.2     30001002 up          mpls             mpls              184.116.102.2
174.11.2.2       12346       ipsec  20          1000             0:01:41:27      2

172.16.241.2     30001002 up          private1         mpls              186.116.102.2
174.11.2.2       12346       ipsec  20          1000             0:01:41:28      2

172.16.241.3     30001003 up          mpls             mpls              184.116.102.2
174.11.3.2       12346       ipsec  20          1000             0:01:40:30      2

172.16.241.3     30001003 up          private1         mpls              186.116.102.2
174.11.3.2       12346       ipsec  20          1000             0:01:40:31      0

172.16.241.4     30001004 up          mpls             mpls              184.116.102.2
174.11.4.2       12346       ipsec  20          1000             0:01:33:46      2

172.16.241.4     30001004 up          private1         mpls              186.116.102.2
174.11.4.2       12346       ipsec  20          1000             0:01:33:46      2

172.16.241.5     30001005 up          mpls             mpls              184.116.102.2
174.11.5.2       12346       ipsec  20          1000             0:01:52:44      0
```

```
172.16.241.5     30001005 up          private1         mpls            186.116.102.2
174.11.5.2       12346       ipsec  20          1000          0:01:52:45      0

172.16.241.6     30001006 up          mpls             mpls            184.116.102.2
174.11.6.2       12346       ipsec  20          1000          0:17:04:30      6

172.16.241.6     30001006 up          private1         mpls            186.116.102.2
174.11.6.2       12346       ipsec  20          1000          0:17:04:31      5

172.16.241.7     30001007 up          mpls             mpls            184.116.102.2
174.11.7.2       12346       ipsec  20          1000          0:01:41:27      13

172.16.241.7     30001007 up          private1         mpls            186.116.102.2
174.11.7.2       12346       ipsec  20          1000          0:01:41:27      13

172.16.241.8     30001008 up          mpls             mpls            184.116.102.2
174.11.8.2       12346       ipsec  20          1000          0:01:41:27      11

172.16.241.8     30001008 up          private1         mpls            186.116.102.2
174.11.8.2       12346       ipsec  20          1000          0:01:41:28      11

172.16.241.9     30001009 up          mpls             mpls            184.116.102.2
174.11.9.2       12346       ipsec  20          1000          0:01:47:08      5

172.16.241.9     30001009 up          private1         mpls            186.116.102.2
174.11.9.2       12346       ipsec  20          1000          0:01:47:09      5

172.16.241.10    300010010up          mpls             mpls            184.116.102.2
174.11.10.2      12346       ipsec  20          1000          0:16:54:13      1

172.16.241.10    300010010up          private1         mpls            186.116.102.2
174.11.10.2      12346       ipsec  20          1000          0:16:54:14      1

172.16.241.11    300010011up          mpls             mpls            184.116.102.2
174.11.11.2      12346       ipsec  20          1000          0:01:52:39      0
```

Related Topics

bfd color, on page 106
show bfd history, on page 747
show bfd summary, on page 750
show bfd tloc-summary-list, on page 751

show bfd summary

show bfd summary—Display summary information about the BFD sessions running on the local vEdge router (on vEdge routers only). BFD sessions between vEdge routers start automatically, with requiring any configuring, as soon as at least two vEdge routers are running in the Cisco SD-WAN network. The sessions run over an IPsec connection between the two devices.

Command Syntax

show bfd summary [**bfd-sessions-flap** | **bfd-sessions-max** | **bfd-sessions-total** | **bfd-sessions-up**]

Syntax Description

None	Display all summary information about BFD sessions running on the vEdge router.
<string>bfd-sessions-up	BFD Sessions That Are Up Display the current number of BFD sessions that are in the Up state.</string>
bfd-sessions-flap	BFD Transitions Display the number of BFD sessions that have transitioned from the Up state.
bfd-sessions-max	Maximum Number of BFD Sessions Display the total number of BFD sessions that have been created since the vEdge router booted up.
bfd-sessions-total	Total Number of BFD Sessions Display the current number of BFD sessions running on the vEdge router.

Command History

Release	Modification
15.2.	Command introduced.
17.1.	Display configured BFD app-route poll interval in command output.

Examples

Show bfd summary

```
vEdge# show bfd summary
sessions-total          4
sessions-up             4
sessions-max            4
sessions-flap           4
poll-interval           600000
```

Related Topics

bfd app-route, on page 105
bfd color, on page 106
show bfd history, on page 747
show bfd sessions, on page 748
show bfd tloc-summary-list, on page 751

show bfd tloc-summary-list

show bfd tloc-summary-list—Display BFD session summary information per TLOC (on vEdge routers only).

Command Syntax

show bfd tloc-summary-list

show bfd tloc-summary-list *interface-name* [**gre** | **ipsec** | **ipsec-ike**] [**sessions-flap** |**sessions-total** |**sessions-up**]

Syntax Description

None	Display all summary information about BFD sessions running on the vEdge router.
sessions-up	BFD Sessions That Are Up Display the current number of BFD sessions that are in the Up state.
sessions-flap	BFD Transitions Display the number of BFD sessions that have transitioned from the Up state.
[**gre** | **ipsec** | **ipsec-ike**]	Encapsulation Type Display information about BFD session with a specific encapsulation type.
interface-name	Specific Interface Display information about BFD sessions on the specified interface.
sessions-total	Total Number of BFD Sessions Display the current number of BFD sessions running on the vEdge router.

Command History

Release	Modification
16.2.3.	Command introduced.
17.2.	Added **ipsec-ike** option.

Examples

Show bfd tloc-summary-list

```
vEdge1# show bfd tloc-summary-list

                   SESSIONS  SESSIONS  SESSIONS
IFNAME     ENCAP   TOTAL     UP        FLAP
-----------------------------------------------
ge0_0      ipsec   10        9         9
ge0_3      ipsec   10        9         9

vEdge2# show bfd tloc-summary-list ge0/4 ipsec
bfd tloc-summary-list ge0/4 ipsec
Interface name         ge0/4
Encapsulation          ipsec
sessions-total         0
sessions-up            0
sessions-flap          0
```

Related Topics

bfd color, on page 106
show bfd history, on page 747
show bfd sessions, on page 748
show bfd summary, on page 750

show bgp neighbor

show bgp neighbor—List the router's BGP neighbors (on vEdge routers only).

Command Syntax

show bgp neighbor [**vpn** *vpn-id*] [**detail**]

show bgp neighbor address-family [*address-family-property*] [**detail**]

Syntax Description

None	List all BGP neighbors.
address-family[*address-family-property*]	BGP Address Family Properties List information about a specific BGP address family property. *address-family-property* can be one of the following: **accepted-prefix-count**, **afi**, **as-path-unchanged**, **def-originate-routemap**, **inbound-soft-reconfig**, **max-prefix-restart-interval**, **max-prefix-threshold-warning**, **max-prefix-warning-only**, **maximum-prefix-count**, **med-unchanged**, **nexthop-self**, **nexthop-unchanged**, **policy-in**, **policy-out**, **private-as**, **route-reflector-client**, **sent-community**, and **sent-def-originate**.
detail	Detailed Information Show detailed information.
vpn*vpn-id*	VPN List the entries in the ARP table for the specified VPN.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show bgp neighbor

```
vEdge# show bgp neighbor

                      MSG   MSG   OUT
AFI
VPN  PEER ADDR    AS  RCVD  SENT  Q    UPTIME      STATE        LAST UPTIME
ID   AFI
-------------------------------------------------------------------------------------------------------
1    10.20.25.18  2   3796  3799  0    0:01:03:17  established  Thu Mar  3 09:33:24 2016
0    ipv4-unicast

vEdge# show bgp neighbor detail
bgp bgp-neighbor vpn 1 10.20.25.18
 as                   2
 local-as-num         1
 remote-router-id     172.16.255.18
 last-read            1
 keepalive            1
 holdtime             3
 cfg-keepalive        0
 cfg-holdtime         0
 adv-4byte-as-cap     true
 rec-4byte-as-cap     true
 adv-refresh-cap      true
 rec-refresh-cap      true
 rec-new-refresh-cap  true
 msg-rcvd             3853
 msg-sent             3856
 prefix-rcvd          1
 prefix-valid         1
 prefix-installed     1
 outQ                 0
 uptime               0:01:04:14
 state                established
 open-in-count        0
 open-out-count       1
 notify-in-count      0
 notify-out-count     0
 update-in-count      2
 update-out-count     2
 keepalive-in-count   3851
 keepalive-out-count  3852
 refresh-in-count     0
 refresh-out-count    1
 dynamic-in-count     0
 dynamic-out-count    0
 adv-interval         1
 conn-established     1
 conn-dropped         0
 local-host           10.20.25.16
 local-port           179
 remote-host          10.20.25.18
 remote-port          58647
 next-hop             10.20.25.16
 read-thread-on       true
 password             d5a2***d0
 last-uptime          "Thu Mar  3 09:33:24 2016"
```

Related Topics

show bgp routes, on page 755
show bgp summary, on page 758

show bgp routes

show bgp routes—List the router's BGP neighbors (on vEdge routers only).

Command Syntax

show bgp routes [*prefix*/*length*] [**vpn** *vpn-id*] [**detail**]

Syntax Description

None	List all BGP neighbors.
detail	Detailed Information Show detailed information.
prefix/*length prefix* **vpn** *vpn-id*	Route Prefix Show the BGP route information for the specified route prefix. If you omit the prefix length, you must specify a VPN identifier so that the Cisco SD-WAN software can find the route that best matches the prefix.
vpn *vpn-id*	VPN List the BGP routes for the specified VPN.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show bgp routes

```
vEdge# show bgp routes vpn 1

                         INFO                        LOCAL                       AS

VPN   PREFIX             ID     NEXTHOP      METRIC   PREF    WEIGHT   ORIGIN      PATH    PATH
STATUS          TAG
-------------------------------------------------------------------------------------------------
1     10.2.2.0/24        0      0.0.0.0      1000     50      0        incomplete  Local
valid,best           0
1     10.2.3.0/24        0      0.0.0.0      1000     50      0        incomplete  Local
valid,best           0
1     10.20.24.0/24      0      0.0.0.0      1000     50      0        incomplete  Local
valid,best           0
```

```
1    56.0.1.0/24        0     0.0.0.0      1000    50     0       incomplete  Local
valid,best           0
1    172.16.255.112/32  0     0.0.0.0      1000    50     0       incomplete  Local
valid,best           0
1    172.16.255.117/32  0     0.0.0.0      1000    50     0       incomplete  Local
valid,best           0
1    172.16.255.118/32  0     10.20.25.18  0       -      0       incomplete  2
valid,best,external  0

vEdge# show bgp routes vpn 1 detail
bgp routes-table vpn 1 10.2.2.0/24
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
bgp routes-table vpn 1 10.2.3.0/24
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
bgp routes-table vpn 1 10.20.24.0/24
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
```

```
bgp routes-table vpn 1 56.0.1.0/24
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
bgp routes-table vpn 1 172.16.255.112/32
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
bgp routes-table vpn 1 172.16.255.117/32
 best-path 1
 advertised-peers 0
  peer-addr 10.20.25.18
 info 0
  nexthop       0.0.0.0
  metric        1000
  local-pref    50
  weight        0
  origin        incomplete
  as-path       Local
  ri-peer       0.0.0.0
  ri-routerid   172.16.255.16
  local         true
  sourced       true
  ext-community SoO:0:600
  path-status   valid,best
  tag           0
bgp routes-table vpn 1 172.16.255.118/32
 best-path 1
 info 0
  nexthop     10.20.25.18
  metric      0
  weight      0
  origin      incomplete
  as-path     2
  ri-peer     10.20.25.18
  ri-routerid 172.16.255.18
```

```
path-status valid,best,external
tag         0
```

Related Topics

show bgp neighbor, on page 753
show bgp summary, on page 758

show bgp summary

show bgp summary—Display the status of all BGP connections (on vEdge routers only).

Command Syntax

show bgp summary [**vpn** *vpn-id*]

Syntax Description

None	List status information about all BGP connections.
vpn*vpn-id*	VPN List status information about BGP connections in the specified VPN.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show bgp summary

```
vEdge# show bgp summaryvpn                    1
bgp-router-identifier  172.16.255.16
local-as               1
rib-entries            13
rib-memory             1456
total-peers            1
peer-memory            4816
Local-soo              SoO:0:600
ignore-soo
                       MSG       MSG       OUT                      PREFIX   PREFIX   PREFIX

NEIGHBOR         AS    RCVD      SENT      Q      UPTIME           RCVD    VALID    INSTALLED
  STATE
-------------------------------------------------------------------------------------------------
10.20.25.18      2     3640      3643      0      0:01:00:41       1       1        1
    established
```

Related Topics

show bgp neighbor, on page 753

show bgp routes, on page 755

show boot-partition

show boot-partition—Display the active boot partition and the software version installed in the boot partitions.

Starting in Release 15.4, this command is replaced with the show software command.

Command Syntax

show boot-partition [*partition-number*]

Syntax Description

None	Display information about the boot partitions on the device, including which partition is active and what software version is installed on each partition.
partition-number	Specific Partition Display information for the specific boot partition. *partition-number* can be 1 or 2.

Command History

Release	Modification
14.1.	Command introduced.
15.3.	Command available in this release and earlier.
15.4.	Replaced with **show software command**.

Examples

Show boot-partition

```
vEdge# show boot-partition
PARTITION  ACTIVE  VERSION  TIMESTAMP
------------------------------------------------------------
1          X       14.2.4   2014-11-11T18:16:49+00:00
2          -       14.2.3   2014-11-11T18:35:14+00:00
```

Related Topics

reboot, on page 652
request software activate, on page 701
request software install, on page 702

show bridge interface

show bridge interface—List information about the interfaces on which bridging is configured (on vEdge routers only).

Command Syntax

show bridge interface

show bridge interface *bridge-id* [*interface-name* [(**admin-status** | **encap-type** | **ifindex** | **mtu** | **oper-status** | **rx-octets** | **rx-pkts** | **tx-octets** | **tx-pkts** | **vlan**)]

Syntax Description

None	List information about all interfaces on which bridging ia configured.
bridge-id	Specific Bridging Domain List information about the interface associated with a specific bridging domain.
interface-name(**admin-status** | **encap-type**|**ifindex** | **mtu** | **oper-status** | **rx-octets** |**rx-pkts** |**tx-octets** |**tx-pkts** | **vlan**)	Specific Bridging Domain Property List information about a specific interface or about a property associated with a specific interface. The options correspond to the column headings in the **show bridge interface** command output.

Command History

Release	Modification
15.3.	Command introduced.

Examples

Show bridge interface

```
vEdge# show bridge interface

                         ADMIN   OPER    ENCAP                 RX    RX      TX    TX
BRIDGE  INTERFACE  VLAN  STATUS  STATUS  TYPE   IFINDEX  MTU   PKTS  OCTETS  PKTS  OCTETS
-------------------------------------------------------------------------------------------
1       ge0/2      1     Up      Up      vlan   34       1500  0     0       2     168
1       ge0/5      1     Up      Up      vlan   36       1500  0     0       2     168
1       ge0/6      1     Up      Up      vlan   38       1500  0     0       2     168
2       ge0/2      2     Up      Up      vlan   40       1500  0     0       3     242
2       ge0/5      2     Up      Up      vlan   42       1500  0     0       3     242
```

```
2       ge0/6       2      Up      Up      vlan    44       1500  0     0       3     242
50      ge0/2       -      Up      Up      null    16       1500  0     0       2     140
50      ge0/5       -      Up      Up      null    19       1500  0     0       2     140
50      ge0/6       -      Up      Up      null    20       1500  0     0       2     140
```

Related Topics

bridge, on page 115
clear bridge mac, on page 580
clear bridge statistics, on page 581
show bridge mac, on page 761
show bridge table, on page 762

show bridge mac

show bridge mac—List the MAC addresses that this vEdge router has learned (on vEdge routers only).

Command Syntax

show bridge mac

Syntax Description

None

Command History

Release	Modification
15.3.	Command introduced.

Examples

Show bridge mac

```
vEdge# show bridge mac

                                                    RX    RX      TX    TX
BRIDGE  INTERFACE  MAC ADDR           STATE        PKTS  OCTETS  PKTS  OCTETS
------------------------------------------------------------------------------
1       ge0/5      aa:01:05:05:00:01  dynamic      2     248     0     0
1       ge0/5      aa:01:05:05:00:02  dynamic      2     248     0     0
1       ge0/5      aa:01:05:05:00:03  dynamic      2     248     0     0
1       ge0/5      aa:01:05:05:00:04  dynamic      2     248     0     0
1       ge0/5      aa:01:05:05:00:05  dynamic      2     248     0     0
2       ge0/5      aa:02:05:05:00:01  dynamic      2     248     0     0
2       ge0/5      aa:02:05:05:00:02  dynamic      2     248     0     0
2       ge0/5      aa:02:05:05:00:03  dynamic      2     248     0     0
2       ge0/5      aa:02:05:05:00:04  dynamic      1     124     0     0
2       ge0/5      aa:02:05:05:00:05  dynamic      1     124     0     0
```

Related Topics

bridge, on page 115
clear bridge mac, on page 580
clear bridge statistics, on page 581
show bridge interface, on page 760
show bridge table, on page 762

show bridge table

show bridge table—List the information in the bridge forwarding table (on vEdge routers only).

Command Syntax

show bridge table

Syntax Description

None

Command History

Release	Modification
15.3.	Command introduced.

Examples

Show bridge table

```
vEdge# show bridge table

                     ROUTING               NUM                   RX     RX       TX     TX
FLOOD   FLOOD
BRIDGE   NAME   VLAN   INTERFACE   MAX-MACS   MACS   AGE-TIME(sec)   PKTS   OCTETS   PKTS   OCTETS
PKTS    OCTETS   LEARN   AGE   MOVE
-------------------------------------------------------------------------------------------------------
1               1      irb1        1024       0      300             2      168      0      0
2       168      0       0     0
2               2      irb2        1024       0      300             3      242      0      0
3       242      0       0     0
50              -      irb50       1024       0      300             2      140      0      0
2       140      0       0     0
```

Related Topics

bridge, on page 115
clear bridge mac, on page 580
clear bridge statistics, on page 581
show bridge interface, on page 760
show bridge mac, on page 761

show cellular modem

show cellular modem—Display cellular modem information and status (on vEdge routers only).

Command Syntax

show cellular modem

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.

Examples

Show cellular modem

```
vEdge# show cellular modem
Modem model number      : MC7354
Firmware version        : SWI9X15C_05.05.58.01
Firmware date           : 2015/03/05 00:02:40
Package                 : 05.05.58.01_ABC_005.029_000
Hardware version        : 1.0
Modem status            : Online
Modem temperature       : 46 deg C
International mobile subscriber identity (IMSI)  : 001010123456799
International mobile equipment identity (IMEI)   : 111115050450742
Integrated circuit card ID (ICCID)               : 89860600502000180724
Mobile subscriber ISDN (MSISDN)                  : 6508338332
Electronic serial number (ESN)                   : 809D9CD1
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 405
show cellular network, on page 764
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

show cellular network

show cellular network—Display cellular network information (on vEdge routers only).

Command Syntax

show cellular network

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.
16.2.	Added support for 2G and 3G technologies.

Examples

For CDMA networks:

Show cellular network

```
vEdge# show cellular network

Registration status                Registered
Roaming status                     @Home
Packet-switched domain state       Attached
System ID, SID                     32766
Network ID, NID                    616
Base station ID, BID               882
```

For GSM networks:

```
vEdge# show cellular network

Registration status                Registered
Roaming status                     @Home
Packet-switched domain state       Attached
Mobile country code, MCC           311
Mobile network code, MNC           480
Network name                       CompanyX
Cell ID                            84759830
Location area code, LAC            56997
```

For HDR networks:

```
vEdge# show cellular network
```

```
Registration status                 Registered
Roaming status                      @Home
Packet-switched domain state        Attached
```

For LTE networks:

```
vEdge# show cellular network

Registration status                   Registered
Roaming status                        @Home
Packet-switched domain state          Attached
Mobile country code, MCC              311
Mobile network code, MNC              480
Network name                          CompanyX
EPS Mobility Management (EMM) state   Registered
   EMM substate                       Normal Service
   EMM connection state               RRC Idle
Cell ID                               84759830
Tracking area code, TAC               7936
```

For WCDMA networks:

```
vEdge# show cellular network

Registration status                 Registered
Roaming status                      @Home
Packet-switched domain state        Attached
Mobile country code, MCC            311
Mobile network code, MNC            480
Network name                        CompanyX
Cell ID                             84759830
Location area code, LAC             56997
Primary scrambling code, PSC        169
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 405
show cellular modem, on page 763
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

show cellular profiles

show cellular profiles—Display cellular profile information (on vEdge routers only).

Command Syntax

show cellular profiles

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.

Examples

Show cellular profiles

```
vEdge# show cellular profiles
           PROFILE  PDN                                                  PRIMARY  SECONDARY
  USER
INTERFACE  ID       TYPE   APN                NAME        AUTH  IP ADDR  DNS      DNS
   NAME
-------------------------------------------------------------------------------------------------
cellular0  1        IPv46  ims                profile_1   None  0.0.0.0  0.0.0.0  0.0.0.0
   -
cellular0  2        IPv4   admin              profile_2   None  0.0.0.0  0.0.0.0  0.0.0.0
   -
cellular0  3        IPv4   internet           profile_3   None  0.0.0.0  0.0.0.0  0.0.0.0
   -
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 405
show cellular modem, on page 763
show cellular network, on page 764
show cellular radio, on page 766
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

show cellular radio

show cellular radio—Display cellular radio band information (on vEdge routers only).

Command Syntax

show cellular radio

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.

Examples

```
vEdge# show cellular radio

Radio mode                                    LTE
Frequency band                                2
Bandwidth                                     20 MHz
Transmit channel                              18800
Receive channel                               800
Received signal strength indicator (RSSI)     -63 dBm
Reference signal receive power (RSRP)         -89 dBm, Excellent
Reference signal receive quality (RSRQ)       -8 dB, Excellent
Signal-to-noise ratio (SNR)                   14.8 dB, Poor
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 405
show cellular modem, on page 763
show cellular network, on page 764
show cellular profiles, on page 765
show cellular sessions, on page 767
show cellular status, on page 768
show interface, on page 827

show cellular sessions

show cellular sessions—Display cellular session information (on vEdge routers only).

Command Syntax

show cellular session

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.

Examples

Show cellular sessions

```
vEdge# show cellular sessions

Data bearer                : LTE
Dormancy state             : Active
Active profile             : 3

IPv4                       :
   Assigned address        : 100.82.104.116/29
   Gateway                 : 100.82.104.117
   Primary DNS server      : 198.224.173.135
   Secondary DNS server    : 198.224.174.135

Rx packets: 82625599, drops: 0, errors: 0, overflows: 0
Tx packets: 83601165, drops: 0, errors: 0, overflows: 0

Rx octets: 24259339642, TX octets: 24233263286
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 403
show cellular modem, on page 763
show cellular network, on page 764
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular status, on page 768
show interface, on page 827

show cellular status

show cellular status—Display cellular status information (on vEdge routers only).

Command Syntax

show cellular status

Syntax Description

None

Command History

Release	Modification
16.1.	Command introduced.

Examples

Show cellular status

```
vEdge# show cellular status

                          SIM      RADIO  SIGNAL
INTERFACE  MODEM STATUS   STATUS   MODE   STRENGTH   NETWORK STATUS  LAST SEEN ERROR
-------------------------------------------------------------------------------------
cellular0  Online         Ready    LTE    Excellent  Registered      None
```

Related Topics

cellular, on page 119
clear cellular errors, on page 581
clear cellular session statistics, on page 582
profile, on page 405
show cellular modem, on page 763
show cellular network, on page 764
show cellular profiles, on page 765
show cellular radio, on page 766
show cellular sessions, on page 767
show interface, on page 827

show certificate installed

show certificate installed—Display the decoded certificate signing request installed on a vBond orchestrator, vManage NMS or vSmart controller. This is the CSR that has been signed by the root CA. Information displayed includes the serial number, the signature algorithm, the issuer, the certificate validity, the public key algorithm and public key, and the signature algorithm.

On a vEdge router, display the board ID certificate.

Command Syntax

show certificate installed

Syntax Description

None

Command History

Release	Modification
14.2.	Command introduced.
15.3.5.	Added command support on vEdge routers.

Examples

Show certificate installed

```
vSmart# show certificate installed
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 305419779 (0x12345603)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, OU=vIPtela Test, O=Viptela
Inc/emailAddress=us@viptela.com
        Validity
            Not Before: Jul 31 15:44:56 2014 GMT
            Not After : Jul 31 15:44:56 2015 GMT
        Subject: L=San Jose, C=US, ST=California, O=vIPtela Inc, OU=Viptela Inc,
CN=VSmart_47af63a3-788a-4c84-b5a7-fbb74eca57db.viptela.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a1:9d:a7:5c:ed:7f:56:e7:ce:32:82:ea:e9:9f:
                    71:d8:14:79:c7:80:0c:22:c4:a4:25:98:6a:0e:49:
                    4a:79:7f:60:a2:73:e7:89:c4:db:73:87:97:6a:9c:
                    42:e8:39:46:1d:9b:00:4b:fb:c0:3c:dc:20:97:d3:
                    8c:1b:d1:7a:03:43:73:65:38:fa:5a:31:2b:4e:d2:
                    e2:0e:16:ae:05:1a:33:b6:fd:58:5f:c9:86:e3:83:
                    b3:07:16:30:34:e9:dc:8a:fe:a7:d8:b6:ee:d7:59:
                    24:1e:9f:30:b8:bb:99:da:b6:56:94:7f:61:f3:5d:
                    9a:3f:39:4d:6f:24:1e:84:db:39:6a:ca:23:94:f3:
                    14:61:7b:d8:d1:45:52:65:e9:17:71:3d:91:a3:1c:
                    45:ba:1a:28:48:ca:17:63:4d:dc:ff:13:8e:84:65:
                    94:8a:3c:44:49:f2:2f:e9:ec:70:e6:cc:f5:23:a7:
                    f4:5d:2f:0d:6a:ec:ce:19:90:af:df:ad:90:76:fa:
                    1b:86:12:51:d1:9f:6a:86:4b:ab:62:d8:5a:cb:35:
                    74:f1:36:09:b8:8c:78:be:1d:eb:9b:b3:5a:79:c6:
                    80:ad:57:55:a9:36:bf:9c:9d:fb:e5:f7:bd:a5:10:
                    e3:4f:b0:d4:7a:a0:e4:59:47:a4:82:c5:eb:d1:71:
                    48:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:VSmart_05_02_2014_22_33_15_077740428.viptela.com
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.54
                  CPS: https://www.verisign.com/cps
```

```
            X509v3 Authority Key Identifier:
                keyid:0D:44:5C:16:53:44:C1:82:7E:1D:20:AB:25:F4:01:63:D8:BE:79:A5

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://SVRSecure-G3-crl.verisign.com/SVRSecureG3.crl

            Authority Information Access:
                OCSP - URI:http://ocsp.verisign.com
                CA Issuers - URI:http://SVRSecure-G3-aia.verisign.com/SVRSecureG3.cer

    Signature Algorithm: sha1WithRSAEncryption
         67:e5:65:5e:75:de:2f:68:9c:37:96:79:dc:91:9d:a9:ef:99:
         93:5e:9a:33:5a:79:cb:b6:84:fe:0b:83:ad:12:a3:04:fb:b7:
         ee:fd:52:9d:68:cc:1c:15:3a:f7:93:8d:cb:ea:a5:ab:4e:86:
         bd:c5:17:df:6f:0b:3c:35:d3:a2:da:c4:1a:9d:d4:34:79:28:
         c2:20:06:ea:6c:99:45:71:cc:85:0a:a2:7f:80:48:2c:25:22:
         e1:da:16:f6:7a:9a:1b:17:84:27:a1:52:ab:84:5c:2d:b0:6f:
         f7:c5:ff:73:6a:f0:19:6e:e5:83:98:59:d3:03:7e:24:f8:bf:
         c6:47:66:6e:80:fd:d6:ee:56:1d:9b:c0:00:f2:38:e5:7d:49:
         19:37:6b:32:79:83:49:b2:d9:06:0f:ba:26:04:d1:8b:ee:dd:
         1a:81:26:1a:c8:a3:77:59:76:06:76:42:76:4e:57:22:97:c8:
         c1:2a:95:f8:8a:f7:10:e7:43:08:d9:61:96:00:6e:55:7f:89:
         6b:c4:03:c9:7d:03:f1:46:23:a0:ff:98:79:84:f8:96:8a:6a:
         56:4d:85:20:ae:89:07:08:33:31:04:c2:9a:c3:29:38:5f:09:
         ed:a2:1a:e2:d0:9b:af:8e:0d:d5:89:b5:43:c2:02:e1:cc:82:
         db:70:f0:4c
```

Related Topics

clear installed-certificates, on page 593
show certificate root-ca-cert, on page 772
show certificate serial, on page 775
show certificate signing-request, on page 776
show certificate validity, on page 777

show certificate reverse-proxy

show certificate reverse-proxy—Display the installed proxy certificate (on vEdge routers only).

Command Syntax

show certificate reverse-proxy

Syntax Description

None

Command History

Release	Modification
18.2.	Command introduced.

Examples

Show certificate reverse-proxy

Examples

```
vEdge# show certificate reverse-proxy  Reverse proxy
certificate-------------------------Certificate:    Data:        Version: 1 (0x0)
Serial Number: 1 (0x1)    Signature Algorithm: sha256WithRSAEncryption       Issuer: C=US,
 ST=California, O=Viptela, OU=ViptelaVmanage, CN=813fd02c-acca-4c19-857b-119da60f257f
   Validity            Not Before: Jan 29 20:11:09 2018 GMT            Not After : Jan 23
20:11:09 2048 GMT        Subject: C=US, ST=California,
CN=e4f6f85a-f0ef-4923-a239-6d08a58fa7a3, O=ViptelaClient        Subject Public Key Info:
          Public Key Algorithm: rsaEncryption                Public-Key: (2048 bit)
         Modulus:                    00:cb:33:1a:fd:25:5f:e5:77:f3:18:fb:6c:70:25:
            47:0d:41:5b:95:8a:5f:48:b7:98:9f:ad:22:09:93:
b6:ca:f0:8e:5e:2e:04:9d:33:3e:b9:07:36:b3:99:
16:20:7c:81:48:1a:b3:1d:36:89:15:d0:24:e6:43:
8a:eb:d4:a9:44:b0:17:b3:23:10:c7:e7:19:84:ee:
4b:42:d9:14:43:75:dd:b6:59:01:6f:15:bb:4d:fe:
39:bd:41:30:bd:cb:02:e7:4a:29:c2:f9:8f:95:c9:
59:bc:24:55:33:29:da:42:1f:d0:27:25:1c:b9:b0:
35:f6:54:55:d6:e4:3c:30:a4:f9:aa:18:52:34:ee:
8f:19:ba:fa:62:4f:ee:db:ce:c4:c6:56:12:70:de:
94:1b:3d:35:c0:fb:38:55:dd:7e:1e:bd:00:ff:55:
f1:7a:bf:3d:e1:24:2b:e1:7a:d8:e1:b3:9c:46:bd:
0a:67:0a:12:10:1b:ef:09:71:91:95:7d:8a:26:c8:
d3:c4:d7:ed:27:ea:08:29:7c:f3:77:93:ab:78:df:
4c:0a:8d:2c:1e:31:17:76:6e:1f:e9:27:78:ed:cf:
d9:5b:8a:dd:59:67:a2:63:37:dc:86:e0:0f:03:44:
16:0b:fa:fa:3c:4a:11:30:3f:1c:80:8f:b9:73:a9:                    f0:91
Exponent: 65537 (0x10001)    Signature Algorithm: sha256WithRSAEncryption
58:81:4d:02:ef:a6:a5:78:ee:02:bc:58:2e:b2:6d:cc:55:34:
02:fe:10:38:dc:67:d9:71:96:9d:01:af:f6:0c:0f:61:e6:12:
92:ee:6b:1f:cf:72:1c:ab:b8:a5:98:d8:22:05:17:6f:6e:e0:
4c:65:d3:05:60:20:b9:ab:6d:66:bf:ca:39:45:4e:8b:ef:02:
37:ff:25:22:9d:eb:95:b4:4e:72:5b:42:c5:c7:61:8e:14:5c:
92:dc:d8:90:aa:d4:29:8b:f8:9e:e8:8b:48:c1:0e:80:f7:e4:
2c:e3:9a:ba:62:63:ab:df:ca:f3:5e:06:2f:1b:69:e6:d4:da:
f8:dc:44:99:a6:45:33:a5:3e:4a:af:6f:f7:bb:ff:fd:66:bd:
71:32:89:45:5e:42:c8:66:07:3e:f4:17:65:fb:f4:e8:5b:7f:
dc:4f:34:da:a3:cf:15:6e:00:4a:69:a3:c3:9a:55:7c:8e:e5:
d7:ae:86:d2:40:a5:c1:f6:82:e8:ef:a2:8c:c5:db:50:cf:cb:
d8:ee:2b:82:9e:da:17:12:16:ae:61:8e:32:17:e4:dd:29:60:
95:50:c8:bd:b8:ab:93:72:ff:13:58:85:85:c2:70:29:71:8f:
5d:8e:ae:ce:48:34:14:3f:24:d1:6e:51:c9:75:7d:78:fd:f6:         77:2f:38:36
```

Related Topics

show certificate reverse-proxy, on page 771
show control connections, on page 788

show certificate root-ca-cert

show certificate root-ca-cert—Display the root certificate installed on a Cisco vEdge device. Information displayed includes the serial number, the signature algorithm, the issuer, the certificate validity, the public key algorithm and public key, and the signature algorithm.

Command Syntax

show certificate root-ca-cert

Syntax Description

None

Command History

Release	Modification
14.2.	Command introduced.

Examples

Show certificate root-ca-cert

```
vSmart# show certificate root-ca-cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16071262098767155600 (0xdf0897bac9371190)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, OU=Viptela Inc, O=Viptela
Inc/emailAddress=us@viptela.com
        Validity
            Not Before: Jul 31 15:44:06 2014 GMT
            Not After : Jul 28 15:44:06 2024 GMT
        Subject: C=US, ST=California, L=San Jose, OU=Viptela Inc, O=Viptela
Inc/emailAddress=us@viptela.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b9:20:3e:f3:65:e7:18:42:cd:09:f9:6c:9b:3d:
                    0d:a8:8e:e0:44:f7:3f:9b:05:86:df:3b:cf:ab:2b:
                    a4:a6:24:c6:8a:b4:f7:af:21:b3:db:8f:38:03:6a:
                    da:63:f3:15:c5:68:af:9b:96:85:e7:80:3a:1a:7e:
                    04:50:77:91:fa:64:a7:93:c5:90:4f:9a:7e:84:d4:
                    e1:2a:02:af:0d:15:7f:10:14:28:6a:ff:0c:7b:f1:
                    48:4f:ca:2d:c1:6a:3b:f0:89:57:d9:9c:bf:8c:36:
                    ef:0f:ae:69:6a:e5:55:a9:58:c9:de:2b:a1:12:fe:
                    a9:df:9e:61:c5:31:ce:a7:f9:49:37:b6:be:5c:37:
                    aa:e5:98:1c:cf:7b:b1:c3:cc:20:69:90:b3:02:dc:
                    d1:4d:8c:00:26:e7:49:a7:3b:e4:73:3d:78:96:f4:
                    c5:be:47:17:d3:57:de:b3:c5:70:ab:fd:20:1e:51:
                    c7:95:31:0b:1d:50:53:06:6c:28:0d:25:b5:62:e2:
                    c8:fe:bc:ea:8f:71:8f:4a:ea:d1:d0:56:ef:a0:3a:
                    1f:55:a7:c6:88:03:68:41:cd:fe:60:50:77:8c:5c:
                    35:4e:90:9d:db:b4:8d:73:b6:a0:f0:b0:29:03:f3:
                    eb:b1:cc:d8:bd:ed:ee:68:cb:77:8d:ef:2c:21:21:
                    94:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Key Identifier:
                91:04:EB:99:69:73:EB:4F:6C:E1:F2:B4:7F:D4:21:E4:D4:54:56:ED
            X509v3 Authority Key Identifier:
```

```
                keyid:91:04:EB:99:69:73:EB:4F:6C:E1:F2:B4:7F:D4:21:E4:D4:54:56:ED
                DirName:/C=US/ST=California/L=San Jose/OU=Viptela Inc/O=Viptela
Inc/emailAddress=us@viptela.com
                serial:DF:08:97:BA:C9:37:11:90

    Signature Algorithm: sha1WithRSAEncryption
         71:a3:64:ee:8a:36:fa:05:60:bb:dd:38:30:c7:39:78:aa:1d:
         4f:14:f6:7c:06:13:41:6f:3a:07:89:be:65:63:fc:08:c6:1f:
         49:99:2b:a7:33:65:83:67:22:e4:d6:e4:78:bd:19:d8:95:33:
         60:61:ac:29:b6:7e:35:9b:e6:f2:d8:57:7f:20:06:df:51:a5:
         dc:d4:83:d6:8d:1b:13:d4:c6:fe:dc:4a:1b:14:25:f4:32:3e:
         7a:d3:e9:f7:3d:fd:8f:47:9c:25:c7:4a:0c:50:99:28:24:90:
         d6:6a:27:eb:a2:28:4d:55:74:98:9c:a8:d6:6d:c6:be:2b:43:
         6e:18:22:64:94:4b:f2:21:fa:d4:fc:33:da:ce:ea:0a:f5:c4:
         24:c2:51:fb:6b:84:76:f3:d7:ac:55:df:ca:7c:88:73:89:0d:
         7e:12:55:5e:e2:0e:5e:28:27:45:66:a4:36:02:09:c0:d0:ae:
         41:5d:54:22:9b:29:f1:84:3e:67:a1:aa:3f:32:83:27:0a:75:
         2b:16:ed:b3:91:aa:e5:24:8f:45:4f:14:7b:0e:f7:05:ef:2e:
         d5:03:29:e7:18:81:a6:7c:c9:1e:38:b1:7a:00:c8:34:e0:ab:
         b7:8d:3a:36:d5:70:11:e2:d1:43:1c:8c:da:32:b8:29:08:31:
         e8:b2:e0:b2
```

Related Topics

show certificate installed, on page 769
show certificate serial, on page 775
show certificate validity, on page 777

show certificate root-ca-crl

To display the decoded CRL of the installed root certificate authority, use the **show certificate root-ca-crl** command in privileged EXEC mode.

show certificate root-ca-crl

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco SD-WAN Release 20.7.1	This command was introduced.

Examples

The following is sample output from the **show certificate root-ca-crl** command showing the decoded CRL of the installed root certificate authority

```
vEdge # show certificate root-ca-crl
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, OU=CA, O=Company
LLC/emailAddress=support@ca.com, CN=CA CA
        Last Update: Sep 24 21:06:00 2021 GMT
        Next Update: Oct 24 21:06:00 2021 GMT
        CRL extensions:
            X509v3 CRL Number:
                3
Revoked Certificates:
```

```
Serial Number: 1234
    Revocation Date: Sep 24 15:40:33 2021 GMT
Serial Number: 1235
    Revocation Date: Sep 24 20:34:48 2021 GMT
Serial Number: 1236
    Revocation Date: Sep 24 21:06:00 2021 GMT
Signature Algorithm: sha256WithRSAEncryption
     a3:2d:7a:3c:7f:57:15:6d:9d:29:16:14:56:6e:3a:75:e8:d5:
     1f:3c:dd:a5:1e:25:44:0c:2a:3d:5d:e9:a0:89:ca:b9:e3:11:
     92:79:aa:35:2a:2d:f2:b8:00:0d:65:6e:d7:bf:89:bf:cf:26:
    14:3c:e3:00:f2:f0:e3:db:38:a9:28:5b:c5:0e:f9:2f:ce:ec:
     3f:49:7d:00:6c:df:08:de:c9:ed:8e:d7:ae:09:c9:c1:f2:f1:
     02:fb:6c:b2:cc:c9:f6:71:3d:fa:8e:6f:e3:f2:62:62:ee:53:
     02:3c:61:6d:7b:df:58:f0:4f:f8:53:5e:6f:ab:02:d4:c4:29:
```

show certificate serial

show certificate serial—Display the serial number for a vBond orchestrator or a vSmart controller. Display the serial number and chassis number for a vEdge router.

Command Syntax

show certificate serial

Syntax Description

None

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show certificate serial

```
vEdge# show certificate serial
Chassis num =  11O2136130018   Board_id_serial_num : 10000161
```

Related Topics

request vsmart-upload serial-file, on page 715
show certificate installed, on page 769
show certificate root-ca-cert, on page 772
show certificate signing-request, on page 776
show certificate validity, on page 777

show certificate signing-request

show certificate signing-request—Display the certificate signing requests installed on a vBond orchestrator, vManage NMS, or vSmart controller. This CSR is the one that has been signed by the device's private key.

Command Syntax

show certificate signing-request [**decoded**]

Syntax Description

None	Display the certificate signing request hash.
decoded	Decoded Certificate Signing Request Display the decrypted hashed certificate signing request.

Command History

Release	Modification
14.2.	Command introduced.

Examples

```
vSmart# show certificate signing-request
-----BEGIN CERTIFICATE REQUEST-----
MIIDUzCCAjsCAQAwgdIxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEfMB0GA1UECxMWdklQdGVsYSBJbmMgUmVncmVz
c2lvbjEUMBIGA1UEChMLdklQdGVsYSBJbmMxQDA+BgNVBAMUN1ZTbWFydF80N2Fm
NjNhMy03ODhhLTRjODQtYjVhNy1mYmI3NGVjYTU3ZGIudmlwdGVsYS5jb20xIjAg
BgkqhkiG9w0BCQEWE3N1cHBvcnRAdmlwdGVsYS5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQChnadc7X9W584ygurpn3HYFHnHgAwixKQlmGoOSUp5
f2Cic+eJxNtzh5dqnELoOUYdmwBL+8A83CCX04wb0XoDQ3NlOPpaMStO0uIOFq4F
GjO2/VhfyYbjg7MHFjA06dyK/qfYtu7XWSQenzC4u5natlaUf2HzXZo/OU1vJB6E
2zlqyiOU8xRhe9jRRVJl6RdxPZGjHEW6GihIyhdjTdz/E46EZZSKPERJ8i/p7HDm
zPUjp/RdLw1q7M4ZkK/frZB2+huGElHRn2qGS6ti2FrLNXTxNgm4jHi+Heubs1p5
xoCtV1WpNr+cnfvl972lEONPsNR6oORZR6SCxevRcUgTAgMBAAGgOzA5BgkqhkiG
9w0BCQ4xLDAqMAkGA1UdEwQCMAAwHQYDVR0OBBYEFBKI38vS/QQkgzzLzxAgyd2P
BVGkMA0GCSqGSIb3DQEBBQUAA4IBAQBbot83yN3VE2XpHqOKnxU6vce0expT4dOn
Idl4L0ftZ39FoubcHKw6cwPjEj9GVV4xBnEsdkYGguiaT/fmpsYMNnEIyeb4pGyy
yuw3L4JpmXPcisY/EDq9VV2nMWTXPTYxNuu2kc/q20kFMyfZcALsZiBt4YEegKHG
3d3KCxwLBmMTLkfK/wFeYXnWYu648aVCWoCywUQNqMQwKzXcznGw86ahMhQl80Ij
ARv0+DmLTWVjSLU1VZSZBQS57M9FeycRm/qfeJVqYj3UXVwSKkAZA2WGg4k88+ty
fsfUQzxBI03GRYlqVJqMsI017S89COXZPnoVCaC05RCqV+jcTZCd
-----END CERTIFICATE REQUEST-----
```

```
vSmart# show certificate signing-request decoded
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=California, L=San Jose, OU=vIPtela Inc Regression, O=Viptela,
Inc., CN=VSmart_7336ac9b-88b5-4124-bc53-3cf0916119ea.viptela.com/emailAddress=us@viptela.com

        Subject Public Key Info:
```

```
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bf:65:1c:cb:e4:d5:4d:72:b8:6c:ec:36:5b:7f:
                    ed:4c:24:a8:85:e8:3a:53:04:b0:69:65:05:6e:8c:
                    bc:0f:42:5c:9b:c4:95:ab:8d:30:09:da:84:49:4b:
                    bb:57:f0:5a:f1:58:d1:09:61:91:3b:92:0f:f2:ba:
                    ca:2a:ab:0a:59:f1:c6:15:2c:92:8c:d8:7b:bd:7d:
                    94:c7:e8:a3:3d:e0:f6:1b:f1:ca:fd:be:a8:ff:d3:
                    3d:5d:60:06:df:a4:aa:3d:b7:c2:e2:20:9d:e0:a1:
                    02:0c:74:c4:8c:9b:b9:1e:3f:18:96:8b:1e:b5:40:
                    6f:cc:16:2c:28:51:7b:fa:62:13:d1:17:34:fd:6c:
                    f9:30:85:cd:dd:17:ae:78:d7:bd:ec:9c:2d:73:b5:
                    c9:04:c7:ca:dc:33:c0:bb:74:6f:45:a4:9c:05:36:
                    1b:de:6d:c9:9a:23:31:84:40:3c:61:3d:ce:ae:17:
                    1f:4f:06:10:50:c8:b0:f8:67:2a:b8:c1:32:c9:c0:
                    af:cc:b0:2e:43:46:f2:11:0b:42:cd:5c:a1:ae:3a:
                    cf:ba:e6:c9:09:15:32:46:d1:69:8e:8c:3f:fd:f7:
                    f2:12:3c:42:00:4e:48:61:39:24:2f:b5:10:14:08:
                    3d:bc:83:87:ea:7d:81:c8:cb:28:07:02:1c:3d:c8:
                    6f:49
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                F1:9E:E9:7C:5A:74:8C:C9:C5:8F:41:D1:9F:BB:4C:7D:8C:4C:C1:12
    Signature Algorithm: sha1WithRSAEncryption
         0b:45:35:41:32:0a:7e:fc:d7:b4:42:dd:11:56:7c:65:03:cb:
         74:41:3c:ac:95:4d:98:9f:28:b7:ac:8d:fd:71:a0:d2:f5:8d:
         d9:d9:34:33:de:74:17:7e:61:00:4f:92:82:06:b1:b1:06:6e:
         6d:43:7e:6c:b0:43:ed:9d:65:cc:ca:24:30:7b:bc:51:36:c4:
         aa:cd:fa:42:75:96:df:6a:74:07:42:d5:e1:d7:99:50:70:b5:
         d5:ff:7d:c5:fd:14:48:f7:a3:c3:f6:80:9e:7c:47:50:2b:fe:
         87:dd:78:fd:19:57:d3:5e:d3:0e:45:5e:30:36:56:69:c3:5d:
         80:b6:3d:ff:3a:35:e0:ad:f4:1d:8e:cf:ea:c6:f9:cf:ce:01:
         15:76:c3:ce:5b:f7:86:2f:57:18:0a:11:81:a4:e3:bf:db:b9:
         dd:9d:51:1b:f9:94:b5:0d:3c:28:c2:f3:54:c8:15:05:83:47:
         37:53:ed:a7:14:70:7b:84:5d:fb:80:70:dd:c4:b4:fe:88:f4:
         7d:43:d2:65:70:85:73:50:20:6c:7f:3a:fc:c2:a4:0a:eb:3d:
         79:e9:99:05:b5:45:2e:cb:e3:9c:ab:e8:22:79:7e:89:03:90:
         5e:da:13:3e:1e:18:45:1f:9d:ca:2b:33:7d:73:85:09:a8:2a:
         ad:66:a7:b7
```

Related Topics

show certificate installed, on page 769
show certificate root-ca-cert, on page 772
show certificate serial, on page 775
show certificate validity, on page 777

show certificate validity

show certificate validity—Display how long a certificate is valid for (on vSmart controllers and vBond orchestrators only).

Command Syntax

show certificate validity

Syntax Description

None

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show certificate validity

```
vSmart# show certificate validity
The certificate is valid from  Apr 20 21:03:38 2015 GMT  (Current date is  Mon Apr 20
23:00:19 GMT 2015 )
& valid until  Apr 19 21:03:38 2016 GMT
```

Related Topics

request certificate, on page 658
show certificate installed, on page 769
show certificate root-ca-cert, on page 772
show certificate serial, on page 775
show certificate signing-request, on page 776

show cli

show cli—Display the CLI settings.

Command Syntax

show cli

Syntax Description

None

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show cli

```
vEdge# show cli
autowizard             false
complete-on-space      false
history                100
idle-timeout           1800
ignore-leading-space   true
output-file            terminal
paginate               true
prompt1                \h\M#
prompt2                \h(\m)#
screen-length          43
screen-width           85
service prompt config true
show-defaults          false
terminal               xterm-256color
timestamp              disable
```

Related Topics

complete-on-space, on page 623
history, on page 639
idle-timeout, on page 639
paginate, on page 645
prompt1, on page 649
prompt2, on page 651
screen-length, on page 716
screen-width, on page 716
timestamp, on page 1048

show clock

show clock—Display the system time.

Command Syntax

show clock

Syntax Description

None	Display time in the local timezone.
	universal Display time in UTC.

Command History

Release	Modification
14.1.	Command introduced.
14.2.	Introduced **universal** option.

Examples

Show clock

```
vEdge# show clock
Mon Jul  7 13:36:00 PDT 2014
vEdge# show clock universal
Mon Jul  7 20:36:05 UTC 2014
```

Related Topics

show uptime, on page 1035
timestamp, on page 1048

show cloudexpress applications

show cloudexpress applications—Display the best path for applications configured with Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only). The best path could be a local interface with Direct Internet Access (DIA), or the path to a remote gateway.

Command Syntax

show cloudexpress applications *vpn-id*

Syntax Description

None	Display the best interface for all applications in all VPNs configured with Cloud OnRamp for SaaS.
vpn-id	Specific VPN Display the best interface for all applications in VPN x configured with Cloud OnRamp for SaaS.

Command History

Release	Modification
16.3.	Command introduced.

Examples

Show cloudexpress applications

```
vEdge# show cloudexpress applications

                                EXIT     GATEWAY
LOCAL  REMOTE
VPN  APPLICATION                TYPE     SYSTEM IP      INTERFACE  LATENCY  LOSS
COLOR  COLOR
-------------------------------------------------------------------------------------
1    salesforce                 gateway  172.16.255.14  -          103      1
lte    lte
1    google_apps                gateway  172.16.255.14  -          47       0
lte    lte
```

Related Topics

clear cloudexpress computations, on page 583
show cloudexpress gateway-exits, on page 781
show cloudexpress local-exits, on page 782
show omp cloudexpress, on page 906

show cloudexpress gateway-exits

show cloudexpress gateway-exits—Display loss and latency on each gateway exit for applications configured with Cloud OnRamp for SaaS (formerly called CloudExpress service) (on vEdge routers only).

Command Syntax

show cloudexpress gateway-exits *vpn-id*

Syntax Description

None	Display loss and latency on each gateway exit for all applications in all VPNs configured with Cloud OnRamp for SaaS.
vpn-id	Specific VPN Display loss and latency on each gateway exit for all applications in VPN x configured with Cloud OnRamp for SaaS.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show cloudexpress gateway-exits

                                                                                LOCAL   REMOTE
VPN  APPLICATION              GATEWAY IP                LATENCY  LOSS  COLOR   COLOR
-------------------------------------------------------------------------------------------
1    salesforce               172.16.255.14             72       2     lte     lte
1    google_apps              172.16.255.14             16       0     lte     lte
```

Related Topics

clear cloudexpress computations, on page 583
show cloudexpress applications, on page 780
show cloudexpress local-exits, on page 782
show omp cloudexpress, on page 906

show cloudexpress local-exits

show 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) (on vEdge routers only).

Command Syntax

show cloudexpress local-exits *vpn-id*

Syntax Description

None	Display application loss and latency for all applications on all DIA interfaces in all VPNs enabled for Cloud OnRamp for SaaS.
vpn-id	Specific VPN Display application loss and latency for all applications on all DIA interfaces in a specific VPN enabled for Cloud OnRamp for SaaS.

Command History

Release	Modification
16.3	Command introduced.

Examples

Show cloudexpress local-exits

```
vEdge# show cloudexpress local-exits

VPN  APPLICATION              INTERFACE                 LATENCY  LOSS
-----------------------------------------------------------------------
```

```
100  salesforce              ge0/0                    89       7
100  salesforce              ge0/2                    80       5
100  office365               ge0/0                    62       3
100  office365               ge0/2                    74       1
100  amazon_aws              ge0/0                    98       6
100  amazon_aws              ge0/2                    107      6
100  oracle                  ge0/0                    75       3
100  oracle                  ge0/2                    81       5
100  sap                     ge0/0                    54       3
100  sap                     ge0/2                    60       4
100  box_net                 ge0/0                    28       2
100  box_net                 ge0/2                    18       3
100  dropbox                 ge0/0                    19       1
100  dropbox                 ge0/2                    31       1
100  jira                    ge0/0                    92       6
100  jira                    ge0/2                    102      3
100  intuit                  ge0/0                    44       2
100  intuit                  ge0/2                    37       8
100  concur                  ge0/0                    76       5
100  concur                  ge0/2                    71       3
100  zoho_crm                ge0/0                    25       1
100  zoho_crm                ge0/2                    20       1
100  zendesk                 ge0/0                    7        1
100  zendesk                 ge0/2                    15       0
100  gotomeeting             ge0/0                    31       2
100  gotomeeting             ge0/2                    21       2
100  webex                   ge0/0                    66       2
100  webex                   ge0/2                    62       3
100  google_apps             ge0/0                    31       0
100  google_apps             ge0/2                    31       1
```

Related Topics

show cloudexpress local-exits, on page 782

show configuration commit list

show configuration commit list—Display a list of all configuration commits on the Cisco vEdge device.

Command Syntax

show configuration commit list [*number*]

Syntax Description

None	List information about all the configuration commits.
number	Specific Number of Commits List information about the specified number of configuration commits.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show configuration commit list

```
vEdge# show configuration commit list
2013-12-06 18:39:20
SNo. ID       User       Client      Time Stamp          Label       Comment
~~~~ ~~       ~~~~       ~~~~~~      ~~~~~~~~~~          ~~~~~       ~~~~~~~
0    10008    admin      cli         2013-12-06 18:39:09             add banner text
1    10007    admin      cli         2013-12-06 18:03:08
2    10006    admin      cli         2013-12-06 18:02:14
3    10005    admin      cli         2013-12-06 17:24:08
4    10004    admin      cli         2013-12-06 10:57:26
5    10003    admin      cli         2013-12-06 10:32:25
6    10002    admin      cli         2013-12-06 10:29:07
7    10001    admin      cli         2013-12-06 10:28:53
8    10000    admin      cli         2013-12-06 10:28:53 Software Release Information
```

Related Topics

commit, on page 622

show container images

show container images—List the Cisco SD-WAN software images associated with the vSmart controller containers (on vContainer hosts only).

Command Syntax

show container images [**instances** *instance-name*]

Syntax Description

None	List information about the software images for all containers.
instances *instance-name*	Specific Container Instance List information about the software images for the specified instance.

Command History

Release	Modification
16.2.	Command introduced.

Examples

Show container images

```
vContainer# show container images

VERSION         INSTANCE
--------------------------------
```

```
99.99.999-2440  first_vsmart
                second_vsmart
99.99.999-2444  vm10
```

Related Topics

container, on page 145
show container instances, on page 785

show container instances

show container instances—List information about the vSmart controller containers running on the container host (on vContainer hosts only).

Command Syntax

show container instances [*instance-parameter*]

Syntax Description

None	List information about all the vSmart controller containers running on the container host
instance-parameter	Specific Instance Parameter List information about a specific parameter for a container instance.*instance-parameter* can be one of the following, which correspond to the column headers in the command output: • **admin-state**(**down**|**up**) • **image***image-name* • **interface**(**host-ip-address***ip-address*|**ip-address***ip-address*) • **oper-state**(**down** |**up**) • **personality**device-type

Release	Modification
16.2.	Command introduced.

Examples

Show container instances

```
vContainer# show container instances

                ADMIN  OPER                                IF                HOST IP
NAME            STATE  STATE  IMAGE           PERSONALITY  NAME  IP ADDRESS  ADDRESS
-------------------------------------------------------------------------------------
first_vsmart    up     up     99.99.999-2440  vsmart       eth0  169.254.0.2  10.0.1.25
second_vsmart   up     up     99.99.999-2440  vsmart       eth0  169.254.0.3  10.0.1.26
vm10            up     up     99.99.999-2444  vsmart       eth0  169.254.0.1  10.0.1.30
```

```
eth1  169.254.1.1  10.0.12.20
eth2  169.254.2.1  10.2.2.20
```

Related Topics

container, on page 145
show container instances, on page 785

show control affinity config

show control affinity config—Display configuration information about the control connections between the vEdge router and one or more vSmart controllers (on vEdge routers only).

Command Syntax

show control affinity config [*index* [*parameter*]]

Syntax Description

None	Display information about all control connections between the vEdge router and vSmart controllers
index[*parameter*]	Information about a Specific Parameter Display configuration information about a specific parameter, starting with the index number of the control connection. *parameter* can be one of the following: **affc-ccl** (current controller group ID list), **affc-ecl** (effective controller group ID list), **affc-equil** (equilibrium status), **affc-ervc** (count of effective required vSmart controllers), and **affc-interface** (interface name).

Release	Modification
16.1.	Command introduced.
16.2.	Display last-resort interface information.

Examples

Show control affinity config

```
vEdge# show 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     ge0/2     2           1(1),  2(1)              1(1)Y,  2(1)Y             Yes
 No
```

Related Topics

show control affinity status, on page 787
show control connections, on page 788
show control local-properties, on page 794

show control affinity status

show control affinity status—Display the status of the control connections between the vEdge router and one or more vSmart controllers (on vEdge routers only).

Command Syntax

show control affinity status [*index* [*parameter*]]

Syntax Description

None	Display information about all control connections between the vEdge router and vSmart controllers
index[*parameter*]	Information about a Specific Parameter Display configuration information about a specific parameter, starting with the index number of the control connection. *parameter* can be one of the following: **affc-acc** (assigned connected vSmart controllers), **affc-interface** (interface name), and **affs-ucc** (unassigned connected vSmart controllers).

Command History

Release	Modification
16.1.	Command introduced.

Examples

Show control affinity status

```
vEdge# show control affinity status

ASSIGNED CONNECTED CONTROLLERS   - System IP( G),..  - System IP of the assigned vSmart
                                                      G is the group ID to which
the vSmart belongs
UNASSIGNED CONNECTED CONTROLLERS - System IP( G),..  - System IP of the unassigned vSmart
                                                      G is the group ID to which
the vSmart belongs

INDEX INTERFACE ASSIGNED CONNECTED CONTROLLERS                      UNASSIGNED CONNECTED
CONTROLLERS
```

```
--------------------------------------------------------------------------------------------------------------
0     ge0/2       172.16.255.19(  1),  172.16.255.20(  2)
```

Related Topics

show control affinity config, on page 786
show control connections, on page 788
show control local-properties, on page 794

show control connection-info

show control connection-info—Display information about the control plane connections on the Cisco vEdge device.

Command Syntax

show control connection-info

Syntax Description

None

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show control connection-info

```
vEdge# show control connection-info
control connection-info "Per-Control Connection Rate: 300 pps"
```

Related Topics

control-session-pps, on page 149

show control connections

show control connections—Display information about active control plane connections (on vSmart controllers and vEdge routers only).

Command Syntax

show control connections [**controller-group-id** *number*] [**detail**]

show control connections *instance-id* [**vbond** | **vedge** | **vsmart**] [*parameters*] [**detail**]

Syntax Description

None	Display information about the active control plane connections to all Cisco vEdge devices in the local domain. Each connection exists on a DTLS connection between the local device and a remote device in the Cisco SD-WAN overlay network.
vbond[*parameters*]	Connections to vBond Orchestrators (On vSmart controllers only.) Display information about the active control plane connections between a vSmart controller and vBond systems in the domain. *parameters* is one or more of the column headers in the **show control connections** command output.
vedge[*parameters*]	Connections to vEdge Routers (On vSmart controllers only.) Display information about the active control plane connections between a vSmart controller and vEdge routers in the domain. *parameters* is one or more of the column headers in the **show control connections** command output. **Note** The interface marked as "last-resort" or admin down is skipped when calculating the number of control connections and partial status is determined based on the other tlocs which are UP. Since the last resort is expected to be down, it is skipped while calculating the partial connection status. Same is the case with admin down interfaces when a particular interface is configured as shutdown. For example, when LTE transport is configured as a last resort circuit, and if the Edge device has 3 tlocs in total including the one with LTE interface, then the device reports partial on 2(4) control connection status.
vsmart[*parameters*]	Connections to vSmart Controllers (On vEdge routers only). Display information about the active control plane connections between a vEdge router and vSmart controllers in the domain. *parameters* is one or more of the column headers in the **show control connections** command output.
controller-group-id *number*	Controller Group (On vEdge routers only). Display information about a specific controller group. *number* can be a value from 0 through 100.
detail	Detailed Information Display detailed information.

Command History

Release	Modification
14.1.	Command introduced.
16.2.	Controller group ID added to vEdge router output.
16.3.	Added IPv6 addresses and ports to output.

Release	Modification
18.2.	Added Proxy column to vEdge router output.

Note The commands **show control connections** and **show control valid-vedges** are supported on vEdge platforms only and do not support on devices with ACT2/TAM modules.

Note The control connections with Cisco vManange goes down for subnet IP 172.17.0.0/16 range on transport interfaces. The IP 172.17.0.0/16 is a reserved range and cannot be used on transport interfaces.

Examples

Show control connections

```
vEdge# show 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  tls  172.16.255.20   200        1      10.0.12.20                                                       23556
 10.0.12.20                               23556 mpls            No    up     0:00:16:30  0

vsmart  tls  172.16.255.20   200        1      10.0.12.20                                                       23556
 10.0.37.20                               23556 lte             Yes   up     0:00:16:22  0

vsmart  tls  172.16.255.19   300        1      10.0.12.19                                                       23556
 10.0.12.19                               23556 mpls            No    up     0:00:16:30  0

vsmart  tls  172.16.255.19   300        1      10.0.12.19                                                       23556
 10.0.37.19                               23556 lte             Yes   up     0:00:16:22  0

vmanage tls  172.16.255.22   200        0      10.0.12.22                                                       23556
 10.0.37.22                               23556 lte             Yes   up     0:00:16:22  0


Manage/vSmart# show control connections

   PEER                                      PEER
      PEER    PEER PEER            SITE       DOMAIN PEER
   PRIV  PEER                                   PUB
INDEX TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP
   PORT  PUBLIC IP                              PORT  REMOTE COLOR    STATE
UPTIME
------------------------------------------------------------------------------------------------------------------------
0     vedge   dtls 172.16.255.11   100        1      2001::a00:50b
   12366 2001::a00:50b                          12366 lte             up
0:00:00:03
```

```
0     vedge   dtls 172.16.255.14   400        1      2001::a01:e0e
   12366 2001::a01:e0e                          12366 lte             up
0:00:00:01
0     vedge   dtls 172.16.255.15   500        1      2001::a01:f0f
   12346 2001::a01:f0f                          12346 lte             up
0:00:00:08
0     vsmart  dtls 172.16.255.20   200        1      2001::a00:c14
   12346 2001::a00:c14                          12346 default         up
0:00:00:17
0     vbond   dtls -               0          0      2001::a00:c1a
   12346 2001::a00:c1a                          12346 default         up
0:00:00:18
1     vedge   dtls 172.16.255.21   100        1      2001::a00:515
   12366 2001::a00:515                          12366 lte             up
0:00:00:03
1     vedge   dtls 172.16.255.16   600        1      2001::a01:1010
   12386 2001::a01:1010                         12386 lte             up
0:00:00:11
1     vbond   dtls -               0          0      2001::a00:c1a
   12346 2001::a00:c1a
```

Related Topics

clear control connections, on page 584
controller-group-id, on page 150
show certificate reverse-proxy, on page 771
show control connections-history, on page 791
show control local-properties, on page 794
show control summary, on page 800
show orchestrator connections, on page 930
tunnel-interface, on page 513

show control connections-history

show control connections-history—Display information about control plane connection attempts initiated by the local device.

Command Syntax

show control connections-history [*index*] [**detail**]

show control connections-history *connection-parameter* [**detail**]

Syntax Description

None	List the history of connections and connection attempts by this Cisco vEdge device.
detail	Detailed Output List detailed connection history information, which includes transmit and receive statistics.

connection-parameter	Specific Connection Parameter List the connection history only for those items match the connection parameter. *connection-parameter* can be one of the following: **domain-id**,**peer-type**, **private-ip**, **private-port**, **public-ip**, **public-port**, **site-id**, and **system-ip**. These values corresponds to the column headers in the output of the show control connections-history command.
index	Specific History Item List the connection history only for the specific item in the history list.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show control connections-history

```
vSmart# show control connections-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.               ORPTMO    - Server's peer timed out.
BIDNTVRFD  - Peer Board ID Cert not verified.        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.        SSLNFAIL  - Failure to create new
SSL context.
CTORGNMMIS - Certificate Org name mismatch.          SERNTPRES - Serial Number not present.
DCONFAIL   - DTLS connection failure.                SYSIPCHNG - System-IP changed.
DEVALC     - Device memory Alloc failures.           TMRALC    - Memory Failure.
DHSTMO     - DTLS HandShake Timeout.                 TUNALC    - Memory Failure.
DISCVBD    - Disconnect vBond after register reply.  TXCHTOBD  - Failed to send challenge
 to BoardID.
DISTLOC    - TLOC Disabled.                          UNMSGBDRG - Unknown Message type or
 Bad Register msg.
DUPSER     - Duplicate Serial Number.                UNAUTHEL  - Recd Hello from
Unauthenticated peer.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer. VBDEST    - vDaemon process terminated.
HAFAIL     - SSL Handshake failure.                  VECRTREV  - vEdge Certification
revoked.
IP_TOS     - Socket Options failure.                 VSCRTREV  - vSmart Certificate
revoked.
LISFD      - Listener Socket FD Error.               VB_TMO    - Peer vBond Timed out.
MGRTBLCKD  - Migration blocked. Wait for local TMO.
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.       XTVSTRDN  - Extra vSmart tear down.

                                                                                    PEER
```

```
                    PEER

        PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE
  PEER             PUBLIC                                    LOCAL      REMOTE     REPEAT

INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT
    PUBLIC IP        PORT    REMOTE COLOR     STATE           ERROR      ERROR      COUNT
DOWNTIME
------------------------------------------------------------------------------------------------------------------------------------
0        vbond    dtls     -                0           0           10.1.14.14       12346
    10.1.14.14       12346   default          connect         DCONFAIL   NOERR      4
2016-02-19T10:47:13-0800
1        vbond    dtls     -                0           0           10.1.14.14       12346
    10.1.14.14       12346   default          connect         DCONFAIL   NOERR      4
2016-02-19T10:47:13-0800
```

```
vSmart# show control connections-history detail
----------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- ::   PEER-PERSONALITY- vbond
----------------------------------------------------------------------------------------
site-id             0
domain-id           0
protocol            dtls
private-ip          10.1.14.14
private-port        12346
public-ip           10.1.14.14
public-port         12346
UUID/chassis-number db383816-8f25-41d5-822a-e7dda8c0ffd8
state               connect [Local Err: ERR_(D)TLS_CONN_FAIL] [Remote Err: NO_ERROR]
downtime            2016-02-19T10:47:13-0800
repeat count        4
previous downtime   2016-02-19T10:46:56-0800

  Tx Statistics-
  --------------
    hello                   0
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      0
    challenge-ack           0
    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0

  Rx Statistics-
  --------------
    hello                   0
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      0
    challenge-ack           0
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0

----------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- ::   PEER-PERSONALITY- vbond
----------------------------------------------------------------------------------------
site-id             0
domain-id           0
```

```
protocol            dtls
private-ip          10.1.14.14
private-port        12346
public-ip           10.1.14.14
public-port         12346
UUID/chassis-number af010b09-539b-412e-bd28-d4ca2f45ea1d
state               connect [Local Err: ERR_(D)TLS_CONN_FAIL] [Remote Err: NO_ERROR]
downtime            2016-02-19T10:47:13-0800
repeat count        4
previous downtime   2016-02-19T10:46:56-0800

  Tx Statistics-
  --------------
    hello                   0
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      0
    challenge-ack           0
    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0

  Rx Statistics-
  --------------
    hello                   0
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      0
    challenge-ack           0
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0
```

Related Topics

clear control connections-history, on page 585
clear orchestrator connections-history, on page 605
show control connections, on page 788
show orchestrator connections-history, on page 932

show control local-properties

show control local-properties—Display the basic configuration parameters and local properties related to the control plane (on vEdge routers, vManage NMSs, and vSmart controllers only).

Command Syntax

show control local-properties [*parameter*]

Syntax Description

None	Display the basic configuration parameters and local properties related to the control plane.

parameter	Information about a Specific Parameter Display configuration information about a specific parameter. *parameter* can be one of the following: **board-serial**, **certificate-not-valid-after**, **certificate-not-valid-before**, **certificate-status**, **certificate-validity**, **device-type**, **dns-cache-flush-interval**, **dns-name**, **domain-id**, **ip-address-list**, **keygen-interva**l, **max-controllers**, **no-activity**, **number-active-wan-interfaces**, **number-vbond-peers**, **organization-name**, **port-hopped**, **protocol**, **register-interval**, **retry-interval**, **root-ca-chain-status**, **root-ca-crl-status site-id**, **system-ip**, **time-since-port-hop**, **tls-port**, **uuid**, **vbond-address-list**, **vedge-list-version**, **vsmart-list-version**, and **wan-interface-list**.

Command History

Release	Modification
14.1.	Command introduced.
16.1.	Added instance field to output for vSmart controllers and vManage NMSs.
16.2.	Added SPI Time Remaining and Last-Resort Interface fields to output for vEdge routers.
16.3.	Added display information about IPv6 WAN interfaces, NAT type, low-bandwidth interface, and vManage connection preference.
17.7	Added **root-ca-crl-status** parameter.
Cisco SD-WAN Release 20.7.1	Added the Hierarchical SD-WAN region assignment to the **REGION IDs** column.
Cisco SD-WAN Release 20.8.1	For Hierarchical SD-WAN architectures, the **REGION IDs** column shows the secondary region also.
Cisco Catalyst SD-WAN Control Components Release 26.2.1 Cisco Catalyst SD-WAN Control Components Release 26.1.2 Cisco Catalyst SD-WAN Control Components Release 20.18.3	In case of an expired certificate, the **certificate-validity** field in the command output shows **Valid - Expired**. Previously it showed only **Expired**.

Usage Guidelines

From Cisco Catalyst SD-WAN Control Components Release 26.2.1 and other releases shown in the modification history, if a certificate is expired, the **certificate-validity** field in the command output shows **Valid - Expired**.

Examples

Show control local-properties

```
vEdge# show control local-properties
personality                  vedge
organization-name            Cisco, Inc.
certificate-status           Installed
root-ca-chain-status         Installed
root-ca-crl-status           Installed

certificate-validity         Valid
certificate-not-valid-before Dec 15 18:06:59 2016 GMT
certificate-not-valid-after  Dec 15 18:06:59 2017 GMT

dns-name                     10.0.12.26
site-id                      100
domain-id                    1
protocol                     dtls
tls-port                     0
system-ip                    172.16.255.11
chassis-num/unique-id        b5887dd3-3d70-4987-a3a4-6e06c1d64a8c
serial-num                   12345714
vsmart-list-version          0
keygen-interval              1:00:00:00
retry-interval               0:00:00:19
no-activity-exp-interval     0:00:00:12
dns-cache-ttl                0:00:02:00
port-hopped                  TRUE
time-since-last-port-hop     0:00:43:16
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


   VM
           PUBLIC           PUBLIC PRIVATE         PRIVATE
PRIVATE                              MAX     CONTROL/            LAST         SPI TIME   NAT
  CON
INTERFACE  IPv4             PORT   IPv4            IPv6
PORT    VS/VM COLOR             STATE CNTRL   STUN         LR/LB  CONNECTION   REMAINING
TYPE PRF
-------------------------------------------------------------------------------------------------------------------------------
ge0/0      10.1.15.15       12426  10.1.15.15      ::
12426    0/0  lte                up    2      no/yes/no   No/No  0:00:00:16   0:11:26:41  E
   5
ge0/3      10.0.20.15       12406  10.0.20.15      ::
12406    0/0  3g                 up    2      no/yes/no   No/No  0:00:00:13   0:11:26:45  N
   5
```

```
vEdge# show control local-properties wan-interface-list

                                        RESTRICT/
           PUBLIC           PUBLIC PRIVATE         PRIVATE
PRIVATE                              MAX     CONTROL/            LAST         SPI TIME
INTERFACE  IPv4             PORT   IPv4            IPv6
PORT    VS/VM COLOR             STATE CNTL   STUN         LR/LB  CONNECTION   REMAINING
                                                                 STUN
-------------------------------------------------------------------------------------------------------------------------------
```

```
ge0/2      10.0.5.11       12366  10.0.5.11       ::
12366    2/0  lte              up    2      no/yes/no   No/No  0:00:16:22   0:11:42:46

vEdge# show control local-properties wan-interface-list | display xml
<config xmlns="http://tail-f.com/ns/config/1.0">
  <control xmlns="http://viptela.com/security">
  <local-properties>
  <wan-interface-list>
    <instance>0</instance>
    <index>0</index>
    <interface>ge0/2</interface>
    <public-ip>10.0.5.11</public-ip>
    <public-port>12366</public-port>
    <private-ip>10.0.5.11</private-ip>
    <private-port>12366</private-port>
    <num-vsmarts>2</num-vsmarts>
    <num-vmanages>0</num-vmanages>
    <weight>1</weight>
    <color>lte</color>
    <carrier>default</carrier>
    <preference>0</preference>
    <admin-state>up</admin-state>
    <operation-state>up</operation-state>
    <last-conn-time>0:00:16:27</last-conn-time>
    <restrict-str>no</restrict-str>
    <control-str>yes</control-str>
    <per-wan-max-controllers>2</per-wan-max-controllers>
    <private-ipv6>::</private-ipv6>
    <spi-change>0:11:42:41</spi-change>
    <last-resort>No</last-resort>
    <wan-port-hopped>TRUE</wan-port-hopped>
    <wan-time-since-port-hop>0:00:19:11</wan-time-since-port-hop>
    <vbond-as-stun-server>no</vbond-as-stun-server>
    <vmanage-connection-preference>5</vmanage-connection-preference>
    <low-bandwidth-link>No</low-bandwidth-link>
  </wan-interface-list>
  </local-properties>
  </control>
</config>

vSmart# show control local-properties
personality                   vsmart
organization-name             Cisco, Inc.
certificate-status            Installed
root-ca-chain-status          Installed
root-ca-crl-status            Installed

certificate-validity          Valid
certificate-not-valid-before  Dec 15 18:07:15 2016 GMT
certificate-not-valid-after   Dec 15 18:07:15 2017 GMT

dns-name                      10.0.12.26
site-id                       100
domain-id                     1
protocol                      dtls
tls-port                      23456
system-ip                     172.16.255.19
chassis-num/unique-id         4fc2a9b0-1dc3-4a1e-b1a4-9c565e6ab12b
serial-num                    12345707
vedge-list-version            0
vsmart-list-version           0
retry-interval                0:00:00:18
no-activity-exp-interval      0:00:00:12
dns-cache-ttl                 0:00:02:00
port-hopped                   FALSE
```

```
time-since-last-port-hop     0:00:00:00
number-vbond-peers           1

INDEX   IP                                        PORT
------------------------------------------------------
0       10.0.12.26                                12346

number-active-wan-interfaces 2

                    PUBLIC          PUBLIC PRIVATE         PRIVATE
         PRIVATE                                  LAST
INSTANCE INTERFACE  IPv4            PORT   IPv4            IPv6
         PORT    VS/VM  COLOR            STATE CONNECTION
-------------------------------------------------------------------------------------------------------
0        eth1       10.0.5.19       12346  10.0.5.19       ::
         12346     1/0   default          up    0:00:00:17
1        eth1       10.0.5.19       12446  10.0.5.19       ::
         12446     0/0   default          up    0:00:00:17
```

```
vManage# show control local-properties
personality                   vmanage
organization-name             Cisco, Inc.
certificate-status            Installed
root-ca-chain-status          Installed
root-ca-crl-status.           Installed

certificate-validity          Valid
certificate-not-valid-before Mar 01 00:07:31 2016 GMT
certificate-not-valid-after  Mar 01 00:07:31 2017 GMT

dns-name                      10.1.14.14
site-id                       200
domain-id                     0
protocol                      dtls
tls-port                      23456
system-ip                     172.16.101.20
chassis-num/unique-id         9f9e3ca9-b909-43c5-be0e-acb819a45dc0
serial-num                    1234560A
vedge-list-version            1
vsmart-list-version           0
retry-interval                0:00:00:19
no-activity-exp-interval      0:00:00:12
dns-cache-ttl                 0:00:02:00
port-hopped                   FALSE
time-since-last-port-hop      0:00:00:00
number-vbond-peers            1

INDEX   IP                 PORT
-------------------------------
0       10.1.14.14         12346

number-active-wan-interfaces 2

                    PUBLIC           PUBLIC  PRIVATE          PRIVATE
                                    LAST
INSTANCE INTERFACE  IP               PORT    IP               PORT     VS/VM  COLOR
     CARRIER             STATE   CONNECTION
-------------------------------------------------------------------------------------------------------
0        eth1       10.0.12.22       12346   10.0.12.22       12346    2/0    default
     default             up       0:00:00:07
1        eth1       10.0.12.22       12446   10.0.12.22       12446    0/0    default
     default             up       0:00:00:08
```

Related Topics

show control connections, on page 788
show orchestrator local-properties, on page 935
show system status, on page 1019
tunnel-interface, on page 513

show control statistics

show control statistics—Display statistics about the packets that a vEdge router or vSmart controller has transmitted and received in the process of establishing and maintaining secure DTLS connections to Cisco vEdge devices in the overlay network (on vEdge routers and vSmart controllers only).

Command Syntax

show control statistics [*counter-name*]

Syntax Description

None	Display statistics about all packets sent and received by the vEdge router or vSmart controller as it establishes and maintains DTLS tunnel connections to the Cisco vEdge devices in the overlay network.
counter-name	Statistics about a Specific Counter Display the statistics for the specific counter. For a list of counters, see the Example Output below.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show control statistic

```
vSmart# show control statistics
Tx Statistics:
--------------
packets                   51181
octets                    3836240
error                     0
blocked                   0
hello                     50894
connects                  0
registers                 283
register-replies          0

dtls-handshake            3
dtls-handshake-failures   0
dtls-handshake-done       3
```

```
challenge                  4
challenge-response         3
challenge-ack              4
challenge-errors           0
challenge-response-errors  0
challenge-ack-errors       0
challenge-general-errors   0
vmanage-to-peer            0
register_to_vmanage        1

Rx Statistics:
--------------
packets                    56725
octets                     4170626
errors                     0
hello                      50897
connects                   855
registers                  0
register-replies           283

dtls-handshake             15
dtls-handshake-failures    0
dtls-handshake-done        4

challenge                  3
challenge-response         4
challenge-ack              3
challenge-failures         0
vmanage-to-peer            1
register_to_vmanage        0
```

Related Topics

show control connections, on page 788
show control summary, on page 800
show orchestrator statistics, on page 937

show control summary

show control summary—List a count of Cisco vEdge devices that the local device is aware of. For devices running on virtual machines (VMs) that have more than one core, this command shows the number of devices that each vdaemon process instance is handling.

Command Syntax

show control summary [*instance*]

Syntax Description

None	Display a count of all the vBond orchestrators, vEdge routers, vManage NMSs, and vSmart controllers in the overlay network.

instance	Devices for a Specific vdaemon Process Display a count of devices for a specific instance of a vdaemon process. Cisco vEdge devices that run on VMs that have more than one core automatically spawn one vdaemon process for each core, to load-balance the Cisco SD-WAN software functions across all the CPUs in the VM server.

Command History

Release	Modification
14.1.	Command introduced.
15.3.3.	Added support for multiple vdaemon processes (for vManage NMS only).
15.4.	Added support for multiple vdaemon processes for all devices running as VMs.
16.3.	Added display of IPv6 addresses and ports.

Examples

Show control summary

```
vEdge# show control summary

           VBOND   VMANAGE  VSMART  VEDGE             LISTENING   LISTENING  LISTENING
INSTANCE   COUNTS  COUNTS   COUNTS  COUNTS  PROTOCOL  IP          IPV6       PORT
-------------------------------------------------------------------------------------
0          1       0        2       3       dtls      10.0.12.22  -          12346
1          1       0        0       2       dtls      10.0.12.22  -          12446
```

Related Topics

show control connections, on page 788
show orchestrator summary, on page 939

show control valid-vedges

show control valid-vedges—List the chassis numbers of the valid vEdge routers in the overlay network (on vSmart controllers only).

Command Syntax

show control valid-vedges

Syntax Description

None

Command History

Release	Modification
14.1.	Command introduced.
14.2	Command renamed from **show control valid-devices**

Examples

Show control valid-vedges

```
vSmart# show control valid-vedges

                SERIAL
CHASSIS NUMBER  NUMBER    VALIDITY
----------------------------------
11OD113140004   10000266  valid
11OD145130082   10000142  staging
11OD252130046   100001FF  valid
11OD252130049   1000020B  valid
11OD252130057   1000020C  staging
R26OC126140004  10000369  valid
```

Related Topics

show control connections, on page 788
show control valid-vsmarts, on page 802
show orchestrator valid-vedges, on page 940

show control valid-vsmarts

List the serial numbers of the valid vSmart controllers in the overlay network (on vEdge routers and vSmart controllers only).

show control valid-vsmarts [*serial-number*]

Syntax Description

None	Display the serial numbers of all valid vSmart controllers in the overlay network.
Serial Number	*serial-number* List whether a specific vSmart serial number is valid**.**

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show control valid-vsmarts

```
vEdge# show control valid-vsmarts
SERIAL NUMBER     ORG
-------------------------------------
9AG05FECDEC9A35F  Cisco Systems
9AG05FECDEC9A362  Cisco Systems
```

Related Topics

show control connections, on page 788
show control valid-vedges, on page 801
show orchestrator valid-vsmarts, on page 942

show crash

Display a list of the core files on the local device. Core files are saved in the /var/crash directory on the local device. They are readable by the "admin" user.

show crash [*index-number*] [**core-filename** *filename*]

Syntax Description

None	List all core files on the local device.
Core Filename	**core-filename** *filename* List a specific core filename.
File Index Number	*index-number* List a specific file by file index number.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show crash

```
vSmart# show crash

INDEX  CORE TIME                CORE FILENAME
-------------------------------------------------------------------
0      Tue Sep  2 17:13:43 2014  core.ompd.866.vsmart.1409703222
```

Related Topics

clear crash, on page 586
file list, on page 637

file show, on page 637
logging disk, on page 298
show logging, on page 891

show crypto pki trustpoints status

To display the trustpoint information, use the **show crypto pki trustpoints status** command.

show crypto pki trustpoints *label* **status**

Syntax Description

label	A user-specified label that is referenced within the **crypto pki trustpoint** command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco SD-WAN Release 20.1.1	This command was introduced.

Example

This example shows how to display the trustpoint information:

```
Router# show crypto pki trustpoints  Root CAstatus

crypto pki trustpoints Root-CA status
Trustpoint Root-CA:
  Issuing CA certificate configured:
    Subject Name:
     cn=ca
    Fingerprint MD5: 653100C5 90CF8698 0BA8E443 BC85D616
    Fingerprint SHA1: DCEC0FCD 12C319C1 61191263 E52007FB 2E8D353A
  Last enrollment status: Granted
  State:
    Keys generated ..... Yes
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

show devices

Display information about the Cisco vEdge devices that a vManage NMS is managing (on vManage NMSs only).

show devices [**device** *device-name*] [**commit-queue**] [**state** *state*]

Syntax Description

None	List information about all devices that the vManage NMS is managing.
Queue Length	**commit-queue** List information about the queue length.
Specific Device	**device** *device-name* List information about a specific device that the vManage NMS is managing.
Specific State	**state** *state* List information about a specific state. *state* can be **admin-state**, **last-transaction-id**, **oper-state**, and **oper-state-error-tag**. These states correspond to the column headings in the output of the **show devices** command.

Command History

Release	Modification
14.2.	Command introduced.

Examples

Display information about all the Cisco vEdge devices that a vManage NMS is managing:

Show devices

```
vManage# show devices
                                                OPER
                                                STATE  LAST
                     QUEUE   WAITING  OPER      ERROR  TRANSACTION
NAME                 LENGTH  FOR      STATE     TAG    ID
-----------------------------------------------------------------------
myvedge              0       [  ]     disabled  -      -
vedge-172.16.255.11  0       [  ]     enabled   -      -
vedge-172.16.255.14  0       [  ]     disabled  -      -
vedge-172.16.255.15  0       [  ]     enabled   -      -
vedge-172.16.255.16  0       [  ]     enabled   -      -
```

```
vedge-172.16.255.21   0       [  ]     enabled   -      -

vsmart-172.16.255.19  0       [  ]     enabled   -      -

vsmart-172.16.255.20  0       [  ]     enabled   -      -
```

show dhcp interface

Display information about interfaces that are DHCPv4 clients (on vEdge routers and vSmart controllers only).

show dhcp interface [**vpn** *vpn-id*] [*interface-name*]**show dhcp interface** [**dns-list**] [**state**]

Syntax Description

None	Display information about all interfaces that are DHCPv4 clients.
DNS Servers	**dns-list** Display the DHCPv4 client DNS information.
Lease State	**state** Display the DHCPv4 client interface state information.
VPN	**vpn** *vpn-id* Display DHCPv4 client interface information for a specific VPN.

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show dhcp interface

```
vEdge# show dhcp interface
                                                                                TIME

VPN   INTERFACE   STATE   ACQUIRED IP          SERVER          LEASE TIME    REMAINING     GATEWAY
         INDEX   DNS
-------------------------------------------------------------------------------------------------------------
0     ge0/4       bound   192.168.178.131/24   192.168.178.1   13:00:00:00   11:15:32:11
192.168.178.1   0       192.168.178.1
```

Related Topics

clear dhcp server-bindings, on page 587
dhcp-helper, on page 179
dhcp-server, on page 181
show dhcp server, on page 807
show ipv6 dhcp interface, on page 877

show dhcp server

Display information about the DHCP server functionality that is enabled on the router (on vEdge routers only).

show dhcp server [**bindings** *mac-address*] [*dhcp-property*]**show dhcp server** [**vpn** *vpn-id*] [**bindings** *mac-address*] [*dhcp-property*]

Syntax Description

None	Display information about all DHCP server functionality enabled on the router.
Client Binding	**bindings** *mac-address* Display the DHCP binding information for the client with the specified MAC address.
DHCP Property	*dhcp-property* Display information about a specific DHCP property. *dhcp-property* can be one of **client-ip** *ip-address*, **host-name** *hostname*, **lease-time**, **least-time-remaining**, and **static-binding** (**false** | **true**).
VPN	**vpn** *vpn-id* Display DHCP server information for a specific VPN.

Command History

Examples

Release	Modification
14.3.	Command introduced.

Show dhcp server

```
vEdge# show dhcp server
                                                                    LEASE TIME  STATIC
VPN  IFNAME  CLIENT MAC         CLIENT IP       LEASE TIME  REMAINING   BINDING  HOST NAME
-------------------------------------------------------------------------------------------
1    ge1/2   00:00:00:79:64:01  192.168.15.101  1:00:00:00  0:13:37:25  false    --
             00:00:00:79:64:02  192.168.15.102  1:00:00:00  0:13:37:20  false    --
             00:0c:29:21:30:d0  192.168.15.103  1:00:00:00  0:16:38:53  false    --
...
```

Related Topics

clear dhcp server-bindings, on page 587
clear dhcp state, on page 588
dhcp-server, on page 181
show dhcp interface, on page 806

show dot1x clients

Display information about the 802.1X clients in the network (on vEdge routers only).

Command Hierarchy

```
show dot1x clients [detail]
show dot1x clients eapol [detail]
show dot1x clients interface interface-name [macaddress mac-address]
```

Syntax Description

None	Display standard information about the 802.1X clients in the network.
Detailed Client Information	**detail** Display detailed information about the 802.1X clients.
EAPOL State	**eapol** Display the Extensible Authentication Protocol over LAN (EAPOL) status for each 802.1X client.
Specific Interface and MAC Address	**interface** *interface-name* [**macaddress** *mac-address*] Display the 802.1X clients on a specific interface, or display a specific client on a specific interface.

Command History

Release	Modification
16.3.	Command introduced.

Examples

Display information about the 802.1X clients on an 802.1X–enabled interface:

Show dot1x clients

```
vEdge# show dot1x clients
                                                  AUTH                EAP                SESSION
  CONNECTED  INACTIVE  SESSION
INTERFACE  MAC ADDRESS        AUTH STATE      METHOD  VLAN  VPN  METHOD  USERNAME  TIME
  TIME       TIME      ID
-------------------------------------------------------------------------------------------------
ge0/1      00:50:b6:0f:1c:84  Authenticating  Radius  12    -    (PEAP)  -         -
  -          1         -

vEdge# show dot1x clients
                                             AUTH                EAP                SESSION
 CONNECTED  INACTIVE
INTERFACE  MAC ADDRESS        AUTH STATE     METHOD  VLAN  VPN  METHOD  USERNAME  TIME
 TIME       TIME      SESSION ID
-------------------------------------------------------------------------------------------------
ge0/1      00:50:b6:0f:1c:84  Authenticated  Radius  12    -    (PEAP)  ravi      9
 9          0         57E1B641-00000001
```

Related Topics

clear dot1x client, on page 590
dot1x, on page 191
show dot1x interfaces, on page 809
show dot1x radius, on page 810
show system statistics, on page 1015

show dot1x interfaces

Display information about 802.1X–enabled interfaces (on vEdge routers only).

show dot1x interfaces

Syntax Description

Syntax Description

None

Command History

Release	Modification
16.3.	Command introduced.

Examples

Display information about the 802.1X on an 802.1Z–enabled interface:

Show dot1x interfaces

```
vEdge# show dot1x interfaces
      802.1X Interface Information:

      Interface ge0/1:
        Operational state           : Up
        Host mode                   : Multi Auth
        MAB server                  : true
        MAB local                   : true
        Wake On LAN                 : true
        Reauthentication period     : 600 seconds
        Inactivity timeout          : 3600 seconds
        Guest VLAN                  : 11
        Auth fail VLAN              : 12
        Auth reject VLAN            : 13
        Default VLAN                :
        Primary radius server       : 192.168.48.12
        Secondary radius server     : 192.168.48.11
        Interim accounting interval : disabled
        Number of connected clients : 1

      802.1X Interface Information:

      Interface ge0/2:
        Operational state           : Down
        Host mode                   : Single Host
```

```
MAB server                  : false
MAB local                   : false
Wake On LAN                 : false
Reauthentication period     : disabled
Inactivity timeout          : disabled
Guest VLAN                  : none
Auth fail VLAN              : none
Auth reject VLAN            : none
Default VLAN                :
Primary radius server       : 192.168.48.11
Secondary radius server     : none
Interim accounting interval : disabled
Number of connected clients : 0
```

Related Topics

clear dot1x client, on page 590
dot1x, on page 191
show dot1x clients, on page 808
show dot1x radius, on page 810
show system statistics, on page 1015

show dot1x radius

Display statistics about the sessions with RADIUS servers being used for IEEE 802.1X and 802.11i authentication (on vEdge routers only).

Command Hierarchy

```
show dot1x radius
```

Syntax Description

None

Command History

Release	Modification
16.3.	Command introduced.

Examples

Display information about the RADIUS servers that are being used for IEEE 802.1X WAN and 802.11i WLAN authentication:

Show dot1x radius

```
vEdge# show dot1x radius
RADIUS server information for 802.1X interface ge0/1:
    Server IP address              : 192.168.48.11
    Server VPN                     : 512
    Server priority                : secondary
    Authentication statistics:
```

```
        Port number                : 1812
        Server is current          : true
        Round trip time            : 0
        Access requests            : 10
        Access retransmissions     : 0
        Access accepts             : 1
        Access rejects             : 0
        Access challenges          : 9
        Malformed access responses : 0
        Bad authenticators         : 0
        Pending requests           : 0
        Timeouts                   : 0
        Unknown types              : 0
        Packets dropped            : 0
    Accounting statistics:
        Port number                : 1813
        Server is current          : true
        Round trip time            : 0
        Requests                   : 5
        Retransmissions            : 0
        Responses                  : 2
        Malformed responses        : 0
        Bad authenticators         : 0
        Pending requests           : 0
        Timeouts                   : 3
        Unknown types              : 0
        Packets dropped            : 0

RADIUS server information for 802.1X interface ge0/1:
    Server IP address              : 192.168.48.12
    Server VPN                     : 512
    Server priority                : primary
    Authentication statistics:
        Port number                : 1812
        Server is current          : false
        Round trip time            : 0
        Access requests            : 1
        Access retransmissions     : 1
        Access accepts             : 0
        Access rejects             : 0
        Access challenges          : 0
        Malformed access responses : 0
        Bad authenticators         : 0
        Pending requests           : 0
        Timeouts                   : 2
        Unknown types              : 0
        Packets dropped            : 0
    Accounting statistics:
        Port number                : 1813
        Server is current          : false
        Round trip time            : 0
        Requests                   : 4
        Retransmissions            : 2
        Responses                  : 0
        Malformed responses        : 0
        Bad authenticators         : 0
        Pending requests           : 0
        Timeouts                   : 6
        Unknown types              : 0
        Packets dropped            : 0
```

Related Topics

clear dot1x client, on page 590

show dot1x interfaces, on page 809
radius, on page 407
show dot1x clients, on page 808
show system statistics, on page 1015

show hardware alarms

Display information about currently active hardware alarms (on vEdge routers only).

show hardware alarms [*alarm-number*]

Syntax Description

None	Display all currently active hardware alarms.
Specific Alarm	*alarm-number* Display information about a specific hardware alarm.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show hardware alarms

```
vEdge# show hardware alarms
ALARM  ALARM                                                    ALARM

ID     INSTANCE  ALARM NAME         ALARM TIME                 CATEGORY  ALARM DESCRIPTION

-------------------------------------------------------------------------------------------------------
5      0         Power Supply Down  Thu Nov 07 14:19:21 PST 2  Minor     Power supply '0'
down or not present
5      1         Power Supply Down  Thu Nov 07 14:19:21 PST 2  Minor     Power supply '1'
down or not present
```

Related Topics

show hardware environment, on page 813
show hardware inventory, on page 816
show hardware real time information, on page 818
show hardware temperature-thresholds, on page 820
show interface sfp detail, on page 844
show interface sfp diagnostic, on page 849

show hardware environment

Display status information about the router components, including component temperature (on vEdge routers only).

show hardware environment [**Fans** [*fan-name*]] [**PEM** [*pem-name*]] [**PIM** [*pim-name*] [**Temperature** [*component-name*]] [**USB**]**show hardware environment** (**measurement** | **status**)

Syntax Description

None	None: Display status information about all router components.
measurement	Component Measurement: List the components and the information in the Measurement column, such as a component's temperature.
status	Component Status: List the components and the information in the Status column.
Temperature [*component-name*]	Component Temperature: Display the temperature of all router components or of a specific component.
Fans [*fan-name*]	Fan Information: Display information about all the fans or about a specific fan. Note that the Cisco SD-WAN software maintains the fans at an optimal fan speed, raising the speed as the ambient temperature increases and decreasing the speed as the temperature decreases, to keep the vEdge router operating at the lowest possible temperature in the green temperature threshold.
PEM [*pem-name*]	PEM Information: Display information about all the power supply modules or about a specific power supply.
PIM [*pim-name*]	PIM Information: Display information about all the Pluggable Interface Modules (PIMs) or about a specific PIM.
USB	USB Information: **USB** Display information about USB controllers.

Command History

Release	Modification
14.1	Command introduced.

Release	Modification
17.1	Display status of router LEDs in the command output.

Output Fields

LEDs

In Releases 17.1 and later, the command output shows the status of the hardware router LEDs, as follows:

- vEdge 100b—System LED
- vEdge 100m—System and WWAN LEDs
- vEdge 100wm—System, WLAN, and WWAN LEDs
- vEdge 1000—Status and System LEDs
- vEdge 2000—PIM Status, Status, and System LEDs

Example

```
vEdge# show hardware environment
                                        HW
                                        DEV
HW CLASS             HW ITEM            INDEX  STATUS  MEASUREMENT
-------------------------------------------------------------------------------------------------
Temperature Sensors  PIM                 0      OK      35 degrees C/95 degrees F
Temperature Sensors  DRAM                0      OK      27 degrees C/81 degrees F
Temperature Sensors  DRAM                1      OK      29 degrees C/84 degrees F
Temperature Sensors  Board               0      OK      29 degrees C/84 degrees F
Temperature Sensors  Board               1      OK      33 degrees C/92 degrees F
Temperature Sensors  Board               2      OK      34 degrees C/93 degrees F
Temperature Sensors  Board               3      OK      33 degrees C/91 degrees F
Temperature Sensors  CPU junction        0      OK      41 degrees C/106 degrees F
Fans                 Tray 0 fan          0      OK      Spinning at 6300 RPM
Fans                 Tray 0 fan          1      OK      Spinning at 4080 RPM
Fans                 Tray 1 fan          0      OK      Spinning at 6300 RPM
Fans                 Tray 1 fan          1      OK      Spinning at 4080 RPM
Fans                 Tray 2 fan          0      OK      Spinning at 5940 RPM
Fans                 Tray 2 fan          1      OK      Spinning at 4020 RPM
Fans                 Tray 3 fan          0      OK      Spinning at 6180 RPM
Fans                 Tray 3 fan          1      OK      Spinning at 3960 RPM
PEM                  Power supply        0      Down    Present: yes; Powered On: no; Fault: no
PEM                  Power supply        1      OK      Present: yes; Powered On: yes; Fault: no
```

```
PIM                  Interface module        0      OK      Present: yes; Powered On: yes; Fault: no

PIM                  Interface module        1      OK      Present: yes; Powered On: yes; Fault: no

PIM                  Interface module        2      OK      Present: yes; Powered On: yes; Fault: no
USB                  External USB Controller 0      Down    In reset

vEdge1000# show hardware environment
                                             HW
                                             DEV
HW CLASS             HW ITEM                 INDEX  STATUS  MEASUREMENT
-------------------------------------------------------------------------------------------------------
Temperature Sensors  DRAM                    0      OK      40 degrees C/105 degrees F
Temperature Sensors  Board                   0      OK      37 degrees C/98 degrees F
Temperature Sensors  Board                   1      OK      38 degrees C/101 degrees F
Temperature Sensors  Board                   2      OK      36 degrees C/96 degrees F
Temperature Sensors  Board                   3      OK      36 degrees C/96 degrees F
Temperature Sensors  CPU junction            0      OK      49 degrees C/120 degrees F
Fans                 Tray 0 fan              0      OK      Spinning at 4560 RPM
Fans                 Tray 0 fan              1      OK      Spinning at 4740 RPM
PEM                  Power supply            0      OK      Powered On: yes; Fault: no
PEM                  Power supply            1      Down    Powered On: no; Fault: no
PIM                  Interface module        0      OK      Present: yes; Powered On: yes; Fault: no
USB                  External USB controller 0      Down    In reset
LED                  Status LED              0      OK      Off
LED                  System LED              0      OK      Red

vEdge100/1000# show hardware environment pem
                     HW
HW                   DEV
CLASS  HW ITEM       INDEX  STATUS  MEASUREMENT
-------------------------------------------------------------
PEM    Power supply  0      OK      Powered On: yes; Fault: no
PEM    Power supply  1      Down    Powered On: no; Fault: no

vEdge# show hardware measurement
                                             HW
                                             DEV
HW CLASS             HW ITEM                 INDEX  MEASUREMENT
-----------------------------------------------------------------------------------------
Temperature Sensors  DRAM                    0      0 degrees C/32 degrees F
Temperature Sensors  Board                   0      0 degrees C/32 degrees F
Temperature Sensors  Board                   1      0 degrees C/32 degrees F
Temperature Sensors  Board                   2      0 degrees C/32 degrees F
Temperature Sensors  Board                   3      0 degrees C/32 degrees F
Temperature Sensors  CPU junction            0      0 degrees C/32 degrees F
PEM                  Power supply            0      Present: no; Powered On: no; Fault: no
PEM                  Power supply            1      Present: no; Powered On: no; Fault: no
PIM                  Interface module        0      Present: yes; Powered On: no; Fault: no
USB                  External USB controller 0      2 USB Ports
```

Operational Commands

show hardware alarms

show hardware inventory

show hardware real-time-information

show hardware temperature-thresholds

Related Topics

show hardware alarms, on page 812
show hardware inventory, on page 816
show hardware real time information, on page 818
show hardware temperature-thresholds, on page 820

show hardware inventory

Display an inventory of the hardware components in the router, including serial numbers (on vEdge routers only).

show hardware inventory [*component-name*]

Syntax Description

	None: Display the inventory of all router components.
component-name	Specific Component: Display inventory information about a specific component. *component-name* can be one of **cpu**, **chassis**, **dram**, **eemc**, **fan-tray**, **flash**, **pim**, and **transceiver**.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

For vEdge routers that support WLAN interfaces, the Description column for the Chassis includes the country code (shows as CC:).

Example

```
vEdge-1000# show hardware inventory
            HW
            DEV
HW TYPE     INDEX  VERSION  PART NUMBER       SERIAL NUMBER     DESCRIPTION
-------------------------------------------------------------------------------------------------------------------------
Chassis     0      3.1      vEdge-1000        11OD145130039     vEdge-1000
CPU         0      None     None              None              Quad-Core Octeon-II
DRAM        0      None     None              None              2048 MB DDR3
Flash       0      None     None              None              Flash: Type - nor, Size - 16.00 MB
eMMC        0      None     None              None              eMMC: Size - 7.31 GB
USB         0      None     None              20046000CBF20D899 USB 0: Manufacturer - SanDisk, Product - Cruzer, Size - 3.74
 GB
PIM         0      None     ge-fixed-8        None              8x 1GE Fixed Module
Transceiver 0      A        FCLF-8521-3       PQM2QLL           Port 0/0, Type 0x8 (Copper), Vendor - FINISAR CORP.
Transceiver 1      A        FCLF-8521-3       PQP6KRT           Port 0/1, Type 0x8 (Copper), Vendor - FINISAR CORP.
Transceiver 7      PB       1GBT-SFP05        PQE5T0T           Port 0/7, Type 0x8 (Copper), Vendor - BEL-FUSE
FanTray     0      None     None              None              Fixed Fan Tray - 2 Fan
vEdge-100# show hardware inventory
          HW
          DEV
HW TYPE   INDEX  VERSION  PART NUMBER   SERIAL NUMBER   HW DESCRIPTION
-----------------------------------------------------------------------------------------
Chassis   0      4.1      vEdge-100M    1780D133150002  vEdge-100. CPLD rev: 0x8, PCB rev: D.
CPU       0      None     None          None            Dual-Core Octeon-III
DRAM      0      None     None          None            2048 MB DDR3
PIM       0      None     ge-fixed-5    None            5x 1GE Fixed Module
PIM       1      None     Wireless LAN  None            Wireless LAN Module
PIM       2      None     Wireless WAN  None            Wireless WAN Module
```

```
FanTray  0      None     None          None            Fixed Fan Tray - 1 Fan
vEdge-100# show hardware inventory Transceiver
hardware inventory Transceiver 1
version          "    "
part-number      "AFBR-5710PZ "
serial-number    "AM12482AZ3K "
hw-description   "Port 0/1, Type 0x01 (1G Fiber SX), Date: 2012/11/29, Vendor: AVAGO "
hardware inventory Transceiver 5
version          "    "
part-number      "AFBR-5710PZ "
serial-number    "AM13412D2Z7 "
hw-description   "Port 0/5, Type 0x01 (1G Fiber SX), Date: 2013/10/11, Vendor: AVAGO
vEdge-100wm# show hardware inventory

          HW
          DEV
HW TYPE   INDEX  VERSION  PART NUMBER   SERIAL NUMBER    HW DESCRIPTION
-------------------------------------------------------------------------------------------------------------------------------
Chassis   0      6.2      81001730400   1780F2215160008  vEdge-100wm-GB. CPLD rev: 0x2, PCB rev: F, CC: US. Mfg Date: 19/05/2016
CPU       0      None     None          None             Dual-Core Octeon-III
DRAM      0      None     None          None             2048 MB DDR3
PIM       0      None     ge-fixed-5    None             5x 1GE Fixed Module
PIM       1      None     Wireless LAN  None             Wireless LAN Module
PIM       2      None     Wireless WAN  None             Wireless WAN Module
FanTray   0      None     None          None             Fixed Fan Tray - 1 Fan
vEdge-Cloud# show hardware inventory

          HW
          DEV                           SERIAL
HW TYPE   INDEX  VERSION  PART NUMBER  NUMBER  HW DESCRIPTION
-------------------------------------------------------------------
Chassis   0      1.0      vEdge-Cloud  sim     vEdge-Cloud
PIM       0      None     ge-8         None    Max 8 x 1GE VM ports

vEdge-Cloud# show hardware alarms
# No entries found.
vEdge-Cloud# show hardware temperature-thresholds
% No entries found.
```

Operational Commands

show hardware alarms

show hardware environment

show hardware temperature-thresholds

show interface sfp detail

show interface sfp diagnostic

Related Topics

show hardware alarms, on page 812
show hardware environment, on page 813
show hardware temperature-thresholds, on page 820
show interface sfp detail, on page 844
show interface sfp diagnostic, on page 849

show hardware poe

show hardware poe—Display the status of PoE interfaces (on vEdge 100 series routers only).

show hardware poe

Syntax Description

None

None	Display status information about all router components.
Component Measurement	**measurement** List the components and the information in the Measurement column, such as a component's temperature.
Component Status	**status** List the components and the information in the Status column.

Component Temperature	**Temperature** [*component-name*] Display the temperature of all router components or of a specific component.

Fan Information	**Fans** [*fan-name*] Display information about all the fans or about a specific fan. Note that the Cisco SD-WAN software maintains the fans at an optimal fan speed, raising the speed as the ambient temperature increases and decreasing the speed as the temperature decreases, to keep the vEdge router operating at the lowest possible temperature in the green temperature threshold.

Examples

```
vEdge# show hardware poe                                POE       MAXIMUM  USED   DEVICE INTERFACE
    ADMIN STATUS   STATUS    POWER    POWER  CLASS
-----------------------------------------------------------------ge0/0        Up
Enabled   15.4     4.3    Class 4
```

Command History

Command introduced in Cisco SD-WAN Software Release 18.2.

Related Topics

show hardware alarms, on page 812
show hardware inventory, on page 816
show hardware real time information, on page 818
show hardware temperature-thresholds, on page 820
show interface, on page 827

show hardware real time information

show hardware real-time-information—Display real-time information about hardware vEdge routers, including board details, hardware components, bootloader version, and temperature threshold history (on vEdge routers only).

show hardware real-time-information

Command History

Release	Modification
17.2	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show hardware real-time-information
Hardware Information
------------------------------------------------
Baseboard Details:
board type:board_type: 20003
board serial number:board_serial_number: 11OG119160463
------------------------------------------------
TPM Details:
Chip name: R5H30211
Firmware name: Board ID 2.0
Firmware version: 0x20A13811
------------------------------------------------
Pheripheral Connected:
HW
DEV
HW TYPE INDEX VERSION PART NUMBER SERIAL NUMBER HW DESCRIPTION
------------------------------------------------------------------------------------------------------------------------------------------------------
Chassis 0 7.0 vEdge-1000 11OG119160463 vEdge-1000. CPLD rev: 0xB, PCB rev: G.
CPU 0 None None None Quad-Core Octeon-II
DRAM 0 None None None 4096 MB DDR3
Flash 0 None None None Flash: Type - nor, Size - 16.00 MB
eMMC 0 None None None eMMC: Size - 7.31 GB
PIM 0 None ge-fixed-8 None 8x 1GE Fixed Module
Transceiver 1 A FCLF8521P2BTL PVM16HM Port 0/1, Type 0x08 (1G Copper), Date: 2016/5/22, Vendor: FINISAR CORP. , Support: Yes
FanTray 0 None None None Fixed Fan Tray - 2 Fans
PEM 0 None None None Manufacturer: NA, Product: NA, Date: NA
PEM 1 None None None Manufacturer: NA, Product: NA, Date: NA
------------------------------------------------
Bootloader version:
Backup U-Boot
U-Boot 2013.07-g1874683 (Build time: Mar 22 2017 - 12:57:51)
U-Boot 2013.07-g1874683 (Build time: Mar 22 2017 - 12:57:51)
Active U-Boot
U-Boot 2013.07-g1874683 (Build time: Mar 22 2017 - 12:57:51)
U-Boot 2013.07-g1874683 (Build time: Mar 22 2017 - 12:57:51)
------------------------------------------------
Temperature threshold history:
------------------------------------------------
Critial Kernel Logs:
kern.err: Jul 12 23:14:03 vedge kernel: Error: PEXP_SLI_INT_SUM[RML_TO]
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] No Caching mode page found
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] No Caching mode page found
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] No Caching mode page found
kern.err: Jul 12 23:14:03 vedge kernel: sd 0:0:0:0: [sda] Assuming drive cache: write through
```

Operational Commands

show hardware alarms

show hardware environment

show hardware temperature-thresholds

show interface sfp detail

show interface sfp diagnostic

Related Topics

show hardware alarms, on page 812
show hardware environment, on page 813
show hardware temperature-thresholds, on page 820
show interface sfp detail, on page 844

show interface sfp diagnostic, on page 849

show hardware temperature-thresholds

show hardware temperature-thresholds—Display temperature thresholds at which green, yellow, and red alarms are generated (on vEdge routers only).

show hardware temperature-thresholds [**board** [*board-number*]] [**cpu**] [**dram**]

Syntax Description

None	None: Display status information about all router components.
board [*board-number*]	Board Temperature Threshold: Display the alarm threshold temperature for all boards in the router or for a specific board.
cpu	CPU Temperature Threshold: Display the alarm threshold temperature for the router's CPU.
dram	DRAM Temperature: Display the alarm threshold temperature for the router's DRAM.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show hardware temperature-thresholds

              HW     FAN     FAN    YELLOW  YELLOW   RED     RED
HW SENSOR     DEV    SPEED   SPEED  ALARM   ALARM    ALARM   ALARM
TYPE          INDEX  NORMAL  HIGH   NORMAL  BAD FAN  NORMAL  BAD FAN
-------------------------------------------------------------------------
Board         0      64      64     65      60       80      75
Board         1      64      64     65      60       80      75
Board         2      64      64     65      60       80      75
Board         3      64      64     65      60       80      75
CPU Junction  0      79      79     80      75       95      90
DRAM          0      64      64     65      60       80      75

vEdge-Cloud# show hardware inventory

         HW
         DEV                          SERIAL
```

```
HW TYPE  INDEX  VERSION  PART NUMBER  NUMBER  HW DESCRIPTION
-------------------------------------------------------------------------
Chassis  0      1.0      vEdge-Cloud  sim     vEdge-Cloud
PIM      0      None     ge-8         None    Max 8 x 1GE VM ports

vEdge-Cloud# show hardware alarms
# No entries found.
vEdge-Cloud# show hardware temperature-thresholds
% No entries found.
```

Operational Commands

show hardware alarms

show hardware environment

show hardware real-time-information

show interface sfp detail

show interface sfp diagnostic

Related Topics

show hardware alarms, on page 812
show hardware environment, on page 813
show hardware real time information, on page 818
show hardware temperature-thresholds, on page 820
show interface sfp diagnostic, on page 849

show history

show history—Display the history of the commands issued in operational mode.

show history [*number*]

Syntax Description

None	None: List all operational commands that have been issued during the current login session.
number	Specific Number of Commands: Display the specified number of most recent commands that have been issued in operational mode.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vm4(config)# show history 12
02:07:53 -- show configuration merge banner
02:09:45 -- show configuration rollback changes 14
02:10:11 -- show full-configuration
02:14:20 -- show full-configuration banner
02:15:52 -- show configuration running
02:18:18 -- show configuration running banner
02:22:06 -- show configuration rollback changes 1
02:22:13 -- show configuration rollback changes 2
02:22:16 -- show configuration rollback changes 3
02:34:36 -- show configuration this omp
02:34:43 -- show configuration this banner
02:35:32 -- show history 12
vm4(config)#
```

Operational Commands

show history

Related Topics

clear history, on page 591
history, on page 639
show history, on page 1092

show igmp groups

show igmp groups—Display information about multicast groups (on vEdge routers only).

show igmp groups [**vpn** *vpn-id*]**show igmp groups vpn** *vpn-id group-property*

Syntax Description

None	None: Display information about all multicast groups.
group-property	Group Properties: *group-property* Display group information for a specific IGMP multicast group. *group-property* can be one of the following: **event**, **expires**, **state**, **up-time**, **v1-expires**, and **v1-members-present**. Note that these options correspond to the column heads in the output of the plain **show igmp groups** command.
vpn [*vpn-id*]	VPN: Display multicast group information for interfaces in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show igmp groups
                          V1
     IF                   MEMBERS                                    V1
VPN  NAME   GROUP         PRESENT  STATE           UPTIME      EXPIRES  EXPIRES  EVENT
-------------------------------------------------------------------------------------
1    ge0/5  229.229.229.229  false    members-present  0:01:33:52  -        -        init-event
```

Operational Commands

clear igmp interface

igmp

show igmp groups

show igmp statistics

how igmp summary

Related Topics

igmp, on page 235
show igmp interface, on page 823
show igmp statistics, on page 824
show igmp summary, on page 826

show igmp interface

show igmp interface—Display information about the interfaces on which IGMP is enabled on the router (on vEdge routers only).

show igmp interface [**vpn** *vpn-id*]**show igmp interface vpn** *vpn-id igmp-property*

Syntax Description

None	None: Display information about all interfaces on which IGMP is enabled.
igmp-property	IGMP Options: Display interface information for a specific IGMP property. *igmp-property* can be one of the following: **event**, **group-count**, **if-addr**, **querier**, **querier-ip**, and **state**. Note that these options correspond to the column heads in the output of the plain **show igmp interface** command.
vpn*vpn-id*	VPN **vpn** *vpn-id* Display IGMP information for interfaces in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show igmp interface

                                                                                  OTHER
     IF                        GROUP                          QUERY               QUERIER
VPN  NAME    IF ADDR           COUNT  QUERIER  QUERIER IP    INTERVAL    STATE    EXPIRY   EVENT
-------------------------------------------------------------------------------------------------
1    ge0/4   10.20.24.15/24    0      true     10.20.24.15   0:00:02:00  querier  -        init-event
1    ge0/5   56.0.1.15/24      1      true     56.0.1.15     0:00:01:51  querier  -        init-event
```

Operational Commands

clear igmp interface

igmp

show igmp groups

show igmp statistics

how igmp summary

Related Topics

clear igmp interface, on page 591
igmp, on page 235
show igmp groups, on page 822
show igmp statistics, on page 824
show igmp summary, on page 826

show igmp statistics

show igmp statistics—Display IGMP statistics (on vEdge routers only).

show igmp statistics [**vpn** *vpn-id*]**show igmp statistics vpn** *vpn-id statistic*

Syntax Description

None	None: Display information about all interfaces on which IGMP is enabled.

group-property	Specific Statistic: *group-property* Display interface information for a specific IGMP statistic. *statistic* can be one of the following: **rx_error**, **rx_general_query**, **rx_group_query**, **rx_leave**, **rx_unknown**, **rx_v1_report**, **rx_v2_reporttx_error**, **tx_general_query**, and **tx_group_query**. Note that these options correspond to the column heads in the output of the plain **show igmp statistics** command.
VPN	VPN: **vpn** *vpn-id* Display IGMP group information for interfaces in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show igmp statistics

     RX       RX                                                TX       TX
     GENERAL  GROUP  RX V1   RX V2   RX     RX       RX     GENERAL  GROUP  TX
VPN  QUERY    QUERY  REPORT  REPORT  LEAVE  UNKNOWN  ERROR  QUERY    QUERY  ERROR
-------------------------------------------------------------------------------
1    0        0      0       0       0      0        0      238      0      0
```

Operational Commands

igmp

show igmp groups

show igmp interface

how igmp summary

Related Topics

igmp, on page 235
show igmp groups, on page 822
show igmp interface, on page 823
show igmp summary, on page 826

show igmp summary

show igmp summary—Display information about the IGMP version and IGMP timers (on vEdge routers only).

show igmp summary [*igmp-property*]

Syntax Description

None	None: Display all IGMP version and timer information.
igmp-property	IGMP Properties: *igmp-property* Display information for a specific IGMP property. *group-property* can be one of the following: **last-member-query-count**, **last-member-query-response-time**, **querier-timeout**, **query-interval**, **query-response-time**, and **version**. Note that these options correspond to the column heads in the output of the plain **show igmp summary** command.

Command History

Release	Modification
14.3	Command introduced.

Output Fields

Output Field	Description
Last Member Query Count	How many group-specific query messages the router sends when it has receives a Leave Group message for a group before assuming that no members of the group remain on the interface. When no members appear to be present, the vEdge router removes the IGMP state for the group.
Last Member Query Response	How long the router waits, in seconds, to receive a response a group-specific query message. The default value is 1 second (1000 milliseconds). You cannot modify this value.
Other Querier Timeout	How long to wait for another IGMP querier to time out before assuming the role of querier. If IGMP on an interface or circuit detects another querier that has a lower IP than its own, it must become a non-querier on that network, and it starts watching for query messages from the querier. If the vEdge router has not received a query message from the querier in the Other Querier Timeout interval, it resumes the role of querier. The default other querier timeout value is 125 seconds. You cannot modify this value.
Query Interval	How often the router sends IGMP general query messages to solicit membership information. The default is 125 seconds. You cannot modify this value.
Query Response Interval	Maximum amount of time, in seconds, that the router waits to receive a response to a general query message. The default is 10 seconds. You cannot modify this value.
Version	IGMP version. Currently, vEdge routers run only IGMPv2.

Example

```
vEdge# show igmp summary
Version                     2
Query Interval              125 seconds
Query Response Interval     10 seconds
Last Member Query Response 1 seconds
Last Member Query Count     2
Other Querier Timeout       255 seconds
```

Operational Commands

igmp

show igmp groups

show igmp interface

how igmp statistics

Related Topics

igmp, on page 235
show igmp groups, on page 822
show igmp interface, on page 823
show igmp statistics, on page 824

show interface

show interface—Display information about IPv4 interfaces on a Cisco vEdge device.

show interface [**detail**] [*interface-name*] [**vpn** *vpn-id*]

Syntax Description

None	None: Display standard information about the interfaces on the Cisco vEdge device.
detail	Detailed Interface Information: Display detailed information about the interfaces (available only on vEdge routers).
interface-name	Specific Interface: Display information about a specific interface. On vEdge routers, *interface-name* can be a physical interface (**ge** *slot*/*port*), a subinterface or VLAN (**ge** *slot*/*port*.*vlan-number*), the interface corresponding to the system IP address (**system**), the management interface (typically, **eth0**), or a GRE tunnel (**gre** *number*). On vSmart controllers, *interface-name* can be an interface (**eth** *number*) or the interface corresponding to the system IP address (**system**).
vpn *vpn-id*	Specific VPN: Display information about interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The following are the fields in the show interface command output:

Output Fields	Description
1Duplex	Whether the interface is operating in duplex or simplex mode. This field does not apply to virtual interfaces, such as GRE, IRB, loopback, and system interfaces..
Encapsulation Type	Encapsulation configured on the interface with the encapsulation command.
Hardware Address	MAC address of the interface.
If Admin Status	Administrative status of the interface; that is, its status as a result of the interface's configuration. The status can be either Up or Down. By default, interfaces are administratively down, and you must include the no shutdown command in the interface's configuration to bring the interface up. An interface that is both administratively and operationally up is able to transmit and receive traffic. To bring down an interface administratively, include the shutdown command in the interface's configuration.
If Oper Status	Operational status of the interface; that is, its status as a result of operational factors. The status can be either Up or Down. An interface can be operationally up if it is Interface is administratively up, the interface link layer state is up, and the interface initialization has completed. An interface that is both administratively and operationally up is able to transmit and receive traffic. If the operational status is down, the interface is functionally down and is not able to transmit or receive any traffic.
MTU	MTU size for packets being send over the interface.
Port Type	Describes the port's function from the point of view of the overlay network. It can be one of the following: **loopback**—Loopback interface. The device's system IP address is listed as a loopback interface. **service**—Interface for data traffic. **transport**—Interface running a DTLS control session.
RX Packets and TX Packets	For GRE interfaces, these fields show counts of the data traffic received and transmitted on GRE tunnels. To display GRE keepalive traffic counts, use the show tunnel gre-keepalives command. To display all GRE tunnel statistics, use the show tunnel statistics gre command.
Speed	Speed of the interface, in megabits per second (Mbps). This field does not apply to virtual interfaces, such as GRE, IRB, loopback, and system interfaces.

Output Fields	Description
TCP MSS Adjust	Maximum segment size (MSS) of TCP SYN packets on the interface. For more information see tcp-mss-adjust.
Uptime	How long the interface has been up, in days, hours, minutes, and seconds.

The following are the additional fields included in the show interface detail command output:

- addr-type—Type of address configured on the interface, either IPv4 or IPv6, and how the address is configured, either dynamic or static.
- allow-service—Services allowed on the interface. For more information, see allow-service.
- arp-add-fails—Packets for which an ARP entry in the forwarding plane could not be created.
- bad-label—Packets dropped because of an invalid next-hop label record for a destination.
- cpu-policer-drops—Packets destined to the control plane dropped because they exceeded the CPU policer limit.
- dot1x-rx-pkts—802.1X packets received on the interface.
- dot1x-tx-pkts—802.1X packets transmitted on the interface.
- filter-drops—Packets dropped because of an implicit or explicit localized data policy (ACL) filter configuration.
- icmp-redirect-rx-drops—
- icmp-redirect-tx-drops—ICMP redirect packets dropped by the interface.
- if-addr, ip-address/broadcast-addr/secondary—Interface's primary unicast and broadcast addresses, and interface's secondary address, if one is configured.
- ifindex—Interface's SNMP index number.
- if-tracker-status—Whether interface tracking is enabled. For more information, see tracker.
- interface-disabled—Incoming packets dropped because the interface port is not enabled.
- mirror-drops—Fragmented packets that are being mirrored to a destination.
- route-lookup-fail—Packets that could not be forwarded because no route is present in the forwarding table (FIB).
- rx-arp-non-local-drops—Received ARP packets that do not match the destination IP address of any local IP address.
- rx-arp-replies—Received ARP replies
- rx-arp-rate-limit-drops—Currently, the software does not increment this counter.
- rx-arp-reply-drops—Currently, the software does not increment this counter.
- rx-arp-request-fail—Packets that could not be received because there is not corresponding MAC address.
- rx-arp-requests—Received ARP requests.
- rx-broadcast-pkts—Received broadcast packets.

- rx-drops—Received packets that were dropped.
- rx-errors—Received packets that were errored.
- rx-ip-ttl-expired—Received IP packets whose time-to-live value expired.
- rx-multicast-pkts—Received multicast packets.
- rx-non-ip-drops—Received packets other than IP or ARP packets that the interface dropped.
- rx-oversize-errors—Currently, the software does not increment this counter.
- rx-octets—Number of octets in received packets.
- rx-packets—Received packets.
- rx-policer-drops—Incoming packets dropped because of the rate exceeded the configured ingress policer rate.
- rx-policer-remark—Received packets remarked as the result of a policer.
- rx-pps—Receipt rate of packets, in packets per second.
- rx-replay-integrity-drops—Received packets dropped because the IPsec packet arrive outside of the anti-replay window or because the integrity check performed by ESP or AH failed. To view the configured anti-replay window, use the show security-info command. To modify the anti-replay window size, use the security ipsec replay-window configuration command.
- rx-undersize-errors—Currently, the software does not increment this counter.
- rx-wred-drops—Incoming packets dropped because of a RED drop profile associated with an interface queue. To configure a RED drop profile, use the drops option when configuring a QoS scheduler.
- shaping-rate—Traffic rate on the interface if rate is configured with the shaping-rate command to be less than the maximum rate.
- split-horizon-drops—BGP packets dropped as a result of split-horizon determination that the router was advertising a route back on the same interface from which it was learned.
- tx-arp-rate-limit-drops—Number of ARP packets generated by the forwarding plane that exceed the CPU rate limit, which is 16 ARP packets sent towards the CPU and 128 ARP packets send towards physical ports.
- tx-broadcast-pkts—Transmission rate of broadcast packets, in packets per second.
- tx-drops—Transmitted packets that were dropped.
- tx-errors—Transmitted packets that were errored.
- tx-icmp-mirrored-drops—ICMP redirect packets dropped by the system.
- tx-icmp-policer-drops—ICMP packets generated by the system that were dropped because of ICMP policer limits.
- tx-multicast-pkts—Transmitted multicast packets.
- tx-no-arp-drops—Packets dropped in the forwarding plane because of a missing ARP entry for a destination IP address.
- tx-octets—Number of octets in transmitted packets.

Example

```
vEdge# show interface
                                       IF      IF                                                                    TCP
                  AF                   ADMIN   OPER    ENCAP                                        SPEED           MSS                 RX       TX
VPN  INTERFACE  TYPE  IP ADDRESS       STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR              MBPS   DUPLEX  ADJUST  UPTIME      PACKETS
PACKETS
-------------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      ipv4  10.1.15.15/24    Up      Up      null   transport  1500  00:0c:29:7d:1e:fe  1000   full    1420    0:19:51:22  795641
857981
0    ge0/1      ipv4  10.1.17.15/24    Up      Up      null   service    1500  00:0c:29:7d:1e:08  1000   full    1420    0:19:42:43  5754     10
0    ge0/2      ipv4  -                Down    Up      null   service    1500  00:0c:29:7d:1e:12  1000   full    1420    0:19:51:27  5752     0
0    ge0/3      ipv4  10.0.20.15/24    Up      Up      null   service    1500  00:0c:29:7d:1e:1c  1000   full    1420    0:19:42:43  5763     9
0    ge0/6      ipv4  57.0.1.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:3a  1000   full    1420    0:19:42:43  5750     10
0    ge0/7      ipv4  10.0.100.15/24   Up      Up      null   service    1500  00:0c:29:7d:1e:44  1000   full    1420    0:19:48:22  7469     1346
0    system     ipv4  172.16.255.15/32 Up      Up      null   loopback   1500  00:00:00:00:00:00  0      full    1420    0:19:42:19  0        0
1    ge0/4      ipv4  10.20.24.15/24   Up      Up      null   service    1500  00:0c:29:7d:1e:26  1000   full    1420    0:19:42:40  13263    7653
1    ge0/5      ipv4  56.0.1.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:30  1000   full    1420    0:19:42:40  5730     8
512  eth0       ipv4  10.0.1.15/24     Up      Up      null   service    1500  00:50:56:00:01:0f  0      full    0       0:19:51:22  47033    31894
```

```
vEdge# show interface detail ge0/0
interface vpn 0 interface ge0/0 af-type ipv4
 if-admin-status         Up
 if-oper-status          Up
 if-addr
  ip-address     10.1.15.15/24
  broadcast-addr 10.1.15.255
  secondary      false
 encap-type              null
 port-type               transport
 ifindex                 1
 mtu                     1500
 hwaddr                  00:0c:29:7d:1e:fe
 speed-mbps              1000
 duplex                  full
 auto-neg                false
 pause-type              ""
 tcp-mss-adjust          1420
 uptime                  0:19:51:44
 allow-service           dhcp,dns,icmp
 rx-packets              795901
 rx-octets               146499972
 rx-errors               0
 rx-drops                2920
 tx-packets              858263
 tx-octets               147918066
 tx-errors               0
 tx-drops                0
 rx-pps                  11
 rx-kbps                 16
 tx-pps                  12
 tx-kbps                 17
 rx-arp-requests         44
 tx-arp-replies          52
 tx-arp-requests         2139
 rx-arp-replies          2085
 arp-add-fails           2
 rx-arp-reply-drops      0
 rx-arp-rate-limit-drops 0
 tx-arp-rate-limit-drops 0
```

```
rx-arp-non-local-drops  13
tx-arp-request-fail     0
tx-no-arp-drops         0
rx-ip-ttl-expired       0
interface-disabled      0
rx-policer-drops        0
rx-non-ip-drops         0
filter-drops            0
mirror-drops            0
cpu-policer-drops       0
tx-icmp-policer-drops   0
tx-icmp-mirrored-drops  0
split-horizon-drops     0
route-lookup-fail       0
bad-label               0
rx-multicast-pkts       7511
rx-broadcast-pkts       2997
tx-multicast-pkts       7437
tx-broadcast-pkts       88
num-flaps               1
shaping-rate            0
dot1x-tx-pkts           0
dot1x-rx-pkts           0
rx-policer-remark       0
```

Operational Commands

show interface arp-stats

show interface description

show interface errors

show interface packet-sizes

show interface port-stats

show interface queue

show interface statistics

show ipv6 interface

show wlan interfaces

Related Topics

show interface arp-stats, on page 833
show interface description, on page 835
show interface errors, on page 836
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface queue, on page 843
show interface statistics, on page 851
show ipv6 interface, on page 879
show wlan interfaces, on page 1039

show interface arp-stats

show interface arp-stats—Display the ARP statistics for each interface (on vEdge routers only).

show interface arp-stats [**vpn** *vpn-id*] [*interface-name*]

Syntax Description

None	None: Display standard information about ARP statistics for each interface.
interface-name	Specific Interface: Display ARP statistics for a specific interface.
vpn*vpn-id*	VPN: Display ARP statistics for interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The following are the fields included in the show interface arp-stats command output:

- rx-arp-requests/tx-arp-replies, RX Requests/Tx Replies—Number of ARP requests received on the interface, and number of replies sent to these ARP requests.
- tx-arp-requests/rx-arp-replies, TX Requests/Rx Replies—Number of ARP requests sent on the interface, and number of replies received to these ARP requests.
- arp-add-fails, Add Fails—Packets for which an ARP entry in the forwarding plane could not be created.
- rx-arp-reply-drops, RX Reply Drops—Currently, the software does not increment this counter.
- rx-arp-rate-limit-drops, RX Rate Limit Drops—Currently, the software does not increment this counter.
- tx-arp-rate-limit-drops, TX Rate Limit Drops—Number of ARP packets generated by the forwarding plane that exceed the CPU rate limit, which is 16 ARP packets sent towards the CPU and 128 ARP packets send towards physical ports.
- rx-arp-non-local-drops, RX Non-Local Drops—Received ARP packets that do not match the destination IP address of any local IP address.
- tx-arp-request-fail—Packets that could not be transmitted because an ARP request for the MAC address corresponding to the destination IP address was unable to retrieve a MAC address.
- tx-no-arp-drops, TX No ARP Drops—Packets dropped in the forwarding plane because of a missing ARP entry for a destination IP address.

Example

```
vEdge# show interface arp-stats
                                                                                                RX      RX           TX           RX          TX        TX
                     AF    RX        TX       TX        RX       ADD    REPLY   RATE-LIMIT   RATE-LIMIT  NON-LOCAL   REQUEST   NO-ARP
VPN  INTERFACE       TYPE  REQUESTS  REPLIES  REQUESTS  REPLIES  FAILS  DROPS   DROPS        DROPS       DROPS       FAIL      DROPS
-------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0           ipv4  0         16       255894    255786   1      0       0            0           11          0         0
0    ge0/1           ipv4  0         17       852858    0        0      0       0            0           0           0         0
0    ge0/2           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    ge0/3           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    ge0/4           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    ge0/5           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    ge0/6           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    ge0/7           ipv4  0         0        0         0        0      0       0            0           0           0         0
0    system          ipv4  -         -        -         -        -      -       -            -           -           -         -
0    vmanage_system  ipv4  -         -        -         -        -      -       -            -           -           -         -
1    ge0/7.23        ipv4  0         8        0         0        0      0       0            0           0           0         0
512  eth0            ipv4  -         -        -         -        -      -       -            -           -           -         -
vEdge# show interface arp-stats ge0/0 | tab
                                                                  RX      RX           TX           RX          TX        TX
                AF    RX        TX       TX        RX       ADD    REPLY   RATE-LIMIT   RATE-LIMIT  NON-LOCAL   REQUEST   NO-ARP
VPN  INTERFACE  TYPE  REQUESTS  REPLIES  REQUESTS  REPLIES  FAILS  DROPS   DROPS        DROPS       DROPS       FAIL      DROPS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      ipv4  0         16       255824    255716   1      0       0            0           11          0         0

vEdge# show interface arp-stats ge0/0
interface vpn 0 interface ge0/0 af-type ipv4
rx-arp-requests         0
tx-arp-replies          16
tx-arp-requests         255828
rx-arp-replies          255720
arp-add-fails           1
rx-arp-reply-drops      0
rx-arp-rate-limit-drops 0
tx-arp-rate-limit-drops 0
rx-arp-non-local-drops  11
tx-arp-request-fail     0
tx-no-arp-drops         0
Release Information
```

Operational Commands

show arp

show interface

show interface description

show interface errors

show interface packet-sizes

show interface port-stats

show interface queue

show interface statistics

Related Topics

show arp, on page 746
show interface, on page 827
show interface description, on page 835
show interface errors, on page 836
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface queue, on page 843
show interface statistics, on page 851

show interface description

show interface description—Display information information, including the configured interface description.

show interface description [**vpn** *vpn-id* [*interface-name*]

Options

None	None: Display information about all interfaces, including any configured interface description.
interface-name	Specific Interface: Display information about a specific interface.
vpn *vpn-id*	VPN: Display information about interfaces in a specific VPN.

Command History

Release	Modification
14.3	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show interface description

                                    IF      IF
                                    ADMIN   OPER
VPN  INTERFACE  IP ADDRESS          STATUS  STATUS  DESCRIPTION
------------------------------------------------------------------------
0    ge0/0      10.1.15.15/24       Up      Up      Internet connection
0    ge0/1      10.1.17.15/24       Up      Up      -
0    ge0/2      -                   Down    Up      -
```

```
0     ge0/3       10.0.20.15/24     Up      Up      -
0     ge0/6       57.0.1.15/24      Up      Up      -
0     ge0/7       10.0.100.15/24    Up      Up      -
0     system      172.16.255.15/32  Up      Up      -
```

Operational Commands

description

show interface

show interface arp-stats

show interface errors

show interface packet-sizes

show interface port-stats

show interface queue

show interface statistics

Related Topics

description, on page 178
show interface, on page 827
show interface arp-stats, on page 833
show interface errors, on page 836
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface queue, on page 843
show interface statistics, on page 851

show interface errors

show interface errors—Display error statistics for interfaces (on vEdge routers only).

show interface errors [**vpn** *vpn-id*] [*interface-name*]

Syntax Description

None	None: Display standard information about errors for each interface.
interface-name	Specific Interface: Display error information for a specific interface.
vpn*vpn-id*	VPN: Display error information for interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

Following are explanations of the output fields:

- arp-add-fails—Packets for which an ARP entry in the forwarding plane could not be created.
- bad-label—Packets dropped because of an invalid next-hop label record for a destination.
- cpu-policer-drops—Packets destined to the control plane dropped because they exceeded the CPU policer limit.
- filter-drops—Packets dropped because of an implicit or explicit localized data policy (ACL) filter configuration.
- fragment-df-drops—Packets dropped because their size is larger than the configure MTU, if the Don't Fragment bit is set.
- interface-disabled—Incoming packets dropped because the interface port is not enabled.
- ip-fwd-null-hop—Packets that could not be forwarded because the next-hop address was invalid or the next hop was unavailable.
- ip-fwd-unknown-nh-type—Packets dropped because the next-hop type was unknown.
- mirror-drops—Fragmented packets that are being mirrored to a destination.
- port-disabled-rx—Incoming packets dropped because the interface port is not enabled.
- port-disabled-tx—Outgoing packets dropped because the interface port is not enabled.
- route-lookup-fail—Packets that could not be forwarded because no route is present in the forwarding table (FIB).
- rx-arp-cpu-rate-limit-drops—ARP reply packets dropped because the number of packets exceeded the CPU rate limit.
- rx-arp-non-local-drops—Received ARP packets that do not match the destination IP address of any local IP address.
- rx-arp-rate-limit-drops—Currently, the software does not increment this counter.
- rx-arp-reply-drops—Currently, the software does not increment this counter.
- rx-dmac-filter-drops—Received packets that do not match the destination MAC address corresponding to the Layer 3 interface.
- rx-fcs-align-errors— In MIPS-based Cisco vEdge devices, like Cisco vEdge 1000 or Cisco vEdge 2000, this counter is the sum of all dropped error packets. The errors may be caused due to:
  - FCS (frame check sequence) errors
  - alignment errors

These errors are detected at the hardware layer but are not related to DMAC (Destination MAC) filter drop or lack of room in the receiver FIFO.

- rx-implicit-acl-drops—Received packets dropped because of an implicit route policy (access list). Router tunnel interfaces also have implicit ACLs, which are also referred to as services. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On vEdge routers, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN. To enable the logging of the headers of packets dropped because they do not match a service configure with an allow-service command, configure policy implicit-acl-logging (on vEdge routers only).
- rx-inb-errors—Currently, the software does not increment this counter.
- rx-interface-not-found—Packets dropped because of an invalid VLAN tag.
- rx-ip-errors—Received packets whose IP or Thernet header could not be parsed.
- rx-ip-ttl-expired—Received IP packets whose time-to-live value expired.
- rx-non-ip-drops—Received packets other than IP or ARP packets that the interface dropped.
- rx-oversize-errors—Currently, the software does not increment this counter.
- rx-policer-drops—Incoming packets dropped because of the rate exceeded the configured ingress policer rate.
- rx-replay-integrity-drops—Received packets dropped because the IPsec packet arrive outside of the anti-replay window or because the integrity check performed by ESP or AH failed. To view the configured anti-replay window, use the show security-info command. To modify the anti-replay window size, use the security ipsec replay-window configuration command.
- rx-undersize-errors—Currently, the software does not increment this counter.
- rx-wred-drops—Incoming packets dropped because of a RED drop profile associated with an interface queue. To configure a RED drop profile, use the drops option when configuring a QoS scheduler.
- split-horizon-drops—BGP packets dropped as a result of split-horizon determination that the router was advertising a route back on the same interface from which it was learned.
- tx-arp-rate-limit-drops—Number of ARP packets generated by the forwarding plane that exceed the CPU rate limit, which is 16 ARP packets sent towards the CPU and 128 ARP packets send towards physical ports.
- tx-arp-request-fail—Packets that could not be transmitted because an ARP request for the MAC address corresponding to the destination IP address was unable to retrieve a MAC address.
- tx-collision-drops—Packets dropped because the interface attempted to send packets at the same time.
- tx-fragment-drops—Packets dropped because of issues related to fragmentation, such as when a fragment exceeds the MTU size when the DF bit is set and when issues occur in reassembling packets after fragmentation.
- tx-fragment-needed—Packets requiring fragmentation because they are larger than the interface's MTU.
- tx-icmp-mirrored-drops—ICMP redirect packets dropped by the system.

- tx-icmp-policer-drops—ICMP packets generated by the system that were dropped because of ICMP policer limits.
- tx-interface-disabled—Currently, the software does not increment this counter.
- tx-no-arp-drops—Packets dropped in the forwarding plane because of a missing ARP entry for a destination IP address.
- tx-underflow-pkts—Packets dropped during transmission because packet data was not made available to the TX FIFO in time. This situation can result in FCS errors on the receiving side.

Example

```
vEdge# show interface errors
interface vpn 0 interface ge0/0
arp-add-fails           25
rx-arp-reply-drops      0
rx-arp-rate-limit-drops 2
tx-arp-rate-limit-drops 0
rx-arp-non-local-drops  183
tx-arp-request-fail     0
tx-no-arp-drops         1
rx-ip-ttl-expired       0
rx-ip-errors            0
interface-disabled      0
rx-policer-drops        0
rx-non-ip-drops         144
filter-drops            0
mirror-drops            0
cpu-policer-drops       0
split-horizon-drops     0
route-lookup-fail       0
bad-label               0
rx-dmac-filter-drops    44
rx-drop-pkts            0
rx-drop-octets          0
rx-wred-drops           0
rx-interface-not-found  0
rx-inb-errors           0
rx-oversize-errors      0
rx-fcs-align-errors     0
rx-undersize-errors     0
tx-underflow-pkts       0
tx-collision-drops      0
...
```

Operational Commands

show interface

show interface arp-stats

show interface description

show interface packet-sizes

show interface port-stats

show interface queue

show interface statistics

Related Topics

show interface, on page 827
show interface arp-stats, on page 833
show interface description, on page 835
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface queue, on page 843
show interface statistics, on page 851

show interface packet-sizes

show interface packet-sizes—Display packet size information for each interface (on MIPS routers only).

show interface packet-sizes [**vpn** *vpn-id*] [*interface-name*]

Syntax Description

None	None: Display standard packet size information for each interface.
interface-name	Specific Interface: *interface-name* Display packet size information for a specific interface.
vpn*vpn-id*	VPN: Display packet size information for interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show interface packet-sizes
                                                                                                                                 RX                                                                   TX
TX      TX      TX
                    RX                          RX PKT  RX PKT  RX PKT  PKT                                             PKT
PKT     PKT     PKT
                RX PKT  PKT     RX PKT   RX PKT     SIZE     SIZE     SIZE      SIZE    TX PKT  TX PKT  TX PKT    TX PKT    SIZE
SIZE    SIZE    SIZE
                SIZE    SIZE    SIZE 65  SIZE 128   256      512      1024      GT      SIZE    SIZE    SIZE 65   SIZE 128  256
512     1024    GT      NUM
VPN  INTERFACE  64      LT 64   127      255        511      1023     1518      1518    64      LT 64   127       255       511
1023    1518    1518    FLAPS
-------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      36054   0       267476   17125160   260171   196894   1857213   0       36396   36396   18471527  18471527  0
0       0       0       0
0    ge0/2      0       0       0        0          0        0        0         0       0       0       0         0         0
0       0       0       0
```

```
0     ge0/4       0        0       0         0          0        0        0        0       0       0       0         0          0
0       0       0        0
0     ge0/5       0        0       0         0          0        0        0        0       0       0       0         0          0
0       0       0        0
0     ge0/6       0        0       0         0          0        0        0        0       0       0       0         0          0
0       0       0        0
0     ge0/7       0        0       0         0          0        0        0        0       0       0       0         0          0
0       0       0        0
0     system      -        -       -         -          -        -        -        -       -       -       -         -          -
-       -       -        0
1     ge0/1       445095   0       4350156   611392     214008   143019   1454843  0       10091   10091   17272     17272      0
0       0       0        1
1     ge0/3       165631   0       2348140   1235047    321523   188447   3458507  0       673392  673392  396377    396377     0
0       0       0        0
512   mgmt0       -        -       -         -          -        -        -        -       -       -       -         -          -
-
```

Operational Commands

show interface

show interface arp-stats

show interface description

show interface errors

show interface port-stats

show interface queue

show interface statistics

Related Topics

show interface, on page 827
show interface arp-stats, on page 833
show interface description, on page 835
show interface errors, on page 836
show interface port-stats, on page 841
show interface queue, on page 843
show interface statistics, on page 851

show interface port-stats

show interface port-stats—Display interface port statistics (on MIPS vEdge routers only).

show interface port-stats [**vpn** *vpn-id*] [*interface-name*]

Syntax Description

None	None: Display standard interface port statistics.
interface-name	Specific Interface: Display port statistics for a specific interface.
vpn*vpn-id*	VPN: vpn vpn-id Display port statistics for a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show interface port-stats
                        RX
                 RX     DMAC    RX    RX      RX     RX                 RX        RX FCS  RX         TX         TX         TX
    TX                     TX        TX
                PAUSE   FILTER  DROP  DROP    WRED   INTERFACE  RX INB  OVERSIZE  ALIGN   UNDERSIZE  UNDERFLOW  COLLISION  PAUSE
  FRAGMENTS  TX          FRAGMENT  WRED   LLQ
VPN  INTERFACE  PKTS    DROPS    PKTS  OCTETS  DROPS  NOT FOUND  ERRORS  ERRORS    ERRORS  ERRORS     PKTS       DROPS      PKTS
   NEEDED     FRAGMENTS  DROPS     DROPS  DROPS
-------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      0       975     0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    ge0/2      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    ge0/4      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    ge0/5      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    ge0/6      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    ge0/7      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
0    system     -       -       -     -       -      -          -       -         -       -          -          -          -
    -          -          -         -      -
1    ge0/1      0       0       0     0       0      0          0       0         0       0          0          0          0
    0          0          0         -      0
1    ge0/3      0       27      0     0       0      0          0       0         0       0          0          0          0
    0          0          34        -      0
512  mgmt0      -       -       -     -       -      -          -       -         -       -          -          -          -
    -          -          -         -      -
```

Operational Commands

show interface

show interface arp-stats

show interface description

show interface errors

show interface packet-sizes

show interface queue

show interface statistics

Related Topics

show interface, on page 827
show interface arp-stats, on page 833
show interface description, on page 835

show interface errors, on page 836
show interface packet-sizes, on page 840
show interface queue, on page 843
show interface statistics, on page 851

show interface queue

show interface queue—Display interface queue statistics (on vEdge routers only).

show interface queue [**vpn** *vpn-id*] [*interface-name*]

Syntax Description

None	None: Display standard interface queue statistics.
interface-name	Specific Interface: Display interface queue statistics for a specific interface.
vpn*vpn-id*	VPN: Display interface queue statistics for interfaces in a specific VPN.

Note The queue drop details are dispalyed when you pass commands, **`show interface statistics`** and **`show interface port-stats`**.

Command History

Release	Modification
14.1	Command introduced.
19.1	Added attributes to the command output: queue-depth, max-depth, avg-queue, queue-pps, queue-drop-pps

Output Fields

QNUM

Queue number. Hardware vEdge routers have 8 queues, numbered 0 through 7. From 17.2.7 Release onwards, vEdge Cloud software router have 8 queues, numbered 0 through 7.

The remaining output fields are self-explanatory.

Example

```
vedge# show interface queue ge0/0
```

```
                                    TAIL     TAIL     RED      RED                                                    QUEUE
                  AF                QUEUED   DROP     DROP     DROP     DROP     TX       TX       QUEUE  MAX     AVG    QUEUE  DROP
VPN  INTERFACE    TYPE  QNUM  QUEUED PACKETS  PACKETS  BYTES    PACKETS  BYTES    PACKETS  BYTES    DEPTH  DEPTH   QUEUE  PPS    PPS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0        ipv4  0     29654  0        0        0        0        29654    9763602  0      0       0      1      0
                         1     0      0        0        0        0        0        0        0      0       0      0      0
                         2     0      0        0        0        0        0        0        0      0       0      0      0
                         3     0      0        0        0        0        0        0        0      0       0      0      0
                         4     0      0        0        0        0        0        0        0      0       0      0      0
                         5     0      0        0        0        0        0        0        0      0       0      0      0
                         6     0      0        0        0        0        0        0        0      0       0      0      0
                         7     0      0        0        0        0        0        0        0      0       0      0      0
```

Operational Commands

show interface

show interface arp-stats

show interface description

show interface errors

show interface packet-sizes

show interface port-stats

show interface statistics

Related Topics

show interface, on page 827
show interface arp-stats, on page 833
show interface description, on page 835
show interface errors, on page 836
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface statistics, on page 851

show interface sfp detail

show interface sfp detail—Display detailed SFP status and digital diagnostic information for bytes 0 through 95 of an SPF A0 section, as described in SFF-8472 (on vEdge routers only). This command also provides information about the types of fiber supported, the distance the SFP can drive, and the wavelength used by the SFP. The output of this command is useful for diagnosing issues with a troublesome SFP link.

show interface sfp detail [*interface-name*]

Syntax Description

None	None: Display detailed information for all interfaces in the router.
interface-name	Interface Name: *interface-name* Display detailed information for the specific interface.

Command History

Release	Modification
16.1	Command introduced.

Output Fields

The output fields are drawn from the SFP addresses listed below. Not all fields are valid or make sense for all SFP types.

Table 17: SFP Types

Field Name	Value	SFP Address
Physical identifier	Physical device identifier	A0.0-1
Connector type	Values such as LC, SC, and RJ45	A0.2
Transceiver compliance (compatibility)	List of compliance values	A0.3 to A0.10, A0.36
Encoding	Values such as 8b10b and 64b66b	A0.11
Nominal speed	Speed, in bps	A0.12, A0.66 to A0.67
Rate select options	Rate identifiers	A0.13
Single-mode fiber link length	Length, in km	A0.14 to 15
50-µm multimode (OM2) fiber link length	Length, in meters	A0.16
65-µm multimode (OM1) fiber link length	Length, in meters	A0.17
50-µm multimode (OM4) active cable/copper link length	Length, in meters	A0.18
50-µm multimode (OM3) fiber link length	Length, in meters	A0.19
Vendor name	16-byte ASCII string	A0.20 to A0.35
Vendor OUI	3-byte hexadecimal string	A0.37 to A0.39
Vendor part number	16-byte ASCII string	A0.40 to A0.55
Vendor revision	4-byte ASCII string	A0.56 to A0.59
Vendor serial number	16-byte ASCII string	A0.68 to A0.83
Date code	Date string as yymmddll, where l is the lot code	A0.84 to A0.91

Field Name	Value	SFP Address
Laser wavelength	Value or compliance string, in nm	A0.60 to A0.61
Feature options	List of bits, as strings	A0.64 to A0.65
Diagnostic monitoring options	List of bits, as strings	A0.92
Enhanced options	List of bits, as strings	A0.93
SFP compliance level	Compliance specification string	A0.94

Fiber SFPs

Example

```
vEdge-1000# show interface sfp detail ge0/5
sfp detail ge0/5
 Present                 Yes
 Physical identifier     SFP/SFP+
 Connector type          "LC (Lucent connector)"
 Transceiver compliance  "1000 Base-SX"
 Encoding                8b/10b
 Nominal speed           "1.20 Gbps"
 Rate select options     Unspecified
 62.5um OM1 fiber length 270m
 50um OM2 fiber length   550m
 Laser wavelength        850nm
 Vendor name             "AVAGO           "
 Vendor OUI              00:17:6a
 Vendor number           "AFBR-5710PZ     "
 Vendor revision         "    "
 Vendor serial number    "AM13412D2Z7     "
 Date code               2013/10/11
 Feature options
  Loss of signal        Yes
  Signal detect         No
  Tx fault              Yes
  Tx disable            Yes
  Rate select           No
  Tunable wavelength    No
  Rx decision threshold No
  Linear receive output No
  Power level           1
  Cooled laser          No
  Timing type           "Internal retimer"
  Paged A2 access       No
 Digital diagnostics
  Supported No
 Enhanced options
  Soft rate select control          No
  Application select control        No
  Soft rate select control/monitor  No
  Soft Rx LOS monitor               No
  Soft Tx fault monitor             No
  Soft Tx disable control/monitor   No
  Supports all alarms/warning flags No
```

Examples

For a 1-Gigabit Ethernet fiber SFP:

```
vEdge-2000# show interface sfp detail ge0/7
sfp detail ge0/7
 Present                 Yes
 Physical identifier     SFP/SFP+
 Connector type          "LC (Lucent connector)"
 Transceiver compliance  "10G Base-SR"
 Encoding                64b/66b
 Nominal speed           "10.30 Gbps"
 Rate select options     Unspecified
 62.5um OM1 fiber length 30m
 50um OM2 fiber length   80m
 50um OM3 fiber length   300m
 Laser wavelength        850nm
 Vendor name             "FINISAR CORP.   "
 Vendor OUI              00:90:65
 Vendor number           "FTLX8571D3BCL   "
 Vendor revision         "A   "
 Vendor serial number    "ARN13Z1         "
 Date code               2014/5/28
 Feature options
  Loss of signal        Yes
  Signal detect         No
  Tx fault              Yes
  Tx disable            Yes
  Rate select           No
  Tunable wavelength    No
  Rx decision threshold No
  Linear receive output No
  Power level           1
  Cooled laser          No
  Timing type           "Internal retimer"
  Paged A2 access       No
 Digital diagnostics
  Supported              Yes
  Calibration type       Internal
  Power measurement type "Average input power"
 Enhanced options
  Soft rate select control          No
  Application select control        No
  Soft rate select control/monitor  No
  Soft Rx LOS monitor               Yes
  Soft Tx fault monitor             Yes
  Soft Tx disable control/monitor   Yes
  Supports all alarms/warning flags Yes
```

For a 10-Gigabit Ethernet fiber SFP:

```
vEdge-2000# show interface sfp detail ge0/3
sfp detail ge0/3
 Present                  Yes
 Physical identifier      SFP/SFP+
 Connector type           "LC (Lucent connector)"
 Transceiver compliance   "10G Base-LR"
 Transceiver compliance   "1000 Base-LX"
 Encoding                 64b/66b
 Nominal speed            "10.30 Gbps"
 Rate select options      "8/4/2G Rx Rate_Select only"
 Single mode fiber length "10.00 km"
 Laser wavelength         1310nm
 Vendor name              "FINISAR CORP.   "
 Vendor OUI               00:90:65
 Vendor number            "FTLX1471D3BCV   "
 Vendor revision          "A   "
 Vendor serial number     "ASK273Z         "
 Date code                2014/11/12
```

```
 Feature options
  Loss of signal        Yes
  Signal detect         No
  Tx fault              Yes
  Tx disable            Yes
  Rate select           Yes
  Tunable wavelength    No
  Rx decision threshold No
  Linear receive output No
  Power level           1
  Cooled laser          No
  Timing type           "Internal retimer"
  Paged A2 access       No
 Digital diagnostics
  Supported              Yes
  Calibration type       Internal
  Power measurement type "Average input power"
 Enhanced options
  Soft rate select control          Yes
  Application select control        No
  Soft rate select control/monitor  Yes
  Soft Rx LOS monitor               Yes
  Soft Tx fault monitor             Yes
  Soft Tx disable control/monitor   Yes
  Supports all alarms/warning flags Yes
```

Copper SFPs

For a 1-Gigabit Ethernet copper SFP:

```
vEdge1000# show interface sfp detail ge0/4
sfp detail ge0/4
 Present                Yes
 Physical identifier    SFP/SFP+
 Connector type         Unknown/unspecified
 Transceiver compliance "1000 Base-T"
 Encoding               8b/10b
 Nominal speed          "1.20 Gbps"
 Rate select options    Unspecified
 Copper min link length 100m
 Vendor name            "FINISAR CORP.   "
 Vendor OUI             00:90:65
 Vendor number          "FCLF-8521-3     "
 Vendor revision        "A   "
 Vendor serial number   "PS21BN1         "
 Date code              2014/7/8
 Feature options
  Loss of signal        No
  Signal detect         No
  Tx fault              No
  Tx disable            Yes
  Rate select           No
  Tunable wavelength    No
  Rx decision threshold No
  Linear receive output No
  Power level           1
  Cooled laser          No
  Timing type           "Internal retimer"
  Paged A2 access       No
 Digital diagnostics
  Supported No
 Enhanced options
  Soft rate select control          No
  Application select control        No
```

```
Soft rate select control/monitor  No
Soft Rx LOS monitor               No
Soft Tx fault monitor             No
Soft Tx disable control/monitor   No
Supports all alarms/warning flags No
```

Operational Commands

show hardware alarms

show hardware environment

show hardware inventory transceiver

show hardware temperature-thresholds

show interface sfp diagnostic

Related Topics

show hardware alarms, on page 812
show hardware environment, on page 813
show hardware inventory, on page 816
show hardware temperature-thresholds, on page 820
show interface sfp diagnostic, on page 849

show interface sfp diagnostic

show interface sfp diagnostic—Display SFP diagnostic information for fiber-based SFPs only (on vEdge routers only). This data is taken from bytes in the SFP A2 page, as described in SFF-8472. This section is not available for copper RJ45 SFPs.

The data for this output is stored in the A2 page of the SFP, and it contains minimum/maximum threshold parameters for laser transmitters and receivers, as well as dynamic run-time data values. This data page also might contain calibration data if the devices were externally calibrated. In this show command, the calibration data is used, if populated; however, it is not specifically be displayed.

show interface sfp diagnostic [*interface-name*]

Syntax Description

None	None: Display SFP diagnostic information for all interfaces in the router.
interface-name	Interface Name: Display SFP diagnostic information for the specific interface.

Command History

Release	Modification
16.1	Command introduced.

Output Fields

The output fields are drawn from the SFP addresses listed below. Not all fields are valid or make sense for all SFP types.

The following information is displayed for SFP diagnostics. Measurement information is presented as floating-point data.

Threshold and measurement data are all floating point data and are specified for accuracy relative to the source data. Measurement units are included in the value label.

In addition to allowing current measurements to be display, each of the following measurements has associated flag status indicating whether the measurement is in or out of alarm or warning state. This data is sourced from A2.112-117 SFP data.

Based on options declared to be supported by the SFP, several bit-based statuses are included in the display output. These include items such as select, transmit disable state, and receive loss-of-signal state, and are from A2.110.

Measurement	High Warning	High Alarm	Low Warning	Low Alarm	Current
Optical laser temperature	A2.44 to A2.45	A2.40 to A2.41	A2.46 to A2.47	A2.42 to A2.43	A2.106 to A2.107
Optical TEC current	A2.52 to A2.53	A2.48 to A2.49	A2.54 to A2.55	A2.50 to A2.51	A2.108 to A2.109
Receive power	A2.36 to A2.37	A2.32 to A2.33	A2.38 to A2.39	A2.34 to A2.35	A2.104 to A2.105
SFP temperature	A2.4 to A2.5	A2.0 to A2.1	A2.6 to A2.7	A2.2 to A2.3	A2.96 to A2.97
Supply voltage	A2.12 to A2.13	A2.8 to A2.9	A2.14 to A2.15	A2.10 to A2.11	A2.98 to A2.99
Transmit bias current	A2.20 to A2.21	A2.16 to A2.17	A2.22 to A2.23	A2.18 to A2.19	A2.100 to A2.101

Example

For a 1-Gigabit Ethernet copper SFP:

```
vEdge-1000# show interface sfp diagnostic ge0/3
sfp diagnostic ge0/3
 Present               Yes
 Diagnostics supported Yes
 SFP control/status
  Data ready         Yes
  Rx LOS             Yes
  Tx fault           No
  Soft rate select 0 No
  Soft rate select 1 No
  Rate select 0      No
  Rate select 1      No
  Soft Tx disable    No
  Tx disable         Yes

                         LOW       LOW       HIGH      HIGH     CURRENT
MEASUREMENT        UNIT  ALARM     WARNING   WARNING   ALARM    VALUE
-------------------------------------------------------------------------
```

```
Laser temperature  C     0.000    0.000    0.000    0.000   0.000
Rx power           mW    0.010    0.016    1.585    1.778   0.000
SFP temperature    C     -13.000  -8.000   73.000   78.000  32.023
Supply voltage     V     2.900    3.000    3.600    3.700   3.250
TEC current        mA    0.000    0.000    0.000    0.000   0.000
Tx bias current    mA    7.000    12.000   80.000   85.000  0.000
Tx power           mW    0.159    0.199    1.259    1.585   0.012


                   LOW    LOW      HIGH     HIGH
MEASUREMENT        ALARM  WARNING  WARNING  ALARM
-------------------------------------------------
Laser temperature  N      N        N        N
Rx power           Y      Y        N        N
SFP temperature    N      N        N        N
Supply voltage     N      N        N        N
TEC current        N      N        N        N
Tx bias current    Y      Y        N        N
Tx power           Y      Y        N        N
```

Operational Commands

show hardware alarms

show hardware environment

show hardware inventory transceiver

show hardware temperature-thresholds

show interface sfp detail

Related Topics

show hardware alarms, on page 812
show hardware environment, on page 813
show hardware inventory, on page 816
show hardware temperature-thresholds, on page 820
show interface sfp detail, on page 844

show interface statistics

show interface statistics—Display interface statistics (on vEdge routers only).

show interface statistics [**vpn** *vpn-id*] [*interface-name*]**show interface detail statistics** [**diff**] [**interface** *interface-name*] [**vpn** *vpn-id*]

Syntax Description

None	None: Display standard interface statistics. Interface traffic rates are computed every 10 seconds.
diff	Statistics Changes: Display the changes in statistics since you last issued the **show interface statistics** command.
interface-name	Interface Name: Display interface statistics for a specific interface.

vpn*vpn-id*	VPN: Display interface statistics for interfaces in a specific VPN.

Command History

Release	Modification
14.1	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show interface statistics
                                                                                                                                                                                                PPPOE  PPPOE  DOT1X
  DOT1X
                    RX       RX        RX      RX     TX       TX        TX      TX     RX   RX    TX   TX    TX     RX     TX
  RX
VPN  INTERFACE  PACKETS  OCTETS    ERRORS  DROPS  PACKETS  OCTETS    ERRORS  DROPS  PPS  Kbps  PPS  Kbps  PKTS   PKTS   PKTS
  PKTS
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0       147389   43326584  0       360    158925   42023634  0       0      12   18    13   16    0      0      0
  0
0    ge0/1       391      54500     0       0      5        210       0       0      0    0     0    0     0      0      0
  0
0    ge0/2       391      54500     0       0      0        0         0       0      0    0     0    0     0      0      0
  0
0    ge0/3       396      54800     0       5      5        210       0       0      0    0     0    0     0      0      0
  0
0    ge0/6       391      54500     0       0      4        168       0       0      0    0     0    0     0      0      0
  0
0    ge0/7       993      139010    0       89     586      233244    0       0      0    0     0    0     0      0      0
  0
0    system      0        0         0       0      0        0         0       0      0    0     0    0     0      0      0
  0
1    ge0/4       1524     148328    0       1      1175     97382     0       0      0    0     0    0     0      0      0
  0
1    ge0/5       391      54500     0       0      4        168       0       0      0    0     0    0     0      0      0
  0
512  eth0        7021     859885    0       0      4194     608754    0       0      5    5     3    5     0      0      0
  0
```

```
vSmart# show interface statistics

                    RX       RX        RX      RX     TX       TX        TX      TX     RX
RX    TX    TX
VPN  INTERFACE  PACKETS  OCTETS    ERRORS  DROPS  PACKETS  OCTETS    ERRORS  DROPS  PPS
Kbps  PPS  Kbps
-------------------------------------------------------------------------------------------------------------------------------
0    eth0        8014     910140    0       0      5664     1032739   0       0      0    0
     0    0
0    eth1        131517   24476039  0       0      154517   37400773  0       0      12
18    14   28
0    eth3        -        -         -       -      -        -         -       -      -    -
     -    -
0    system      0        0         0       0      0        0         0       0      0    0
     0    0
512  eth2        414      56320     0       0      7        558       0       0      0    0
     0    0
```

Operational Commands

show interface

show interface arp-stats

show interface buffer-pool-status

show interface description

show interface errors

show interface packet-sizes

show interface port-stats

show interface queue

Related Topics

show interface, on page 827
show interface arp-stats, on page 833
show system buffer-pool-status, on page 1011
show interface description, on page 835
show interface errors, on page 836
show interface packet-sizes, on page 840
show interface port-stats, on page 841
show interface queue, on page 843

show ip dns-snoop

Display details of a fully qualified domain name (FQDN) and its corresponding IP address mapping information.

The DNS snooping agent (DSA) maintains an "IP cache" table of fully qualified domain names (FQDN) and their corresponding IP addresses. The command displays the complete information in this table (**all** option), or details for specific FQDN's (**pattern** option) or IP addresses (**address** option).

(for Cisco IOS XE SD-WAN devices)

Command Syntax

show ip dns-snoop {**address** *ip-address* | **all** **pattern** *pattern*}

Syntax Description

address *ip-address*	Display details for a specific IP address in the DSA IP cache table.
all	Display details for all IP addresses in the DSA IP cache table.
pattern *pattern*	Display details for a specific FQDN in the DSA IP cache table, matching a text pattern.

Command Mode

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2	Command introduced.

Examples

Example

```
Device# show ip dns-snoop all
IP Address            Client(s)      Expire      RegexId      Dirty Match
------------------------------------------------------------------------------
192.168.0.1           0x1 992        0xef270000  0x00         cisco\.com
```

show ip fib

To display the IPv4 entries in the local forwarding table (on Cisco vEdge routers only), use the **show ip fib** command in privileged EXEC mode.

show ip fib [**vpn** *vpn-id*] [*ipv4-prefix/length*] [**tloc** { **color** *color* | **tloc-ip** *ip-address* }]

Syntax Description

	None: List standard information about the IPv4 entries in the forwarding table.
ipv4-prefix/length	Specific Prefix: List the forwarding table entry for the specified IPv4 prefix.
tloc [**color** *color* | **tloc-ip** *ip-address*]	TLOC-Specific Entries: Display forwarding table IPv4 entries for specific TLOCs.
vpn *vpn-id*	VPN-Specific Routes: List only the forwarding table IPv4 entries for the specified VPN.

Command History

Release	Modification
14.1	Command introduced.
Cisco SD-WAN Release 20.9.1	This command was modified. Support was added to display interservice replicated route VPN.

Examples

The following is a sample output from the **show ip fib vpn** command that shows the replicated route VPNs:

```
vEdge# show ip fib vpn 102
                          NEXTHOP     NEXTHOP   NEXTHOP  NEXTHOP  SA
VPN     PREFIX            IF NAME     ADDR      LABEL    VPN      INDEX    TLOC IP
  COLOR
-------------------------------------------------------------------------------------------------
102     10.0.100.0/24     ge0/4.105   -         -        -        -        -
   -
102     10.51.51.16/32    ge0/4.105   -         -        -        -        -
   -
102     10.61.61.0/24     -           -         -        6        -        -
   -
```

Examples

The following is a sample output from the **show ip fib** command:

```
vEdge# show ip fib
                          NEXTHOP     NEXTHOP          NEXTHOP  SA

VPN     PREFIX            IF NAME     ADDR             LABEL    INDEX    TLOC IP
 COLOR
-------------------------------------------------------------------------------------------------
0       10.0.5.0/24       ge0/0       10.1.15.13       -        -        -
 -
0       10.0.12.0/24      ge0/0       10.1.15.13       -        -        -
 -
0       10.0.20.0/24      ge0/3       -                -        -        -
 -
0       10.0.20.15/32     ge0/3       -                -        -        -
 -
0       10.0.100.0/24     ge0/7       -                -        -        -
 -
0       10.0.100.15/32    ge0/7       -                -        -        -
 -
0       10.1.14.0/24      ge0/0       10.1.15.13       -        -        -
 -
0       10.1.15.0/24      ge0/0       -                -        -        -
 -
0       10.1.15.15/32     ge0/0       -                -        -        -
 -
0       10.1.16.0/24      ge0/0       10.1.15.13       -        -        -
 -
0       10.1.17.0/24      ge0/1       -                -        -        -
 -
0       10.1.17.15/32     ge0/1       -                -        -        -
 -
0       57.0.1.0/24       ge0/6       -                -        -        -
 -
0       57.0.1.15/32      ge0/6       -                -        -        -
 -
0       172.16.255.15/32  system      -                -        -        -
 -
1       10.2.2.0/24       ipsec       10.0.5.11        2        13       172.16.255.11
 lte
1       10.2.3.0/24       ipsec       10.0.5.21        2        15       172.16.255.21
 lte
1       10.20.24.0/24     ge0/4       -                -        -        -
 -
1       10.20.24.15/32    ge0/4       -                -        -        -
 -
1       10.20.25.0/24     ipsec       10.1.16.16       2        16       172.16.255.16
 lte
1       56.0.1.0/24       ge0/5       -                -        -        -
 -
1       56.0.1.15/32      ge0/5       -                -        -        -
```

```
 -
1       60.0.1.0/24          ipsec       10.1.16.16       2        16       172.16.255.16
 lte
1       61.0.1.0/24          ipsec       10.1.16.16       2        16       172.16.255.16
 lte
1       172.16.255.112/32    ipsec       10.0.5.21        2        15       172.16.255.21
 lte
1       172.16.255.112/32    ipsec       10.0.5.11        2        13       172.16.255.11
 lte
1       172.16.255.117/32    ge0/4       10.20.24.17      -        -        -
 -
1       172.16.255.118/32    ipsec       10.1.16.16       2        16       172.16.255.16
 lte
512     10.0.1.0/24          eth0        -                -        -        -
 -
512     10.0.1.15/32         eth0        -                -        -        -
 -
```

Examples

The following is a sample output from the **show ip routes** command:

```
vEdge# show ip routes
Codes Proto-sub-type:
  IA -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                                      PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP

VPN     PREFIX               PROTOCOL   SUB TYPE  IF NAME     ADDR             VPN      TLOC
 IP           COLOR             ENCAP  STATUS
-------------------------------------------------------------------------------------------
0       10.0.5.0/24          ospf        -         ge0/0       10.1.15.13       -        -
              -                  -      F,S
0       10.0.12.0/24         ospf        -         ge0/0       10.1.15.13       -        -
              -                  -      F,S
0       10.0.20.0/24         connected   -         ge0/3       -                -        -
              -                  -      F,S
0       10.0.100.0/24        connected   -         ge0/7       -                -        -
              -                  -      F,S
0       10.1.14.0/24         ospf        -         ge0/0       10.1.15.13       -        -
              -                  -      F,S
0       10.1.15.0/24         ospf        -         ge0/0       -                -        -
              -                  -      -
0       10.1.15.0/24         connected   -         ge0/0       -                -        -
              -                  -      F,S
0       10.1.16.0/24         ospf        -         ge0/0       10.1.15.13       -        -
              -                  -      F,S
0       10.1.17.0/24         connected   -         ge0/1       -                -        -
              -                  -      F,S
0       57.0.1.0/24          connected   -         ge0/6       -                -        -
              -                  -      F,S
0       172.16.255.15/32     connected   -         system      -                -        -
              -                  -      F,S
1       10.2.2.0/24          omp         -         -           -                -
172.16.255.11    lte                ipsec  F,S
1       10.2.3.0/24          omp         -         -           -                -
172.16.255.21    lte                ipsec  F,S
1       10.20.24.0/24        ospf        -         ge0/4       -                -        -
              -                  -      -
```

```
1      10.20.24.0/24       connected  -         ge0/4       -                -        -
            -                  -      F,S
1      10.20.25.0/24       omp        -         -           -                -
172.16.255.16    lte              ipsec  F,S
1      56.0.1.0/24         connected  -         ge0/5       -                -        -
            -                  -      F,S
1      60.0.1.0/24         omp        -         -           -                -
172.16.255.16    lte              ipsec  F,S
1      61.0.1.0/24         omp        -         -           -                -
172.16.255.16    lte              ipsec  F,S
1      172.16.255.112/32   omp        -         -           -                -
172.16.255.11    lte              ipsec  F,S
1      172.16.255.112/32   omp        -         -           -                -
172.16.255.21    lte              ipsec  F,S
1      172.16.255.117/32   ospf       E2        ge0/4       10.20.24.17      -        -
            -                  -      F,S
1      172.16.255.118/32   omp        -         -           -                -
172.16.255.16    lte              ipsec  F,S
512    10.0.1.0/24         connected  -         eth0        -                -        -
            -                  -      F,S
```

Examples

The following is a sample output from the **show interface** command:

```
vEdge# show interface

                                    IF      IF
                TCP
                                    ADMIN   OPER    ENCAP
SPEED           MSS                  RX       TX
VPN  INTERFACE  IP ADDRESS          STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR
MBPS   DUPLEX  ADJUST  UPTIME       PACKETS  PACKET
------------------------------------------------------------------------------------------
0    ge0/0      10.1.15.15/24      Up      Up      null   transport  1500  00:0c:29:7d:1e:fe
  10     full    0       0:02:38:45  96014    95934
0    ge0/1      10.1.17.15/24      Up      Up      null   service    1500  00:0c:29:7d:1e:08
  10     full    0       0:02:38:45  226      4
0    ge0/2      -                  Down    Up      null   service    1500  00:0c:29:7d:1e:12
  10     full    0       0:02:38:45  226      0
0    ge0/3      10.0.20.15/24      Up      Up      null   service    1500  00:0c:29:7d:1e:1c
  10     full    0       0:02:38:45  230      4
0    ge0/6      57.0.1.15/24       Up      Up      null   service    1500  00:0c:29:7d:1e:3a
  10     full    0       0:02:38:45  226      4
0    ge0/7      10.0.100.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:44
  10     full    0       0:02:37:09  906      577
0    system     172.16.255.15/32   Up      Up      null   loopback   1500  00:00:00:00:00:00
  10     full    0       0:02:25:04  0        0
1    ge0/4      10.20.24.15/24     Up      Up      null   service    1500  00:0c:29:7d:1e:26
  10     full    0       0:02:25:22  1152     951
1    ge0/5      56.0.1.15/24       Up      Up      null   service    1500  00:0c:29:7d:1e:30
  10     full    0       0:02:25:22  216      4
512  eth0       10.0.1.15/24       Up      Up      null   service    1500  00:50:56:00:01:0f
  1000   full    0       0:02:38:38  6198     3
```

Examples

The following is a sample output from the **show omp routes** command:

```
vEdge# show omp routes
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
```

```
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
U   -> TLOC unresolved
```

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP
	COLOR	ENCAP	PREFERENCE				
1	10.2.2.0/24	172.16.255.19	103	2	C,I,R	installed	172.16.255.11
	lte	ipsec	-				
		172.16.255.20	103	2	C,R	installed	172.16.255.11
	lte	ipsec	-				
1	10.2.3.0/24	172.16.255.19	81	2	C,I,R	installed	172.16.255.21
	lte	ipsec	-				
		172.16.255.20	81	2	C,R	installed	172.16.255.21
	lte	ipsec	-				
1	10.20.24.0/24	0.0.0.0	32769	2	C,Red,R	installed	172.16.255.15
	lte	ipsec	-				
		0.0.0.0	32779	2	C,Red,R	installed	172.16.255.15
	lte	gre	-				
1	10.20.25.0/24	172.16.255.19	77	2	C,I,R	installed	172.16.255.16
	lte	ipsec	-				
		172.16.255.20	73	2	C,R	installed	172.16.255.16
	lte	ipsec	-				
1	56.0.1.0/24	0.0.0.0	32769	2	C,Red,R	installed	172.16.255.15
	lte	ipsec	-				
		0.0.0.0	32779	2	C,Red,R	installed	172.16.255.15
	lte	gre	-				
1	60.0.1.0/24	172.16.255.19	78	2	C,I,R	installed	172.16.255.16
	lte	ipsec	-				
		172.16.255.20	72	2	C,R	installed	172.16.255.16
	lte	ipsec	-				
1	61.0.1.0/24	172.16.255.19	79	2	C,I,R	installed	172.16.255.16
	lte	ipsec	-				
		172.16.255.20	71	2	C,R	installed	172.16.255.16
	lte	ipsec	-				
1	172.16.255.112/32	172.16.255.19	82	2	C,I,R	installed	172.16.255.21
	lte	ipsec	-				
		172.16.255.19	104	2	C,I,R	installed	172.16.255.11
	lte	ipsec	-				
		172.16.255.20	82	2	C,R	installed	172.16.255.21
	lte	ipsec	-				
		172.16.255.20	104	2	C,R	installed	172.16.255.11
	lte	ipsec	-				

Operation Commands

ip route

ipv6 route

route-consistency-check

show interface

show ip routes

show ipv6 fib

show omp routes

Related Topics

ip route, on page 267
ipv6 route, on page 275
route-consistency-check, on page 429
show interface, on page 827
show ip routes, on page 865
show ipv6 fib, on page 878
show omp routes, on page 914

show ip mfib oil

show ip mfib oil—Display the list of outgoing interfaces from the Multicast Forwarding Information Base (MFIB) (on vEdge routers only).

show ip mfib oil show ip mfib oil [*group-number*] [*group-address*] [*source-address*] [**mcast-oil-list** *number*]

Syntax Description

None	None: List standard information about outgoing interfaces from the MFIB.
group-number group-address source-address **mcast-oil-list**	Specific Information: List more specific information from the MFIB.

Command History

Release	Modification
14.2	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show ip mfib oil

VPN                                OIL         OIL REMOTE
ID   GROUP       SOURCE   INDEX  INTERFACE   SYSTEM
-------------------------------------------------------------
1    224.0.1.39  0.0.0.0
1    224.0.1.40  0.0.0.0
1    225.0.0.1   0.0.0.0  0      -           172.16.255.14
```

Operational Commands

show ip mfib summary

show ip mfib stats

Related Topics

show ip mfib summary, on page 861
show ip mfib stats, on page 860

show ip mfib stats

show ip mfib stats—Display packet transmission and receipt statistics for active entries in the Multicast Forwarding Information Base (MFIB) (on vEdge routers only). Packet rates are computed every 10 seconds.

Command Syntax

show ip mfib stats

Syntax Description

None

Output Fields

Rx Policy Drop, Tx Policy Drop

The number of inbound or outbound packets dropped as the result of applying a policy. The remaining output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.
16.3	Added Rx Policy Drop and Tx Policy Drop fields to command output.

Examples

```
vEdge# show ip mfib stats

                                                                RX       RX       TX       TX                              RX       TX       INVALID
                          RX     RX       TX     TX       CTRL  PACKETS  OCTETS   PACKETS  OCTETS   AVG                RPF      POLICY   POLICY   OIL      TX
VPN  GROUP       SOURCE   PKTS   OCTETS   PKTS   OCTETS   PKTS  (PPS)    (KBPS)   (PPS)    (KBPS)   REPLICATION        FAILURE  DROP     DROP     FAILURE  FAILURE
-------------------------------------------------------------------------------------------------------------------------------------------------------------
1    224.0.1.39  0.0.0.0  0      0        0      0        0     0        0        0        0        0.00               0        0        0        0        0
1    224.0.1.40  0.0.0.0  0      0        0      0        0     0        0        0        0        0.00               0        0        0        0        0
```

Command History

show ip mfib oil

show ip mfib summary

show multicast topology

Related Topics

show ip mfib oil, on page 859
show ip mfib summary, on page 861
show multicast topology, on page 900

show ip mfib summary

show ip mfib summary—Display a summary of all active entries in the Multicast Forwarding Information Base (MFIB) (on vEdge routers only).

show ip mfib summary show ip mfib summary [*group-number*] [*group-address*] [*source-address*] [**num-service-oils** | **num-tunnel-oils** | **upstream-if** | **upstream-tunnel**]

Syntax Description

None	None: List standard information about outgoing interfaces from the MFIB.
[*group-number* | *group-address* | *source-address*] [**num-service-oils | num-tunnel-oils | upstream-if |upstream-tunnel**]	Specific Information: List more specific information from the MFIB.

Command History

Release	Modification
14.2	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
vEdge# show ip mfib summary

 NUM      NUM
VPN                      UPSTREAM  UPSTREAM  SERVICE  TUNNEL
ID   GROUP       SOURCE   IF        TUNNEL    OILS     OILS
-----------------------------------------------------------------
1    224.0.1.39  0.0.0.0  ---       0.0.0.0   0        0
1    224.0.1.40  0.0.0.0  ---       0.0.0.0   0        0
1    225.0.0.1   0.0.0.0  ge0/4     0.0.0.0   0        1
```

Operational Commands

show ip mfib oil

show ip mfib stats

Related Topics

show ip mfib oil, on page 859
show ip mfib stats, on page 860

show ip nat filter

show ip nat filter—Display the NAT translational filters (on vEdge routers only).

show ip nat filter [**nat-vpn** *vpn-id*]

Syntax Description

nat-vpn *vpn-id*	VPN Identifier: Identifier of the VPN that traffic destined for the NAT is coming from.

Command History

Release	Modification
14.2	Command introduced.

Output Fields

The output fields are self-explanatory.

Example

```
VEdge# show ip nat filter nat-vpn
                              PRIVATE     PRIVATE     PRIVATE  PRIVATE  PUBLIC      PUBLIC      PUBLIC  PUBLIC

NAT  NAT                    SOURCE      DEST        SOURCE   DEST     SOURCE      DEST        SOURCE  DEST    FILTER       IDLE
       OUTBOUND  OUTBOUND  INBOUND  INBOUND
VPN  IFNAME  VPN  PROTOCOL  ADDRESS     ADDRESS     PORT     PORT     ADDRESS     ADDRESS     PORT    PORT    STATE
TIMEOUT     PACKETS   OCTETS    PACKETS  OCTETS
-------------------------------------------------------------------------------------------------------------------------------
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  4697     4697     10.1.15.15  10.1.14.14  64931   64931   established
0:00:00:41  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  14169    14169    10.1.15.15  10.1.14.14  28467   28467   established
0:00:00:44  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  21337    21337    10.1.15.15  10.1.14.14  44555   44555   established
0:00:00:47  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  28505    28505    10.1.15.15  10.1.14.14  40269   40269   established
0:00:00:50  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  39513    39513    10.1.15.15  10.1.14.14  31859   31859   established
0:00:00:53  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  46681    46681    10.1.15.15  10.1.14.14  1103    1103    established
0:00:00:56  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  57176    57176    10.1.15.15  10.1.14.14  38730   38730   established
0:00:00:35  1         98        1         98
0    ge0/0   0    icmp      10.1.15.15  10.1.14.14  64600    64600    10.1.15.15  10.1.14.14  33274   33274   established
0:00:00:38  1         98        1         98
0    ge0/0   0    udp       10.1.15.15  10.0.5.19   12346    12346    10.1.15.15  10.0.5.19   64236   12346   established
0:00:19:59  38        8031      23        5551
0    ge0/0   0    udp       10.1.15.15  10.0.12.20  12346    12346    10.1.15.15  10.0.12.20  64236   12346   established
0:00:19:59  36        7470      23        5551
0    ge0/0   0    udp       10.1.15.15  10.0.12.22  12346    12346    10.1.15.15  10.0.12.22  64236   12346   established
0:00:19:59  679       598771    434       92925
0    ge0/0   0    udp       10.1.15.15  10.1.14.14  12346    12346    10.1.15.15  10.1.14.14  64236   12346   established
0:00:19:59  34        3825      9         3607
0    ge0/0   0    udp       10.1.15.15  10.1.14.14  12346    12350    10.1.15.15  10.1.14.14  64236   12350   established
0:00:19:59  38        5472      23        3634
0    ge0/0   0    udp       10.1.15.15  10.1.16.16  12346    12346    10.1.15.15  10.1.16.16  64236   12346   established
0:00:19:59  38        5472      23        3634
```

Operational Commands

show ip nat interface

show ip nat interface-statistics

Related Topics

nat, on page 346
show ip nat interface, on page 863
show ip nat interface-statistics, on page 864

show ip nat interface

show ip nat interface—List the interfaces on which NAT is enabled and the NAT translational filters on those interfaces (on vEdge routers only).

Command Syntax

show ip nat interface [**nat-vpn** *vpn-id*] [*nat-parameter*]

Syntax Description

None	List information about all NAT interfaces in all VPNs.

Table 18: Syntax Description

nat-parameter	Specific NAT Interface Parameter: List specific NAT interface information. *nat-parameter* can be one of the following, which correspond to the column heads in the command output: **fib-filter-count**, **filter-count**, **filter-type**, **ip**, **mapping-type**, and **number-ip-pools**.
nat-vpn *vpn-id*	Specific VPN: List information for NAT interface only for the specified VPN.

Command History

Release	Modification
14.2.	Command introduced.

Output Fields

In the Map Type field, all SD-WAN NAT types are endpoint-independent.

The other output fields are self-explanatory.

Output

```
vEdge# show ip nat interface
                                                                  FIB                    NUMBER

                                                          FILTER  FILTER                 IP
VPN  IFNAME     MAP TYPE             FILTER TYPE          COUNT   COUNT   IP             POOLS
```

```
-------------------------------------------------------------------------------------------------------------
1    natpool1   endpoint-independent  address-port-restricted  0       0       10.15.1.4/30    4
1    natpool7   endpoint-independent  address-port-restricted  0       0       10.21.26.15/32  1
1    natpool8   endpoint-independent  address-port-restricted  0       0       10.21.27.15/32  1
1    natpool9   endpoint-independent  address-port-restricted  0       0       10.21.28.15/32  1
1    natpool10  endpoint-independent  address-port-restricted  0       0       10.21.29.15/32  1
1    natpool11  endpoint-independent  address-port-restricted  0       0       10.21.30.15/32  1
1    natpool12  endpoint-independent  address-port-restricted  0       0       10.21.31.15/32  1
1    natpool13  endpoint-independent  address-port-restricted  0       0       10.21.32.15/32  1
1    natpool14  endpoint-independent  address-port-restricted  0       0       10.21.33.15/32  1
1    natpool15  endpoint-independent  address-port-restricted  0       0       10.21.34.15/32  1
1    natpool16  endpoint-independent  address-port-restricted  0       0       10.21.35.15/32  1
```

Operational Commands

nat

show ip nat filter

show ip nat interface-statistics

Related Topics

nat, on page 346
show ip nat filter, on page 862
show ip nat interface-statistics, on page 864

show ip nat interface-statistics

show ip nat interface-statistics—List packet, NAT, and ICMP statistics for the interfaces on which NAT is enabled (on vEdge routers only).

Command Syntax

show ip nat filter interface-statistics [**nat-vpn** *vpn-id*]

Syntax Description

Table 19: Syntax Description

None	Display statistics for all interfaces in all VPNs.
nat-vpn *vpn-id*	VPN: Display statistics for the interfaces in the specified VPN.

Command History

Release	Modification
14.2.	Command introduced.

```
vEdge# show ip nat interface-statistics
                                                NAT   NAT     NAT     NAT                                  INBOUND
                        NAT     NAT     NAT
              NAT       NAT       NAT     NAT     MAP   FILTER  FILTER  STATE  NAT      OUTBOUND  INBOUND  ICMP
NAT         NAT         MAP     MAP     FILTER    NAT MAP
              OUTBOUND  INBOUND  ENCODE  DECODE  ADD   ADD     LOOKUP  CHECK  POLICER  ICMP      ICMP     ERROR    NAT
FRAGMENTS   UNSUPPORTED NO      CANNOT  MAP       IP POOL
VPN  IFNAME  PACKETS   PACKETS  FAIL    FAIL    FAIL  FAIL    FAIL    FAIL   DROPS    ERROR     ERROR    DROPS    FRAGMENTS
```

```
FAIL       PROTO       PORTS  XLATE   MISMATCH  EXHAUSTED
-------------------------------------------------------------------------------------------------------------------
1    ge0/4   0         0        0       0     0       0       0       0       0       0       0       0
0          0           0      0       0         0
1    ge0/5   0         0        0       0     0       0       0       0       0       0       0       0
0          0           0      0       0         0

vEdge# show ip nat interface-statistics | notab
ip nat interface-statistics nat-vpn 1 nat-ifname natpool1
 nat-outbound-packets      0
 nat-inbound-packets       0
 nat-encode-fail           0
 nat-decode-fail           0
 nat-map-add-fail          0
 nat-filter-add-fail       0
 nat-filter-lookup-fail    0
 nat-state-check-fail      0
 nat-policer-drops         0
 outbound-icmp-error       0
 inbound-icmp-error        0
 inbound-icmp-error-drops  0
 nat-fragments             0
 nat-fragments-fail        0
 nat-unsupported-proto     0
 nat-map-no-ports          0
 nat-map-cannot-xlate      0
 nat-filter-map-mismatch   0
 nat-map-ip-pool-exhausted 0
...
```

Operational Commands

nat

show ip nat filter

show ip nat interface-statistics

Related Topics

nat, on page 346
show ip nat filter, on page 862
show ip nat interface, on page 863

show ip routes

To display the IPv4 entries in the local route table, use the **show ip routes** command in privileged EXEC mode. On Cisco vSmart controllers, the route table incorporates forwarding information.

show ip routes [**vpn** *vpn-id*] [*ipv4-address*] [*ipv4prefix/length*] [**bgp**] [**connected**] [**gre**] [**nat**] [**natpool-inside**] [**natpool-outside**] [**omp**] [**ospf**] [**static**] [**summary** [**protocol** *protocol*]] [**detail**]

Syntax Description

	None: List standard information about the entries in the local IPv4 route table.
detail	Detailed Information: List detailed information about the entries in the local IPv4 route table.

ipv4-address *ipv4prefix /length* **vpn** *vpn-id*	IP Address or Route Prefix: List route information for the specified route prefix. If you omit the prefix length, you must specify a VPN identifier so that the Cisco SD-WAN software can find the route that best matches the prefix.
nat	NAT Routes: List routes learned from static routes that are advertised to a different VPN (configured using the **ip route vpn** command).
natpool-inside **natpool-outside**	NAT Pool Routes: List routes learned from NAT pools that are advertised by OMP (*natpool-inside*) and routes learned from the service side (*natpool-outside*) for Cisco vEdge devices acting as NATs.
protocol	Routes Learned from a Protocol or Connected Networks: List routes learned from one or more specific protocols—bgp, connected, gre, omp, ospf, and static. The protocol static includes both routes that are statically configured on the local device as well as routes learned from a DHCP server if one or more interfaces in VPN 0 are configured to learn their IP addresses via DHCP.
summary [**summary** *protocol]*	Summary of Routes: List summary information about the IP routes in the route table or about routes learned from the specified protocol. Protocol can be bgp, connected, omp, ospf, or static.
vpn *vpn-id*	VPN-Specific Routes: List only the route table entries for the specified VPN.

Note Any BFD event (up/down) for a vEdge peer will result in withdrawal and re-installation of all OMP routes learnt from the remote vEdge, consequently, re-setting the uptime as well.

Command History

Release	Modification
14.1	Command introduced.
16.3	Added support for displaying NAT-related routes.
17.1	Display omp-tag and ospf-tag fields in detailed output.
17.2	Renamed natpool-omp and natpool-service options to natpool-inside and natpool-outside.
Cisco SD-WAN Release 20.9.1	This command was modified. Support was added to display interservice VPN route replication in detailed output.

Examples

The following is a sample output from the **show ip route vpn** command:

```
vEdge# show ip route vpn 102
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
```

```
  B -> blackhole, R -> recursive, L -> import

                                                PROTOCOL  NEXTHOP     NEXTHOP   NEXTHOP

VPN    PREFIX              PROTOCOL         SUB TYPE  IF NAME     ADDR      VPN      TLOC
IP  COLOR   ENCAP  STATUS
------------------------------------------------------------------------------------------
102    10.0.100.0/24       static           -         -           -         101      -
    -       -      F,S,L
102    10.10.25.44/32      static           -         -           -         101      -
    -       -      F,S,L
102    10.10.25.45/32      static           -         -           -         101      -
    -       -      F,S,L
102    192.168.25.0/24     connected        -         ge0/4.102   -         -        -
    -       -      F,S
```

The following is a sample output from the **show ip routes** command:

```
vEdge# show ip routes
Codes Proto-sub-type:
  IA -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive
                                    PROTOCOL  NEXTHOP  NEXTHOP          NEXTHOP

VPN  PREFIX              PROTOCOL   SUB TYPE  IF NAME  ADDR             VPN      TLOC IP
       COLOR             ENCAP  STATUS
-------------------------------------------------------------------------------------------
0    0.0.0.0/0          static     -         ge0/0    10.1.15.13       -        -
       -                -      F,S
0    10.0.20.0/24        connected  -         ge0/3    -                -        -
       -                -      F,S
0    10.0.100.0/24       connected  -         ge0/7    -                -        -
       -                -      F,S
0    10.1.15.0/24        connected  -         ge0/0    -                -        -
       -                -      F,S
0    10.1.17.0/24        connected  -         ge0/1    -                -        -
       -                -      F,S
0    10.57.1.0/24        connected  -         ge0/6    -                -        -
       -                -      F,S
0    172.16.255.15/32    connected  -         system   -                -        -
       -                -      F,S
1    10.1.17.15/32       nat        -         ge0/1    -                0        -
       -                -      F,S
1    10.20.24.0/24       ospf       -         ge0/4    -                -        -
       -                -      -
1    10.20.24.0/24       connected  -         ge0/4    -                -        -
       -                -      F,S
1    10.20.25.0/24       omp        -         -        -                -        172.16.255.16
    lte              ipsec  F,S
1    10.56.1.0/24        connected  -         ge0/5    -                -        -
       -                -      F,S
1    10.60.1.0/24        omp        -         -        -                -        172.16.255.16
    lte              ipsec  F,S
1    10.61.1.0/24        omp        -         -        -                -        172.16.255.16
    lte              ipsec  F,S
512  10.0.1.0/24         connected  -         eth0     -                -        -
       -                -      F,S
```

The following is a sample output from the **show ip routes summary** command:

```
vEdge# show ip routes summary

     ADDRESS
VPN  FAMILY   PROTOCOL   RECEIVED  INSTALLED
-----------------------------------------------
0    ipv4     connected  6         6
0    ipv4     static     0         0
0    ipv4     ospf       5         4
0    ipv4     bgp        0         0
0    ipv4     omp        0         0
1    ipv4     connected  3         3
1    ipv4     static     0         0
1    ipv4     ospf       0         0
1    ipv4     bgp        1         1
1    ipv4     omp        4         4
512  ipv4     connected  1         1
512  ipv4     static     0         0
```

The following is a sample output from the **show ip routes detail** command:

```
vEdge# show ip routes 172.16.255.112/32 detail
Codes Proto-sub-type:
IA -> ospf-inter-area,
E1 -> ospf-external1, E2 -> ospf-external2,
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
e -> bgp-external, i -> bgp-internal
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive

-------------------------------------------
VPN 1 PREFIX 172.16.255.112/32
-------------------------------------------
proto ospf
proto-sub-type E2
distance 110
metric 20
uptime 2:17:37:59
omp-tag 100
ospf-tag 20
nexthop-ifname ge0/0
nexthop-addr 10.2.2.12
status F,S
```

Related Topics

ip route, on page 267
route-consistency-check, on page 429
show ip fib, on page 854
show ipv6 routes, on page 885
show omp routes, on page 914

show ipsec ike inbound-connections

show ipsec ike inbound-connections—Display information about the IKE sessions that remote IKE peers have established to the local router (on vEdge routers only).

Command Syntax

show ipsec ike inbound-connections

show ipsec ike inbound-connections *source-ip-address* [*source-port* [*destination-ip-address* [*destination-port*]]] [(**ciphersuite** *suite* | **new-key-hash** *hash* | **new-spi** *spi* | **old-key-hash** *hash* | **old-spi** *spi*)]]]]

Syntax Description

	None: Display information for all the IKE sessions that have been established to the local router.
source-ip-address [*source-port*[*destination-ip-address*[*destination-port*]]] [(**ciphersuite** *suite* | **new-key-hash** *hash* |**new-spi** *spi* |**old-key-hash** *hash* | **old-spi** *spi*)]]]]	Specific IKE-Enabled IPsec Tunnel Connection: Display information for a specific IKE-enabled IPsec tunnel.

Command History

Release	Modification
17.2	Command introduced.

Example

For the following example, the output of the **show ipsec ike inbound-connections** command on the vEdge1 router shows the IKE-enabled IPsec tunnel connection that originates on the vEdge2 router, whose tunnel source IP address is 10.1.16.16. The command output on the vEdge2 router shows the connection from vEdge1, whose tunnel source IP address is 10.1.15.15.

```
vEdge1# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.1/30
  tunnel-source      10.1.15.15
  tunnel-destination 10.1.16.16
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$jr37xShEUPZF2zuiZFpTqqBHSlCHVX1XLut1o62mh7c=
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge2# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.2/30
  tunnel-source      10.1.16.16
  tunnel-destination 10.1.15.15
  ike
   version      2
```

```
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$/O+yus2zpknCbyK5YUfZMQehghSsXCXzfRpc9bj6YsY=
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge1# show ipsec ike inbound-connections

SOURCE                                SOURCE  DEST                                 DEST    NEW     OLD     CIPHER           NEW        OLD
IP                                    PORT    IP                                   PORT    SPI     SPI     SUITE            KEY HASH   KEY HASH
-------------------------------------------------------------------------------------------------------------------------------------------------
10.1.16.16                            4500    10.1.15.15                           4500    257     256     aes256-cbc-sha1  ****01be   ****a0df

vEdge2# show ipsec ike inbound-connections

SOURCE                                SOURCE  DEST                                 DEST    NEW     OLD     CIPHER           NEW        OLD
IP                                    PORT    IP                                   PORT    SPI     SPI     SUITE            KEY HASH   KEY HASH
-------------------------------------------------------------------------------------------------------------------------------------------------
10.1.15.15                            4500    10.1.16.16                           4500    257     256     aes256-cbc-sha1  ****4485   ****48e3
```

Related Topics

show ipsec ike outbound-connections, on page 870
show ipsec ike sessions, on page 872

show ipsec ike outbound-connections

show ipsec ike outbound-connections—Display information about the IKE sessions that the local router has established to remote IKE peers (on vEdge routers only).

Command Syntax

show ipsec ike outbound-connections

show ipsec ike outbound-connections *source-ip-address* [*source-port* [*destination-ip-address* [*destination-port*] [*spi*]]] [(**ciphersuite** *suite* | **key-hash** *hash* | **tunnel-mtu** *mtu*)]]]]

Syntax Description

	None: Display information for all the IKE sessions that have been established to remote IKE peers.
source-ip-address [*source-port* [*destination-ip-address*] [*destination-port*] [*spi*]]] [(**ciphersuite** *suite* |**tunnel-mtu** *mtu*)]]]]	Specific IKE-Enabled IPsec Tunnel Connection: Display information for a specific IKE-enabled IPsec tunnel.

Command History

Release	Modification
17.2	Command introduced.

Examples

On the vEdge1 router, the output of the **show ipsec ike outbound-connections** command shows the IKE-enabled IPsec tunnel connection that originates from the local router, whose tunnel source IP address is 10.1.15.15. The command output on the vEdge2 router shows the connection originating from that router, 10.1.15.15.

```
vEdge1# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.1/30
  tunnel-source      10.1.15.15
  tunnel-destination 10.1.16.16
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$jr37xShEUPZF2zuiZFpTqqBHSlCHVX1XLut1o62mh7c=
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge2# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.2/30
  tunnel-source      10.1.16.16
  tunnel-destination 10.1.15.15
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$/O+yus2zpknCbyK5YUfZMQehghSsXCXzfRpc9bj6YsY=
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge1# show ipsec ike outbound-connections

SOURCE                              SOURCE  DEST                              DEST           CIPHER
IP                                  PORT    IP                                PORT    SPI    SUITE            KEY HASH  TUNNEL MTU
-------------------------------------------------------------------------------------------------------------------------------------
10.1.15.15                          4500    10.1.16.16                        4500    257    aes256-cbc-sha1  ****55b5  1418

vEdge2# show ipsec ike outbound-connections

SOURCE                              SOURCE  DEST                              DEST           CIPHER
IP                                  PORT    IP                                PORT    SPI    SUITE            KEY HASH  TUNNEL MTU
-------------------------------------------------------------------------------------------------------------------------------------
10.1.16.16                          4500    10.1.15.15                        4500    257    aes256-cbc-sha1  ****cf49  1418
```

Related Topics

show ipsec ike inbound-connections, on page 868
show ipsec ike sessions, on page 872

show ipsec ike sessions

show ipsec ike sessions—Display information about the IKE sessions on the router (on vEdge routers only).

Command Syntax

show ipsec ike sessions

Syntax Description

None

Command History

Release	Modification
17.2	Command introduced.

Examples

```
vEdge1# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.1/30
  tunnel-source      10.1.15.15
  tunnel-destination 10.1.16.16
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$jr37xShEUPZF2zuiZFpTqqBHSlCHVX1XLut1o62mh7c=
    !
   !
  !
  ipsec
   rekey         14400
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge2# show running-config vpn 1 interface ipsec1
vpn 1
 interface ipsec1
  ip address 10.1.1.2/30
  tunnel-source      10.1.16.16
  tunnel-destination 10.1.15.15
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        16
   authentication-type
    pre-shared-key
     pre-shared-secret $8$/O+yus2zpknCbyK5YUfZMQehghSsXCXzfRpc9bj6YsY=
    !
   !
  !
  ipsec
   rekey         14400
```

```
   replay-window 32
   cipher-suite  aes256-cbc-sha1
  !
  no shutdown
 !
!

vEdge1# show ipsec ike sessions

     IF                          SOURCE              DEST

VPN  NAME    VERSION  SOURCE IP   PORT    DEST IP     PORT  INITIATOR SPI     RESPONDER SPI     CIPHER SUITE     DH GROUP        STATE        UPTIME

-------------------------------------------------------------------------------------------------------------------------------------------------------------
1    ipsec1  2        10.1.15.15  4500    10.1.16.16  4500  ccb1a7c4a770752e  6179faf6884bfd38  aes256-cbc-sha1  16 (MODP-4096)  ESTABLISHED
0:00:08:38

vEdge2# show ipsec ike sessions

     IF                          SOURCE              DEST

VPN  NAME    VERSION  SOURCE IP   PORT    DEST IP     PORT  INITIATOR SPI     RESPONDER SPI     CIPHER SUITE     DH GROUP        STATE        UPTIME

-------------------------------------------------------------------------------------------------------------------------------------------------------------
1    ipsec1  2        10.1.16.16  4500    10.1.15.15  4500  ccb1a7c4a770752e  6179faf6884bfd38  aes256-cbc-sha1  16 (MODP-4096)  ESTABLISHED
0:00:09:23
```

Related Topics

show ipsec ike inbound-connections, on page 868
show ipsec ike outbound-connections, on page 870

show ipsec inbound-connections

show ipsec inbound-connections—Display information about IPsec tunnels that originate on remote routers (on vEdge routers only).

Command Syntax

show ipsec inbound-connections

show ipsec inbound-connections *local-tloc-address* [*local-color* [*remote-tloc-address* [*remote-color* [(**dest-ip** |**dest-port** | **source-ip** | **source-port**)]]]]

Syntax Description

	None: Display information for all the IPsec connections that originate on the vEdge router. The tunnel connections are listed in order according to the local TLOC address.
local-tloc-address [*local-color* [*remote-tloc-address*[*remote-color* [(**dest-ip** |**dest-port** |**source-ip** |**source-port**)]]]]	Specific Tunnel Connection: Display information for a specific IPsec connection.

Command History

Release	Modification
14.1	Command introduced.

Release	Modification
15.2	Command renamed from **show tunnel inbound-connections**.
16.2	Display negotiated encryption algorithm in command output.

Examples

```
vEdge# show 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
-------------------------------------------------------------------------------------------------------------------------------------------
10.0.5.11                       12406   10.1.15.15                    12406   172.16.255.11    lte              172.16.255.15    lte
  AES-GCM-256           8
10.1.14.14                      12406   10.1.15.15                    12406   172.16.255.14    lte              172.16.255.15    lte
  AES-GCM-256           8
10.1.16.16                      12406   10.1.15.15                    12406   172.16.255.16    lte              172.16.255.15    lte
  AES-GCM-256           8
10.0.5.21                       12406   10.1.15.15                    12406   172.16.255.21    lte              172.16.255.15    lte
  AES-GCM-256           8
```

Related Topics

show ipsec local-sa, on page 874
show ipsec outbound-connections, on page 875

show ipsec local-sa

show ipsec local-sa—Display security association information for the IPsec tunnels that have been created for local TLOCs (on vEdge routers only).

Command Syntax

show ipsec local-sa

show ipsec local-sa *tloc-address* [*color* [**spi** [(**auth-key-hash** |**encrypt-key-hash** | **ip** |**port**)]]]]

Syntax Description

	None: Display information for the security associations for all IPsec tunnels that originate on the local router. The SA information is listed in order according to the local TLOC address.
tloc-address [*color* [(**spi** [(**auth-key-hash** | [**encrypt-key-hash** |**ip** |**port**)]]]]	Specific SA: Display information for a specific security association.

Command History

Release	Modification
14.1	Command introduced.
15.2	Command renamed from **show tunnel local-sa**.

Release	Modification
16.3	Add display for IPv6 source IP addresses.

Examples

```
vEdge# show ipsec local-sa
                                    SOURCE          SOURCE                          SOURCE

TLOC ADDRESS     TLOC COLOR       SPI     IPv4            IPv6                            PORT    KEY HASH

-------------------------------------------------------------------------------------------------------------------
172.16.255.11    lte              256     10.0.5.11       ::                              12366   *****cfdc

172.16.255.11    lte              257     10.0.5.11       ::                              12366   *****cfdc
```

Related Topics

rekey, on page 419
request security ipsec-rekey, on page 700
show ipsec inbound-connections, on page 873
show ipsec outbound-connections, on page 875

show ipsec outbound-connections

show ipsec outbound-connections—Display information about the IPsec connections to remote routers (on Cisco vEdge devices only).

Command Syntax

show ipsec outbound-connections [*source-ip-address*]

show ipsec outbound-connections [**authentication-used** *string* |**tunnel-mtu** *number*]

show ipsec outbound-connections (**remote-tloc-address** *ip-address* | **remote-tloc-color** *color*)

Syntax Description

	None: Display information for all the IPsec connections that originate on the local Cisco vEdge device.
authentication-used *string*	Authentication Type: Display information for the IPsec connections that use the specified authentication.
remote-tloc-address *ip-address*	TLOC Address: Display the IPsec connection information for a specific TLOC address.
remote-tloc-color *color*	TLOC Color: Display the IPsec connection information for a specific TLOC color.

tunnel-mtu *number*	Tunnel MTU Size: Display information for the IPsec connections with the specified MTU size.

Command History

Release	Modification
14.1	Command introduced.
15.2	Command renamed from **show tunnel outbound-connections**.
16.2	Display negotiated encryption algorithm in command output.
Cisco SD-WAN Release 20.6.1	The output of this command was modified. Starting from Cisco SD-WAN Release 20.6.1, 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.

Examples

The following is a sample output of the **show ipsec outbound-connections** for Cisco SD-WAN Release 20.6.1 and later.

```
Device# show sdwan ipsec outbound-connections
SOURCE    SOURCE  DEST             DEST                            REMOTE            REMOTE
   INTEGRITY                     NEGOTIATED
IP                PORT    IP               PORT    SPI     TUNNEL MTU  TLOC ADDRESS     TLOC
 COLOR    USED              KEY HASH    ENCRYPTION ALGORITHM  TC SPIs    PEER      PEER SPI

                                                                        KEY-HASH

-------------------------------------------------------------------------------------------------
10.1.15.15        12366   10.0.5.11       12367   268     1442        172.16.255.11    lte
           ip-udp-esp       *****26f0  AES-GCM-256          8        NONE        0
10.1.15.15        12366   10.0.5.21       12377   268     1442        172.16.255.21    lte
           ip-udp-esp       *****4961  AES-GCM-256          8        NONE        0
10.1.15.15        12366   10.1.14.14      12366   268     1442        172.16.255.14    lte
           ip-udp-esp       *****7c97  AES-GCM-256          8        NONE        0
10.1.15.15        12366   10.1.16.16      12366   268     1442        172.16.255.16    lte
           ip-udp-esp       *****072e  AES-GCM-256          8        NONE        0
```

The following is a sample output of the **show ipsec outbound-connections** command for releases before Cisco SD-WAN Release 20.6.1.

```
Device# show 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

10.1.15.15                    12406   10.0.5.11                   12406   262     1413        172.16.255.11    lte
           AH_SHA1_HMAC   *****f5a8  AES-GCM-256          8
10.1.15.15                    12406   10.0.5.21                   12406   261     1413        172.16.255.21    lte
           AH_SHA1_HMAC   *****afe6  AES-GCM-256          8
10.1.15.15                    12406   10.1.14.14                  12406   262     1413        172.16.255.14    lte
           AH_SHA1_HMAC   *****c4cc  AES-GCM-256          8
10.1.15.15                    12406   10.1.16.16                  12406   262     1413        172.16.255.16    lte
           AH_SHA1_HMAC   *****a3dd  AES-GCM-256          8
```

Related Topics

rekey, on page 419
show ipsec inbound-connections, on page 873
show ipsec local-sa, on page 874

show ipv6 dhcp interface

show ipv6 dhcp interface—Display information about interfaces that are DHCPv6 clients (on Cisco vEdge devices and Cisco Catalyst SD-WAN Controllersonly).

Command Syntax

show ipv6 dhcp interface [**vpn** *vpn-id*] [*interface-name*]

show ipv dhcp interface [**dns-list**] [**state**]

Syntax Description

	None: Display information about all interfaces that are DHCPv6 clients.
dns-list	DNS Servers: Display the DHCPv6 client DNS information.
state	Lease State: Display the DHCPv6 client interface state information.
vpn *vpn-id*	VPN: Display DHCPv6 client interface information for a specific VPN.

Output Fields

The state can be one of **bound**, **init**, **rebind**, **release**, **renew**, and **request**.

The DNS column lists the IPv6 addresses of the DNS servers returned by DHCPv6.

The remaining output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show ipv6 dhcp interface

                                                                                                                  TIME
VPN  INTERFACE  STATE  ACQUIRED IP       SERVER                                  LEASE TIME  REMAINING
GATEWAY  INDEX  DNS
-------------------------------------------------------------------------------------------------------------------------
0    ge0/1      init   -                                                        -           -           -
```

```
0    ge0/2      bound  2001::a00:55e/64  0:1:0:1:1f:80:20:ef:0:c:29:6:79:94  0:02:00:00  0:01:58:08  -
       0      fec0::1

       1      fec0::2

       2      fec0::3
```

Related Topics

ipv6 dhcp-client, on page 274
show dhcp interface, on page 806
show ipv6 interface, on page 879

show ipv6 fib

show ipv6 fib—Display the IPv6 entries in the local forwarding table (on Cisco vEdge devices only).

Command Syntax

show ipv6 fib [**vpn** *vpn-id*]

show ipv6 fib [**vpn** *vpn-id*] [**tloc**color *color* | **tloc-ip** *ip-address*]

show ipv6 fib vpn *vpn-id* [*ipv4-prefix*/*length*]

Syntax Description

	None: List standard information about the IPv6 entries in the forwarding table.
ipv4-prefix/length	Specific Prefix: List the forwarding table entry for the specified IPv6 prefix.
tloc [**color** *color* | **tloc-ip** *ip-address*]	TLOC-Specific Entries: Display forwarding table IPv6 entries for specific TLOCs.
vpn *vpn-id*	VPN-Specific Routes List only the forwarding table IPv4 entries for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
vEdge# show ipv6 fib
                                                NEXTHOP     NEXTHOP          NEXTHOP  SA
VPN  PREFIX                                     IF NAME     ADDR             LABEL    INDEX    TLOC IP          COLOR
-------------------------------------------------------------------------------------------------------------------------
0    ::/0                                       ge0/2       2001::100:50d    -        -        -                -
0    ::/0                                       ge0/1       2001::100:1a17   -        -        -                -
0    2001::a00:500/120                          ge0/2       -                -        -        -                -

0    2001::a00:50b/120                          ge0/2       -                -        -        -                -
0    2001::a00:1a00/120                         ge0/1       -                -        -        -                -
0    2001::a00:1a0b/128                         ge0/1       -                -        -        -                -
0    2001::a00:6510/128                        loopback1    -               -        -        -                -
0    2001::a00:6502/128                        loopback2    -               -        -        -                -
0    2001::a00:6503/128                        loopback3    -               -        -        -                -
0    2001::a00:7504/128                        loopback4    -               -        -        -                -
0    fe80::20c:29ff:feab:b762/128               ge0/1       -                -        -        -                -

0    fe80::20c:29ff:feab:b76c/128               ge0/2       -                -        -        -                -

0    fe80::20c:29ff:feab:b776/128               ge0/3       -                -        -        -                -

0    fe80::20c:29ff:feab:b780/128               ge0/4       -                -        -        -                -

0    fe80::20c:29ff:feab:b78a/128               ge0/5       -                -        -        -                -

0    fe80::20c:29ff:feab:b794/128               ge0/6       -                -        -        -                -

0    fe80::20c:29ff:feab:b79e/128               ge0/7       -                -        -        -                -
```

Related Topics

show ipv6 interface, on page 879
show ipv6 routes, on page 885
show ip fib, on page 854
show omp routes, on page 914

show ipv6 interface

show ipv6 interface—Display information about IPv6 interfaces on a Cisco SD-WAN device.

Command Syntax

show ipv6 interface [**detail**] [*interface-name*] [**vpn** *vpn-id*]

Syntax Description

	None: Display standard information about the interfaces on the Cisco SD-WAN device.
detail	Detailed Interface Information: Display detailed information about the interfaces (available only on Cisco vEdge devices).

interface-name	Specific Interface: Display information about a specific interface. On Cisco vEdge devices, *interface-name* can be a physical interface (**ge** *slot*/*port*), a subinterface or VLAN (**ge** *slot*/*port*.*vlan-number*), the interface corresponding to the system IP address (**system**), the management interface (typically, **eth0**), or a GRE tunnel (**gre** *number*). On Cisco Catalyst SD-WAN Controllers, *interface-name* can be an interface (**eth** *number*) or the interface corresponding to the system IP address (**system**).
vpn *vpn-id*	Specific VPN: Display information about interfaces in a specific VPN.

Output Fields

The remaining output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

Example 1

```
vEdge# show ipv6 interface

                                      IF      IF                                                                  TCP

               AF                     ADMIN   OPER    ENCAP                                       SPEED           MSS
              RX       TX
VPN  INTERFACE  TYPE  IPV6 ADDRESS       STATUS  STATUS  TYPE   PORT TYPE  MTU  HWADDR             MBPS   DUPLEX  ADJUST
  UPTIME      PACKETS  PACKETS  LINK LOCAL ADDRESS
-------------------------------------------------------------------------------------------------------------------
0    ge0/1      ipv6  2001::a00:1a0b/120 Up      Up      null   service    1500 00:0c:29:ab:b7:62  1000   full    1420
  0:01:30:00  2        6        fe80::20c:29ff:feab:b762/64
0    ge0/2      ipv6  2001::a00:50b/120  Up      Up      null   service    1500 00:0c:29:ab:b7:6c  1000   full    1420
  0:01:30:00  21       5        fe80::20c:29ff:feab:b76c/64
0    ge0/3      ipv6  fd00:1234::/16     Up      Up      null   service    1500 00:0c:29:ab:b7:76  1000   full    1420
  0:01:08:33  0        8        fe80::20c:29ff:feab:b776/64
0    ge0/4      ipv6  -                  Up      Up      null   service    1500 00:0c:29:ab:b7:80  1000   full    1420
  0:01:30:00  18       5        fe80::20c:29ff:feab:b780/64
0    ge0/5      ipv6  -                  Down    Up      null   service    1500 00:0c:29:ab:b7:8a  1000   full    1420
  0:01:44:19  1        1        fe80::20c:29ff:feab:b78a/64
0    ge0/6      ipv6  -                  Down    Up      null   service    1500 00:0c:29:ab:b7:94  1000   full    1420
  0:01:44:19  0        1        fe80::20c:29ff:feab:b794/64
0    ge0/7      ipv6  -                  Up      Up      null   service    1500 00:0c:29:ab:b7:9e  1000   full    1420
  0:01:43:02  55       5        fe80::20c:29ff:feab:b79e/64
0    system     ipv6  -                  Up      Up      null   loopback   1500 00:00:00:00:00:00  10     full    1420
  0:01:29:31  0        0        -
0    loopback1  ipv6  2001::a00:6501/128 Up      Up      null   transport  1500 00:00:00:00:00:00  10     full    1420
  0:03:49:09  0        0        -
0    loopback2  ipv6  2001::a00:6502/128 Up      Up      null   transport  1500 00:00:00:00:00:00  10     full    1420
  0:03:49:05  0        0        -
0    loopback3  ipv6  2001::a00:6503/128 Up      Up      null   transport  1500 00:00:00:00:00:00  10     full    1420
  0:03:49:01  0        0        -
0    loopback4  ipv6  2001::a00:6504/128 Up      Up      null   transport  1500 00:00:00:00:00:00  10     full    1420
  0:03:48:54  0        0        -
```

Example 2

```
vEdge# show ipv6 interface detail ge0/1
interface vpn 0 interface ge0/1 af-type ipv6
 if-admin-status       Up
 if-oper-status        Up
 if-addrv6
  ipv6-address 2001::a00:1a0b/120
  secondary-v6 false
  link-local   false
 if-addrv6
  ipv6-address fe80::20c:29ff:fe9b:a9bb/64
  secondary-v6 false
  link-local   true
 encap-type            null
 port-type             service
 ifindex               2
 mtu                   1500
 hwaddr                00:0c:29:9b:a9:bb
 speed-mbps            1000
 duplex                full
 auto-neg              false
 pause-type            tx_pause,rx_pause
 tcp-mss-adjust        1420
 uptime                0:03:54:48
 rx-packets            332832
 rx-octets             64713372
 rx-errors             0
 rx-drops              0
 tx-packets            66
 tx-octets             5472
 tx-errors             0
 tx-drops              16
 rx-pps                24
 rx-kbps               37
 tx-pps                0
 tx-kbps               0
 rx-ip-ttl-expired     0
 interface-disabled    0
 rx-policer-drops      0
 rx-non-ip-drops       0
 filter-drops          0
 mirror-drops          0
 cpu-policer-drops     0
 tx-icmp-policer-drops 0
 split-horizon-drops   0
 route-lookup-fail     0
 bad-label             0
 rx-multicast-pkts     21
 rx-broadcast-pkts     0
 tx-multicast-pkts     6
 tx-broadcast-pkts     2
 num-flaps             2
 rx-policer-remark     0
```

Example 3

```
vSmart# show ipv6 interface eth1
                                                    IF      IF
           TCP                                   LINK
               AF                                ADMIN   OPER    ENCAP                                      SPEED
          MSS                RX       TX       LOCAL
VPN  INTERFACE  TYPE  IPV6 ADDRESS                STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR             MBPS
   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS  ADDRESS
-------------------------------------------------------------------------------------------------------------------
0    eth1       ipv6  2001:a0:5:0:20c:29ff:fea4:333d/64  Up      Up      null   transport  1500  00:0c:29:a4:33:3d  1000
   full    -       0:00:34:45  202689   163339   -
```

Related Topics

show interface, on page 827
show ipv6 neighbor, on page 882
show ipv6 routes, on page 885

show ipv6 neighbor

show ipv6 neighbor—Display the entries in the Address Resolution Protocol (ARP) table for IPv6 neighbors, which lists the mapping of IPv6 addresses to device MAC addresses (on Cisco vEdge devices and Cisco Catalyst SD-WAN Controllers only).

Command Syntax

show ipv6 neighbor [**vpn** *vpn-id*]

Syntax Description

	None: List all the IPv6 entries in the ARP table.
vpn *vpn-id*	Specific VPN: List the IPv6 ARP table entries for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show ipv6 neighbor
      IF
VPN   NAME    IP                          MAC                STATE    IDLE TIMER  UPTIME
-------------------------------------------------------------------------------------------
0     ge0/2   2001::2                     00:0c:bd:06:47:57  static   -           0:00:00:37
0     ge0/2   fe80::20c:bdff:fe06:4757    00:0c:bd:06:47:57  static   -           0:00:00:38
0     ge0/2   fe80::250:b6ff:fe0f:1c84    00:50:b6:0f:1c:84  dynamic  0:00:00:00  0:00:00:34
```

Related Topics

clear arp, on page 577
show arp, on page 746
show ipv6 interface, on page 879
show ipv6 routes, on page 885

show ipv6 policy access-list-associations

show ipv6 policy access-list-associations—Display the IPv6 access lists that are operating on each interface (on Cisco vEdge devices only).

Command Syntax

show ipv6 policy access-list-associations

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
vEdge# show ipv6 policy access-list-associations

             INTERFACE  INTERFACE
NAME         NAME       DIRECTION
----------------------------------------
ipv6-policy  ge0/2      out
```

Related Topics

access-list, on page 28
show policy access-list-associations, on page 964

show ipv6 policy access-list-counters

show ipv6 policy access-list-counters—Display the number of packets counted by IPv6 access lists configured on the Cisco vEdge device (on Cisco vEdge devices only).

Command Syntax

show ipv6 policy access-list-counters

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
vEdge# show ipv6 policy access-list-counters

NAME         COUNTER NAME   PACKETS   BYTES
-----------------------------------------------------------
ipv6-policy  ipv6-counter   1634      135940
```

Related Topics

access-list, on page 30
show policy access-list-counters, on page 965

show ipv6 policy access-list-names

show ipv6 policy access-list-names—Display the names of the IPv6 access lists configured on the Cisco vEdge device (on Cisco vEdge devices only).

Command Syntax

show policy access-list-names

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show ipv6 policy access-list-names

NAME
--------------------
ipv6-policy
```

Related Topics

access-list, on page 30
show policy access-list-names, on page 966

show ipv6 policy access-list-policers

show ipv6 policy access-list-policers—Display information about the policers configured in IPv6 access lists (on Cisco vEdge devices only).

Command Syntax

show ipv6 policy 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.

```
vEdge# show policy 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
```

Related Topics

clear policer statistics, on page 612
show policer, on page 963
show policy access-list-policers, on page 967

show ipv6 routes

show ipv6 routes—Display the IPv6 entries in the local route table. On Cisco Catalyst SD-WAN Controllers, the route table incorporates forwarding information.

Command Syntax

show ipv6 routes [**detail**] [*ipv6-address*] [*ipv6-prefix/length*] [**bgp**] [**connected**] [**omp**] [**ospf**] [**static**] [**summary protocol** *protocol*] [**vpn** *vpn-id*]

show ipv6 routes vpn *vpn-id* [**detail**] [*ipv6-address*] [*ipv6-prefix*/*length*] [**bgp**] [**connected**] [**omp**] [**ospf**] [**static**]

Syntax Description

	None: List standard information about the entries in the local IPv6 route table.
detail	Detailed Information: List detailed information about the entries in the local IPv6 route table.
ipv6-address *ipv6-prefix*/*length* *prefix* **vpn** *vpn-id*	IP Address or Route Prefix: List route information for the specified IPv6 route prefix. If you omit the prefix length, you must specify a VPN identifier so that the Cisco SD-WAN software can find the route that best matches the prefix.
	Routes Learned from a Protocol: List routes learned from one or more specific protocols—**bgp**, **connected**, **omp**, **ospf**, and **static**. The protocol **static** includes both routes that are statically configured on the local device as well as routes learned from a DHCP server if one or more interfaces in VPN 0 are configured to learn their IP addresses via DHCP.
summary protocol *protocol*	Summary of Routes Learned from a Protocol: List summary information about the IP routes in the route table or about routes learned from the specified protocol. *protocol* can be **bgp**, **connected**, **omp**, **ospf**, or **static**.
vpn *vpn-id*	VPN-Specific Routes: List only the route table entries for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
vEdge# show ipv6 routes
Codes Proto-sub-type:
  IA -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive
                                          PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN    PREFIX              PROTOCOL       SUB TYPE  IF NAME     ADDR             VPN      TLOC IP          COLOR
```

```
      ENCAP  STATUS
------------------------------------------------------------------------------------------------------------------------------------
0      fd00::/16          connected       -         ge0/3       -               -       -               -
      -      F,S
```

Related Topics

show ip routes, on page 865
show ipv6 interface, on page 879
show ipv6 neighbor, on page 882

show jobs

show jobs—View a list of the files that are currently being monitored on the local device. This command is the same as the UNIX jobs command.

Command Syntax

show jobs

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
15.4	Command introduced.

Examples

Start and stop monitoring a file, and view the files that are being monitored:

```
vEdge# monitor start /var/log/vsyslog
vEdge# show jobs
JOB COMMAND
1   monitor start /var/log/vsyslog
vEdge# log:local7.notice: Dec 16 14:55:26 vsmart SYSMGR[219]:
%Viptela-vsmart-SYSMGR-5-NTCE-200025: System clock set to Wed Dec 16 14:55:26 2015  (timezone
 'America/Los_Angeles')
log:local7.notice: Dec 16 14:55:27 vsmart SYSMGR[219]: %Viptela-vsmart-SYSMGR-5-NTCE-200025:
 System clock set to Wed Dec 16 14:55:27 2015  (timezone 'America/Los_Angeles')

vEdge# monitor stop /var/log/vsyslog
vEdge#
```

Related Topics

job stop, on page 640
monitor start, on page 643
monitor stop, on page 643

show licenses

show licenses—Display the licenses for the software packages used by the Cisco SD-WAN software.

Command Syntax

show licenses [**list** | **package** *package-name*]

Syntax Description

	None: Display the licenses for all the software packages used by the Cisco SD-WAN software.
package *package-name*	Display the License for an Individual Package: Display the license for a specific software package.
list	List the Software Package Licenses: List the software packages used by the Cisco SD-WAN software.

Output Fields

The output of the **show licenses** command is quite extensive. To read all the licenses, it is recommended that you save the command output to a file:

vEdge# **show licenses** | **save** *filename*

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show licenses list
LIST OF PACKAGES
licenses
acl
apmd
attr
base-files
base-passwd
bash
beecrypt
bison
busybox
bzip2
coreutils
cracklib
db
e2fsprogs
elfutils
ethtool
```

```
file
flex
freeradius-client
gdb
grep
icu
init-ifupdown
initscripts
iperf
iproute2
iptables
kmod
libevent
libpam
libtool
liburcu
libxml2
logrotate
lttng-ust
modutils-initscripts
ncurses
net-tools
netbase
ntp
ocf-linux
openssh
openssl
opkg
opkg-config-base
pciutils
perl
procps
protobuf
protobuf-c
psplash
python-smartpm
quagga
rpm
rpm-postinsts
shadow
shadow-securetty
strace
sysfsutils
sysklogd
sysvinit
sysvinit-inittab
tar
tcpdump
tinylogin
tunctl
tzdata
udev
udev-extraconf
update-rc.d
usbutils
util-linux
v86d
valgrind
viptela-cp
```

Related Topics

show version, on page 1036

show log

show log—Display the contents of system log (syslog) files.

Command Syntax

show log *filename* [**tail** *number*]

Syntax Description

Filename	Filename: Name of the syslog file.
tail *number*	Last Lines in the File: Display the last lines in the file. In *number*, specify the number of lines to display.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
17.1	Command introduced.

Example

```
vEdge# show log messages tail 10
local7.info: Jan 25 13:46:42 vedge DHCP_CLIENT[651]: %Viptela-vedge-DHCP_CLIENT-6-INFO-1300004: Requesting renew [50%] for interface eth0 address
10.0.1.33/24
local7.info: Jan 25 13:46:42 vedge DHCP_CLIENT[651]: %Viptela-vedge-DHCP_CLIENT-6-INFO-1300010: Renewed address 10.0.1.33/24 for interface eth0
local7.info: Jan 25 13:46:42 vedge DHCP_CLIENT[651]: %Viptela-vedge-vdhcpcd-6-INFO-1400002: Notification: 1/25/2018 21:46:42 dhcp-address-renewed
severity-level:minor host-name:"vm13" system-ip::: vpn-id:512 if-name:"eth0" client-mac:"00:50:56:00:01:21" ip:10.0.1.33
auth.info: Jan 25 14:11:31 vedge sshd[31600]: Accepted publickey for admin from 10.0.1.1 port 59156 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1s
authpriv.info: Jan 25 14:11:31 vedge sshd[31600]: pam_unix(sshd:session): session opened for user admin by (uid=0)
local1.info: Jan 25 14:11:32 vedge confd[474]: audit user: admin/99 assigned to groups: viptela-reserved-system-write-task,netadmin
local1.info: Jan 25 14:11:32 vedge confd[474]: audit user: admin/99 CLI 'startup'
local1.info: Jan 25 14:11:32 vedge confd[474]: audit user: admin/99 CLI aborted
local7.info: Jan 25 14:11:34 vedge SYSMGR[257]: %Viptela-vedge-sysmgrd-6-INFO-1400002: Notification: 1/25/2018 22:11:34 system-login-change
severity-level:minor host-name:"vm13" system-ip::: user-name:"admin" user-id:99
local1.info: Jan 25 14:11:38 vedge confd[47
```

Related Topics

file list, on page 637
file show, on page 637
logging disk, on page 298
logging server, on page 305
show crash, on page 803
show logging, on page 891

show logging

show logging—Display the settings for logging syslog messages.

Command Syntax

show logging [*logging-parameter*]

Syntax Description

	None: Display all logging information.
logging-parameter	Specific Logging Parameter: Display information for a specific logging parameter. *logging-parameter* can be **disk_filename**, **disk_filerotate**, **disk_filesize**, **disk_priority**, **disk_status**, **host_name**, **host_priority**, **host_status**, and **host_vpn_id**.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
Edge# show logging

System logging to  in vpn 0 is disabled
Priority for host logging is set to: info

System logging to disk is enabled
Priority for disk logging is set to:  info
File name for disk logging is set to:  /var/log/vsyslog
File size for disk logging is set to:  10 MB
File recycle count for disk logging is set to:  10

Syslog facility is set to: local7
```

Related Topics

file list, on page 637
file show, on page 637
logging disk, on page 298
logging server, on page 305
show crash, on page 803

show log, on page 890

show logging process

To view messages logged by binary trace for a process or processes, use the **show logging process** command in the privileged EXEC mode.

show logging process *process-name*
[**extract-pcap to-file** *path* | [**end timestamp** *ts*] [**module** *name*] [**internal**] [**start** { **last** { *n* { **days** | **hours** | **minutes** | **seconds** } **clear boot** } | **timestamp** *ts* } [**end** { **last** { *n* { **days** | **hours** | **minutes** | **seconds** } **clear boot** } | **timestamp** *ts* }]] [**level** *level*] [**fru** *slot*] [**reverse** | [**trace-on-failure** | **metadata**] [**to-file** *path*]]]

Syntax Description

process-name	Shows logs for one or more Cisco SD-WAN processes. You can specify a comma-separated list of processes, for example, `fpmd, ftm`. 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'.
extract-pcap to-file *path*	Extracts pcap data to a file.
end timestamp *ts*	Shows logs up to the specified timestamp.
module *name*	Selects logs for specific modules.
internal	Selects all logs.
start{ **last** { *n* {**days** | **hours** | **minutes** | **seconds**} | **clear** | **boot**} | **timestamp** *ts*}[**end**{ **last** { *n* {**days** | **hours** | **minutes** | **seconds**} | **clear** | **boot**} | **timestamp** *ts*}]	Shows logs collected between the specified start and end times.
level *level*	Shows logs for the specified and higher levels.
fru *slot*	Shows logs from a specific FRU.
reverse	Shows logs in reverse chronological order.
to-file *path*	Decodes files stored in disk and writes output to file.
trace-on-failure	Shows the trace on failure summary.
metadata	Shows metadata for every log message.

Command Default

None

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'.

Usage Guidelines

Table 20: 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

```
Device# show logging process fpmd internal start last boot
Logging display requested on 2020/11/09 07:13:08 (UTC) for Hostname: [Device], Model:
[ISR4451-X/K9], Version: [17.04.01], SN: [FOC23125GHG], MD_SN: [FGL231432EQ]

Displaying logs from the last 7 days, 0 hours, 14 minutes, 55 seconds
executing cmd on chassis local ...

2020/11/02 07:00:59.314166 {fpmd_pman_R0-0}{1}: [btrace] [7403]: (note): Btrace started for
 process ID 7403 with 512 modules
2020/11/02 07:00:59.314178 {fpmd_pman_R0-0}{1}: [btrace] [7403]: (note): File size max used
 for rotation of tracelogs: 8192
2020/11/02 07:00:59.314179 {fpmd_pman_R0-0}{1}: [btrace] [7403]: (note): File size max used
 for rotation of TAN stats file: 8192
2020/11/02 07:00:59.314179 {fpmd_pman_R0-0}{1}: [btrace] [7403]: (note): File rotation
timeout max used for rotation of TAN stats file: 600
2020/11/02 07:00:59.314361 {fpmd_pman_R0-0}{1}: [btrace] [7403]: (note): Boot level config
 file [/harddisk/tracelogs/level_config/fpmd_pman_R0-0] is not available. Skipping
2020/11/02 07:00:59.314415 {fpmd_pman_R0-0}{1}: [benv] [7403]: (note): Environment variable
 BINOS_BTRACE_LEVEL_MODULE_PMAN is not set
2020/11/02 07:00:59.314422 {fpmd_pman_R0-0}{1}: [benv] [7403]: (note): Environment variable
 FPMD_BTRACE_LEVEL is not set
2020/11/02 07:00:59.314424 {fpmd_pman_R0-0}{1}: [fpmd_pman] [7403]: (note):
BTRACE_FILE_SIZE_MAX_BYTES temporarily set to 8192, now cleared.
```

show logging profile sdwan

To view messages logged by binary trace for Cisco-SD-WAN-specific processes and process modules, use the **show logging profile sdwan** command in the privileged EXEC mode. The messages are displayed in chronological order.

show logging profile sdwan

[**extract-pcap to-file** *path* | [**end timestamp** *ts*] [**module** *name*] [**internal**] [**start** { **last** { *n* { **days** | **hours** | **minutes** | **seconds** } **clear boot** } | **timestamp** *ts* } [**end** { **last** { *n* { **days** | **hours** | **minutes** | **seconds** } **clear boot** } | **timestamp** *ts* }]] [**level** *level*] [**fru** *slot*] [**reverse** | [**trace-on-failure** | **metadata**] [**to-file** *path*]]]

Syntax Description

extract-pcap to-file *path*	Extracts pcap data to a file.
end timestamp *ts*	Shows logs up to the specified timestamp.
module *name*	Selects logs for specific modules.
internal	Selects all logs.
start{ **last** { *n* {**days** | **hours** | **minutes** | **seconds**} | **clear** | **boot**} | **timestamp** *ts*}[**end**{ **last** { *n* {**days** | **hours** | **minutes** | **seconds**} | **clear** | **boot**} | **timestamp** *ts*}]	Shows logs collected between the specified start and end times.
level *level*	Shows logs for the specified and higher levels.
fru *slot*	Shows logs from a specific FRU.
reverse	Shows logs in reverse chronological order.
to-file *path*	Decodes files stored in disk and writes output to file.
trace-on-failure	Shows the trace on failure summary.
metadata	Shows metadata for every log message.

Command Default

None

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'.

Usage Guidelines

Table 21: 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

The following example shows a truncated output of the **show logging profile sdwan start last boot internal** command. From the timestamps, we can see that the messages are shown in a chronological order.

```
Device# show logging profile sdwan start last boot internal
Logging display requested on 2020/11/18 18:59:16 (UTC) for Hostname: [Device], Model:
[ISR4451-X/K9], Version: [17.04.01], SN: [FOC23125GHG], MD_SN: [FGL231432EQ]

Displaying logs from the last 1 days, 10 hours, 0 minutes, 20 seconds
executing cmd on chassis local …
.
.
.
2020/11/20 10:25:52.195149 {vdaemon_R0-0}{1}: [misc] [10969]: (ERR): Set chassis-number -
ISR4451-X/K9-FOC23125GHG in confd
2020/11/20 10:25:52.198958 {vdaemon_R0-0}{1}: [misc] [10969]: (ERR): Root-CA file exists -
 Set it in CDB
2020/11/20 10:25:52.200462 {vdaemon_R0-0}{1}: [vipcommon] [10969]: (debug): chasfs
property_create success sw-vip-vdaemon-done
2020/11/20 10:25:52.201467 {vip_confd_startup_sh_R0-0}{1}: [btrace_sh] [6179]: (note):
INOTIFY /tmp/chassis/local/rp/chasfs/rp/0/0/confd/ CREATE sw-vip-vdaemon-done
2020/11/20 10:25:52.202184 {vip_confd_startup_sh_R0-0}{1}: [btrace_sh] [6179]: (note):
INOTIFY /tmp/chassis/local/rp/chasfs/rp/0/0/confd/ CLOSE_WRITE-CLOSE sw-vip-vdaemon-done
2020/11/20 10:25:52.238625 {vdaemon_R0-0}{1}: [vipcommon] [10969]: (debug):
[/usr/sbin/iptables -w -A LOGGING -m limit --limit 5/m -j LOG --log-prefix "iptables-dropped:"
 --log-level 6] exited with ret: 2, output: iptables v1.8.3 (legacy): Couldn't load match
`limit':No such file or directory
2020/11/20 10:25:52.242402 {vdaemon_R0-0}{1}: [vipcommon] [10969]: (debug):
[/usr/sbin/ip6tables -w -A LOGGING -m limit --limit 5/m -j LOG --log-prefix
"ip6tables-dropped:" --log-level 6] exited with ret: 2, output: ip6tables v1.8.3 (legacy):
 Couldn't load match `limit':No such file or directory
2020/11/20 10:25:52.254181 {vdaemon_R0-0}{1}: [misc] [10969]: (ERR): Error removing
/usr/share/viptela/proxy.crt
2020/11/20 10:25:52.692474 {vdaemon_R0-0}{1}: [confd] [10969]: (ERR): Flags=1, device-type=1,
 vbond-dns=0, domain-id=0, site-id=0, system-ip=0, wan-intf=0, org-name=0, cert-inst=0,
root-cert-inst=0, port-offset=0, uuid=0
2020/11/20 10:25:52.692486 {vdaemon_R0-0}{1}: [confd] [10969]: (ERR): Returning 0
.
.
.
2020/11/20 10:26:24.669716 {fpmd_pmanlog_R0-0}{1}: [btrace] [14140]: (note): Btrace started
 for process ID 14140 with 512 modules
2020/11/20 10:26:24.669721 {fpmd_pmanlog_R0-0}{1}: [btrace] [14140]: (note): File size max
 used for rotation of tracelogs: 8192
.
.
.
2020/11/20 10:26:25.001528 {fpmd_R0-0}{1}: [fpmd] [14271]: (note): FPMD BTRACE INIT DONE
2020/11/20 10:26:25.001551 {fpmd_R0-0}{1}: [vipcommon] [14271]: (note): Vipcommon btrace
init done
2020/11/20 10:26:25.001563 {fpmd_R0-0}{1}: [chmgr_api] [14271]: (note): Chmgr_api btrace
init done
2020/11/20 10:26:25.022479 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): Btrace started
 for process ID 14364 with 512 modules
2020/11/20 10:26:25.022484 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): File size max
 used for rotation of tracelogs: 8192
2020/11/20 10:26:25.022484 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): File size max
 used for rotation of TAN stats file: 8192
2020/11/20 10:26:25.022485 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): File rotation
 timeout max used for rotation of TAN stats file: 600
```

```
2020/11/20 10:26:25.022590 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): Boot level
config file [/harddisk/tracelogs/level_config/ftmd_pmanlog_R0-0] is not available. Skipping
2020/11/20 10:26:25.022602 {ftmd_pmanlog_R0-0}{1}: [btrace] [14364]: (note): Setting level
 to 5 from [BINOS_BTRACE_LEVEL_MODULE_BTRACE_SH]=[NOTICE]
2020/11/20 10:26:25.037903 {fpmd_R0-0}{1}: [cyan] [14271]: (warn): program path package
name rp_security does not match .pkginfo name mono
2020/11/20 10:26:25.038036 {fpmd_R0-0}{1}: [cyan] [14271]: (note): Successfully initialized
 cyan library for /tmp/sw/rp/0/0/rp_security/mount/usr/binos/bin/fpmd with
/tmp/cyan/0/mono.cdb
2020/11/20 10:26:26.206844 {ftmd_R0-0}{1}: [tdllib] [14517]: (note): Flag tdlh stale epoch
 for all tdl handles
2020/11/20 10:26:26.206853 {ftmd_R0-0}{1}: [tdllib] [14517]: (note): Detect newly epoch
file generated: /tmp/tdlresolve/epoch_dir/active, new epoch:
/tmp/tdlresolve/epoch_dir//2020_11_20_10_23_8925.epoch
2020/11/20 10:26:26.206866 {ftmd_R0-0}{1}: [tdllib] [14517]: (note): epoch file read
/tmp/tdlresolve/epoch_dir//2020_11_20_10_23_8925.epoch
2020/11/20 10:26:26.334529 {plogd_R0-0}{1}: [plogd] [5353]: (debug):   Sending: facility
16. %Cisco-SDWAN-RP_0-CFGMGR-4-WARN-300001: R0/0: CFGMGR: Connection to ftm is up
2020/11/20 10:26:26.334580 {plogd_R0-0}{1}: [plogd] [5353]: (debug):   Sending: facility
16. %Cisco-SDWAN-Atlantis-B4-FTMD-4-WARN-1000007: R0/0: FTMD: Connection to TTM came up.
p_msgq 0x564c7606bc30 p_ftm 0x564c7514d8b0
2020/11/20 10:26:26.335175 {IOSRP_R0-0}{1}: [iosrp] [15606]: (warn):  *Nov 20 10:26:26.335:
 %Cisco-SDWAN-RP_0-CFGMGR-4-WARN-300001: R0/0: CFGMGR: Connection to ftm is up
.
.
.
```

show monitor event-trace sdwan

To display event trace messages for Cisco SD-WAN subsystem components, use the **show monitor event-trace** command in the privileged EXEC mode.

show monitor event-trace sdwan [**all**] *component* { **all** | **back** *hour:minute* | **clock** *hour:minute* | **from-boot** *seconds* | **latest** | **parameters** }

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
all	Displays all event trace messages currently in memory.
back *mmm* | *hhh:mm* }	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified either in minutes or in hours and minutes format (mmm or hh:mm).
clock *hh:mm*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
date	(Optional) Day of the month.
month	(Optional) Displays the month of the year.
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime).
latest	Displays only the event trace messages since the last command was entered.

parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.
detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace** command will stop displaying messages.

Example

The following is sample output from the **show monitor event-trace** command for the SD-WAN device. Notice that each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Device# show monitor event-trace sdwan all
*Nov  6 23:30:51.393: <-cfg[2] A: vrf_activate IPv4 table 0x3
*Nov  6 23:30:51.754: <-fib[2] A: vrf_activate IPv4 table 0x3
*Nov  6 23:30:51.754: ->omp[3] A: vrf IPv4
*Nov  6 23:30:52.108: <-omp[2] A: redist IPv4 ospf
*Nov  6 23:30:52.108: <-ospf A: protocol topo 3 proc ospf
*Nov  6 23:30:52.108: <-omp[2] A: redist IPv4 connected
*Nov  6 23:30:52.108: <-omp[2] A: redist IPv4 static
*Nov  6 23:30:52.108: <-omp[2] A: redist IPv4 nat
```

```
Device# req pla sof sdwan admin-tech
Requested admin-tech initiated.
[vm5:/bootflash/vmanage-admin/var/tech]$ vim sdwan_trace
*Nov  6 23:30:51.393: <-cfg[2] A: vrf_activate IPv4 table 0x3
*Nov  6 23:30:51.755: <-fib[2] A: vrf_activate IPv4 table 0x3
*Nov  6 23:30:51.755: ->omp[3] A: vrf IPv4
*Nov  6 23:30:52.107: <-omp[2] A: redist IPv4 ospf
*Nov  6 23:30:52.107: <-ospf A: protocol topo 3 proc ospf
*Nov  6 23:30:52.107: <-omp[2] A: redist IPv4 connected
*Nov  6 23:30:52.107: <-omp[2] A: redist IPv4 static
*Nov  6 23:30:52.108: <-omp[2] A: redist IPv4 nat
```

show multicast replicator

show multicast replicator—List information about multicast replicators (on Cisco vEdge devices only).

Command Syntax

show multicast replicator [**vpn** *vpn-id*]

Syntax Description

	None: List standard information about multicast replicators.
vpn *vpn-id*	VPN-Specific Replicators: List only the multicast replicators in the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge# show multicast replicator

     REPLICATOR      REPLICATOR  LOAD
VPN  ADDRESS         STATUS      PERCENT
-----------------------------------------
1    172.16.255.14   UP          -
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

show multicast rpf

show multicast rpf—List multicast reverse-path forwarding information (on Cisco vEdge devices only).

Command Syntax

show multicast rpf [**vpn** *vpn-id*]

Syntax Description

	None: List standard RPF information.
vpn *vpn-id*	VPN-Specific RPF Information: List the RPF information only for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge# show multicast rpf

                                        RPF   RPF
                  RPF       NEXTHOP     NBR   IF      RPF
VPN   RPF ADDRESS STATUS    COUNT       ADDR  NAME    TUNNEL
-------------------------------------------------------------
1     10.20.25.18 resolved  1           -     ge0/4   -
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957

show pim rp-mapping, on page 958
show pim statistics, on page 959

show multicast topology

show multicast topology—List information related to the topology of the multicast domain (on Cisco vEdge devices only).

Command Syntax

show multicast topology [**vpn** *vpn-id*]

Syntax Description

	None: List standard information related to the topology of the multicast domain.
vpn *vpn-id*	VPN-Specific Topology Information: List multicast topology information only for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge show multicast topology
Flags:
  S: SPT switchover
OIF-Flags:
  A: Assert winner

                            JOIN                                    UPSTREAM       UPSTREAM  UPSTREAM                                  OIF
 OIF
VPN  GROUP      SOURCE      TYPE   FLAGS  RP ADDRESS  REPLICATOR     NEIGHBOR       STATE     INTERFACE      UP TIME     EXPIRES     INDEX  NAME
 FLAGS  OIF TUNNEL
-------------------------------------------------------------------------------------------------------------------------------------------------
1    225.0.0.0  0.0.0.0     (*,G)  -      58.0.1.100  172.16.255.14  172.16.255.14  joined    172.16.255.14  0:01:26:52  0:00:00:31  1      ge0/0
 -      -
1    225.0.0.1  0.0.0.0     (*,G)  -      58.0.1.100  172.16.255.14  172.16.255.14  joined    172.16.255.14  0:01:26:52  0:00:00:31  1      ge0/0
 -      -
1    225.0.0.2  0.0.0.0     (*,G)  -      58.0.1.100  172.16.255.14  172.16.255.14  joined    172.16.255.14  0:01:26:52  0:00:00:31  1      ge0/0
 -      -
1    225.0.0.3  0.0.0.0     (*,G)  -      58.0.1.100  172.16.255.14  172.16.255.14  joined    172.16.255.14  0:01:26:52  0:00:00:31  1      ge0/0
 -      -
1    225.0.0.4  0.0.0.0     (*,G)  -      58.0.1.100  172.16.255.14  172.16.255.14  joined    172.16.255.14  0:01:26:52  0:00:00:31  1      ge0/0
 -      -
1    225.0.0.9  56.0.1.100  (S,G)  -      -           -              56.0.1.100     joined    ge0/0          0:00:53:27  0:00:00:33  517    -
 -      172.16.255.14
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show ip mfib oil, on page 859
show ip mfib stats, on page 860
show ip mfib summary, on page 861
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

show multicast tunnel

show multicast tunnel—List information about the IPsec tunnels between multicast peers (on Cisco vEdge devices only).

Command Syntax

show multicast tunnel [**vpn** *vpn-id*]

Syntax Description

	None: List standard information about the multicast IPsec tunnels.
vpn *vpn-id*	VPN-Specific Tunnels: List IPsec tunnel information only for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge# show multicast tunnel

     TUNNEL          TUNNEL
VPN  ADDRESS         STATUS  REPLICATOR
---------------------------------------
1    172.16.255.11   UP      no
     172.16.255.14   UP      yes
     172.16.255.15   UP      no
     172.16.255.21   UP      no
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

show nms-server running

show nms-server running—Display whether a vManage NMS server is operational (on vManage NMSs only).

Command Syntax

show nms-server running

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.2	Command introduced.

Example

Display the operational status of a vManage server.

```
vManage# show nms-server running
nms-server running true
```

Related Topics

request nms-server

show notification stream

show notification stream—Display notifications about events that have occurred on the Cisco SD-WAN device.

Command Syntax

show notification stream viptela [**from** *date-time*] [**last** *number*] [**to** *date-time*]

Syntax Description

	None: Display notifications about all events.
to (*ccyy-mm-dd* | *hh:mm:ss* | *ccyy-mm***T***hh:mm:ss*)	Event End Time: Display notifications of events that have occurred up until the specified date and time.
to (*ccyy-mm-dd* | *hh:mm:ss* | *ccyy-mm***T***hh:mm:ss*)	Event Start Time: Display notifications of events that have occurred up until the specified date and time.
to *number*	Most Recent Events: Display the most recent event notifications up to the specified number of events.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show notification stream viptela
notification
eventTime 2013-12-06T11:47:11.420432+00:00
interface-state-change
  vpn-id 512
  if-name eth0
  new-state up
 !
!
notification
eventTime 2013-12-06T10:28:54.665583+00:00
interface-state-change
  vpn-id 0
  if-name ge0/7
  new-state up
 !
!
notification
eventTime 2013-12-06T18:32:25.568821+00:00
interface-state-change
  vpn-id 0
  if-name system
  new-state up
 !
!
notification
eventTime 2013-12-06T18:32:25.585694+00:00
omp-state-change
  new-state up
 !
!
notification
eventTime 2013-12-06T18:32:26.780149+00:00
interface-state-change
  vpn-id 0
  if-name ge0/0
  new-state up
 !
!
```

Related Topics

file list, on page 637
trap group, on page 507
trap target, on page 509

show ntp associations

show ntp associations—Display information about the status connections to peers.

Command Syntax

show ntp associations

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show ntp associations

IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  LAST EVENT   COUNT
-------------------------------------------------------------------------------
1    18402    80a3    yes   no            none  reject     unreachable  10
2    18403    967a    yes   yes           none  sys.peer   sys_peer     7
```

Related Topics

ntp, on page 356
show ntp peer, on page 905

show ntp peer

show ntp peer—Display information about the NTP peers with which the Cisco SD-WAN software is synchronizing its clocks.

Command Syntax

show ntp peer [*index*] [*parameter*]

Syntax Description

	None: Display standard information about the interfaces on the Cisco SD-WAN device.
parameter	Specific Parameter: Display information about a specific NTP parameter. *parameter* can be one of the following: **delay**, **jitter**, **offset**, **poll**, **reach**, **refif**, **remote**, **st**, **type**, and **when**.
index	Specific Peer: Display information about a specific peer, identified by its index number in the **show ntp peer** command output.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show ntp peer
INDEX  REMOTE          REFID         ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET  JITTER
------------------------------------------------------------------------------------------
1      127.127.1.0     .LOCL.        14  l     5d    64    0      0.000    0.000   0.000
2      *98.191.213.7   18.26.4.105   2   u     113   1024  377    140.919  -4.328  13.535
```

Related Topics

ntp, on page 356
show ntp associations, on page 904

show omp cloudexpress

show omp cloudexpress—Display OMP routes for applications configured with Cloud OnRamp for SaaS (formerly called CloudExpress service) (on Cisco vEdge devices only).

Command Syntax

show omp cloudexpress [**detail**]

Syntax Description

	None: Display OMP routes for all applications in all VPNs configured with Cloud OnRamp for SaaS.
detail	Detailed Information: List detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.
Cisco SD-WAN Release 20.7.1	Added APP TYPE and SUBAPP ID columns to the command output.

The following example shows the command output as it appears beginning with Cisco SD-WAN Release 20.7.1.

```
vEdge#show omp cloudexpress
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
                     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    172.16.255.16   3    0     0       amazon_aws  172.16.255.16  C,R
                                                   172.16.255.20  C,R
```

The following example shows the command output as it appears for releases before Cisco SD-WAN Release 20.7.1.

```
vEdge#show omp cloudexpress
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

                     APP
VPN  ORIGINATOR      ID   APP NAME     FROM PEER      STATUS
-----------------------------------------------------------
1    172.16.255.14   1    salesforce   172.16.255.19  C,I,R
                                       172.16.255.20  C,I,R
1    172.16.255.14   16   google_apps  172.16.255.19  C,I,R
                                       172.16.255.20  C,I,R
```

Related Topics

clear cloudexpress computations, on page 583
show cloudexpress applications, on page 780
show cloudexpress gateway-exits, on page 781
show cloudexpress local-exits, on page 782

show omp multicast-auto-discover

show omp multicast-auto-discover—List the peers that support multicast (on Cisco vEdge devices and vSmart controllers only).

Command Syntax

show omp multicast-auto-discover [**detail**]

show omp multicast-auto-discover [**detail**] [**family ipv4**] [**entries advertised** *destination-peer-address*]

show omp multicast-auto-discover [**detail**] [**family ipv4**] [**entries received** *source-peer-address*] [**loss-reason** *reason* | **status** *status*]

Syntax Description

	None: List standard information about the PIM IPsec tunnels.
family ipv4 entries advertised [*destination-peer-address*]	Advertised Multicast Sources: List the multicast sources advertised.
detail	Detailed Information: List detailed information.
family ipv4 entries received *source-peer-address* [**loss-reason** *reason* | **status** *status*]	Received Multicast Sources List the multicast sources received. Include the **loss-reason** option to list specific reasons for losses of multicast sources. *reason* can be **distance**, **invalid**, **none**, **omp-version**, **origin-metric**, **origin-protocol**, **origin-protocol-subtype**, **peer-id**, **personality**, **preference**, **site-id**, **stale-entry**, **tloc-id**, and **tloc-preference**. Include the **status** option to list specific route-table status. *status* can be **C** (for chosen), **Ext** (for extranet), **I** (for installed), **Inv** (for invalid), **L** (for looped), **R** (for resolved), **Red** (for redistributed), **Rej** (for rejected), **S** (for stale), and **U** (for unknown).

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge# show 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
```

Related Topics

show omp multicast-routes, on page 909
show multicast topology, on page 900

show omp multicast-routes

show omp multicast-routes—List the multicast routes that OMP has learned from PIM join messages (on Cisco vEdge devices and vSmart controllers).

Command Syntax

show omp multicast-routes [**detail**]

show omp multicast-routes [**detail**] [**family ipv4**] [**entries**]

Syntax Description

	None: List standard information about the routes that OMP has learned from PIM join messages.
detail	Detailed Information: List detailed information.
family ipv4 [**entries**]	Multicast Routes for a Protocol Family: List the multicast routes for the IPv4 protocol family.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.2	Command introduced.

Example

```
vEdge# show 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
```

Related Topics

show omp multicast-auto-discover, on page 907
show multicast topology, on page 900

show omp peers

show omp peers—Display information about the OMP peering sessions that are active on the local vSmart controller or Cisco vEdge device.

Command Syntax

show omp peers [**detail**]

show omp peers *ip-address* [**detail**]

Syntax Description

	None: List information about all OMP peering sessions on the local device.
detail	Detailed information: Display detailed information.
ip-address	Specific OMP Peer: Display configuration OMP peering session information about a specific peer.

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.
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 SD-WAN device.
Region ID	Region assigned for Hierarchical SD-WAN. When you use the command on a device, this is the region to which the device is assigned. When you use the command on a Cisco SD-WAN Controller, this shows the region(s) that the Cisco SD-WAN Controller is managing. 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 SD-WAN administrative site where the connected Cisco SD-WAN device is located.
state	Operational state of the connection to the Cisco 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.

Field	Explanation
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 SD-WAN device: • vEdge - Cisco vEdge device vsmart - vSmart controller
upcount	Number of times an OMP peering session has come up.
Uptime	How long the OMP session between the Cisco SD-WAN devices has been up and operational.

Command History

Release	Modification
14.1	Command introduced.
14.3	Down-in-gr stated added.
Cisco SD-WAN Release 20.6.1	Added Region ID to output.

Examples

Example 1

```
vEdge# show 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 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 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

The following example shows the output when you execute the command on a Cisco vEdge device, and shows the REGION ID field added in Cisco SD-WAN Release 20.6.1.

```
vEdge# show omp peers
R -> routes received
I -> routes installed
S -> routes sent

                  DOMAIN  OVERLAY   SITE      REGION
PEER       TYPE   ID      ID        ID        ID        STATE    UPTIME       R/I/S
-------------------------------------------------------------------------------------
10.0.0.1   vsmart 1       1         50000122  2         up       0:00:01:04   0/0/25
```

Example 5

When you execute the command on a Cisco SD-WAN Controller, use the **detail** keyword to show the region-id field added in Cisco SD-WAN Release 20.6.1. The region-id field shows the region(s) that the Cisco SD-WAN Controller is managing.

```
vsmart1# show omp peers detail

peer                    10.0.0.1
type                    vedge
domain-id               1
site-id                 21000
overlay-id              1
region-id               1
state                   up
version                 1
legit                   yes
control-up              yes
staging                 no
upcount                 5
downcount               4
…
```

Related Topics

clear omp peer, on page 602
show control connections, on page 788
show omp routes, on page 914
show omp services, on page 919
show omp summary, on page 921
show omp tlocs, on page 924

show omp routes

To display information about OMP routes on Cisco Catalyst SD-WAN Controllers and Cisco vEdge devices only, use the **show omp routes** command. OMP routes carry information that the learns from the routing protocols running on its local network including routes learned from BGP and OSPF as well direct, connected, and static routes.

Command Syntax

show omp routes [*ipv4 prefix IP / length*] [**family** *family-address*] [**vpn** *vpn-id*] [**advertised**] [**received**] [**detail**]

Syntax Description

	None: Lists routing information about all OMP peering sessions on the local device.
ipv4 prefix	Displays the route prefix. Lists OMP route information for the specified route prefix.
IP	Displays IP address of the specific route. Lists OMP IP address for the specific route.
length	Displays the route length.
detail	Detailed information: Lists detailed route information about OMP peering sessions on the local device.
family *family address*	Family: Lists OMP route information for the specified IP family. *family address* can be *ipv4* or *ipv6*.
vpn *vpn-id*	VPN-Specific Routes: Lists the OMP routes for the specified VPN.
received	Received Servers: Displays the services received by OMP peering sessions.
advertised	Advertised Servers: Displays the services advertised by OMP peering sessions.

Command History

Release	Modification
14.1	Command introduced.
Cisco SD-WAN Release 20.7.1	**advertised** and **received** are added in this release.
Cisco SD-WAN Release 20.7.1	Added **REGION ID** to the output to show the Hierarchical SD-WAN region ID.
Cisco SD-WAN Release 20.8.1	Added **PREFERENCE** and **AFFINITY GROUP NUMBER** to the output to indicate the affinity group preference order and the affinity ID.

Examples

The following is a sample output from the **show omp routes** command:

```
vEdge# show omp routes
------------------------------------------------
omp route entries for vpn 1 route 10.2.2.0/24
------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
path-id         70
label           1005
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.11
     type             installed
     tloc             172.16.255.11, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id       1
     site-id          100
     region-id        None
     region-path      65534
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
```

The following is a sample output from the **show omp routes vpn detail** command:

```
vEdge# show omp routes vpn 1 172.16.255.118/32 detail
------------------------------------------------
omp route entries for vpn 1 route 172.16.255.118/32
------------------------------------------------
            RECEIVED FROM:
peer            172.16.255.19
path-id         1118
label           1005
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.16
     type             installed
     tloc             172.16.255.16, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id       1
     site-id          600
     region-id        None
     region-path      65534
     preference       not set
     tag              not set
     origin-proto     eBGP
     origin-metric    0
```

```
     as-path          not set
     community        not set
     unknown-attr-len not set
            RECEIVED FROM:
peer            172.16.255.20
path-id         1093
label           1005
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.16
     type             installed
     tloc             172.16.255.16, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id       1
     site-id          600
     region-id        None
     region-path      65534
     preference       not set
     tag              not set
     origin-proto     eBGP
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
% No entries found.
```

The following is a sample output from the **show omp routes vpn received** command:

```
vEdge# show omp routes vpn 1  received
-------------------------------------------------
omp route entries for vpn 1 route 10.2.2.0/24
-------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
path-id         70
label           1005
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.11
     type             installed
     tloc             172.16.255.11, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id       1
     site-id          100
     region-id        None
     region-path      65534
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
```

The following is a sample output from the **show omp routes vpn advertised** command:

```
vEdge# show omp routes vpn 1 advertised
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

VPN    PREFIX              TO PEER
-----------------------------------------
1      10.2.2.0/24         172.16.255.19
                           172.16.255.20
1      10.2.3.0/24         172.16.255.19
                           172.16.255.20
1      172.16.255.112/32   172.16.255.19
                           172.16.255.20
```

The following is a sample output from the **show omp routes received detail** command:

```
vEdge# show omp routes received detail
-------------------------------------------------
omp route entries for vpn 1 route 10.2.2.0/24
-------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
path-id         70
label           1005
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.11
     type             installed
     tloc             172.16.255.11, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id       1
     site-id          100
     region-id        None
     region-path      65534
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
```

The following is a sample output from the **show omp routes advertised detail** command:

```
vEdge# show omp routes advertised  detail
-------------------------------------------------
omp route entries for vpn 1 route 10.2.2.0/24
-------------------------------------------------
            ADVERTISED TO:
```

```
peer    172.16.255.19
    Attributes:
     originator       172.16.255.11
     label            1005
     path-id          70
     tloc             172.16.255.11, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     site-id          100
     overlay-id       1
     preference       not set
     region-id        None
     region-path      65534
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
            ADVERTISED TO:
peer    172.16.255.20
    Attributes:
     originator       172.16.255.11
     label            1005
     path-id          70
     tloc             172.16.255.11, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     site-id          100
     overlay-id       1
     preference       not set
     region-id        None
     region-path      65534
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
```

Related Topics

clear omp routes, on page 604
show control connections, on page 788
show omp peers, on page 910
show omp services, on page 919
show omp summary, on page 921
show omp tlocs, on page 924

show omp services

show omp services—Display the services learned from OMP peering sessions (on vSmart controllers and Cisco vEdge devices only).

Command Syntax

show omp services [**vpn** *vpn-id*] [**detail**]

show omp services [**advertised** | **received**] [**vpn** *vpn-id*] [**detail**]

show omp services [**vpn** *vpn-id*] **originator** *ip-address* [**advertised** | **received**] [**detail**]

show omp services [**vpn** *vpn-id*] **service** *service-name* [**advertised** | **received**] [**detail**]

Syntax Description

	None: List information about the services learned from OMP peering sessions.
advertised	Advertised Services: List information about the services advertised by OMP peering sessions.
detail	Detailed Information: Display detailed information.
received	Received Services: List information about the services received by OMP peering sessions.
originator *ip-address*	Service Originator: List the services learned from a specific OMP peer.
service *service-name*	Specific Service: List information about the specific service.
vpn *vpn-id*	VPN: List OMP service information learned from a specific VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vSmart# show 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
```

Related Topics

show control connections, on page 788
show omp peers, on page 910
show omp routes, on page 914
show omp summary, on page 921
show omp tlocs, on page 924

show omp summary

show omp summary—Display information about the OMP sessions running between vSmart controllers and Cisco vEdge devices (on vSmart controllers and Cisco vEdge devices only).

Command Syntax

show 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.

Field	Explanation
personality	Cisco vEdge device personality.
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.
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.
vsmart-peers	Number of vSmart peers that are up.

Command History

Release	Modification
14.1	Command introduced.
Cisco SD-WAN Release 20.6.1	Added device-role and region-id fields.

Example

```
vEdge# show 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 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
```

Related Topics

show control connections, on page 788
show omp peers, on page 910
show omp routes, on page 914
show omp services, on page 919
show omp tlocs, on page 924

show omp tlocs

To display information learned from the TLOC routes advertised over the OMP sessions running between and Cisco Catalyst SD-WAN Controllers and Cisco vEdge devices only, use the **show omp tlocs** command in privileged EXEC mode.

Command Syntax

show omp tlocs [**detail**] [**color lte**] [**encap ipsec**] [**ip** *ip-address*] [**advertised**] [**received**]

Syntax Description

	None: Lists information about all TLOCs that the local device has learned about.
detail	Detailed information: Displays the detailed information.
color lte	Color Information: Displays the TLOC color information.
encap ipsec	TLOC Encapsulation: Displays the TLOC encapsulation information.
ip *ip-address*	TLOC IP Address: Displays the TLOC IP address.
received	Received Servers: Displays the services received by OMP peering sessions.
advertised	Advertised Servers: Displays the services advertised by OMP peering sessions.

Command History

Release	Modification
14.1	Command introduced.
16.3	Add display of IPv6 information.
Cisco SD-WAN Release 20.7.1	**advertised** and **received** are added in this release.

Examples

The following is a sample output from the **show omp tlocs** command:

```
vEdge# show omp tlocs
-------------------------------------------------
tloc entries for 172.16.255.11
                 lte
                 ipsec
-------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
status          C,Red,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         357
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.0.5.11
     public-port       12347
     private-ip        10.0.5.11
     private-port      12347
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     bfd-status        up
     domain-id         not set
     site-id           100
     overlay-id        not set
     preference        0
     region-id         None
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x80000014
     carrier           default
     restrict          0
     on-demand          0
     groups            [ 0 ]
     bandwidth         0
     qos-group         default-group
     border             not set
     unknown-attr-len  not set
```

The following is a sample output from the **show omp tlocs advertised** command:

```
vEdge# show omp tlocs advertised
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Stg -> staged
IA  -> On-demand inactive
Inv -> invalid

ADDRESS
```

```
FAMILY   TLOC IP          COLOR            ENCAP  TO PEER
-------------------------------------------------------------------------
ipv4     172.16.255.11    lte              ipsec  172.16.255.19
                                                   172.16.255.20
```

The following is a sample output from the **show omp tlocs received** command:

```
vEdge# show omp tlocs received
----------------------------------------------------
tloc entries for 172.16.255.11
                 lte
                 ipsec
----------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
status          C,Red,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         357
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.0.5.11
     public-port       12347
     private-ip        10.0.5.11
     private-port      12347
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     bfd-status        up
     domain-id         not set
     site-id           100
     overlay-id        not set
     preference        0
     region-id         None
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x80000014
     carrier           default
     restrict          0
     on-demand          0
     groups            [ 0 ]
     bandwidth         0
     qos-group         default-group
     border             not set
     unknown-attr-len  not set
```

The following is a sample output from the **show omp tlocs received detail** command:

```
vEdge# show omp tlocs received detail
----------------------------------------------------
tloc entries for 172.16.255.14
                 lte
                 ipsec
----------------------------------------------------
            RECEIVED FROM:
peer            172.16.255.19
```

```
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         443
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.1.14.14
     public-port       12366
     private-ip        10.1.14.14
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     bfd-status        up
     domain-id         not set
     site-id           400
     overlay-id        not set
     preference        0
     region-id         None
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x80000000
     carrier           default
     restrict          0
     on-demand          0
     groups            [ 0 ]
     bandwidth         0
     qos-group         default-group
     border             not set
     unknown-attr-len  not set
           RECEIVED FROM:
peer            172.16.255.20
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         443
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.1.14.14
     public-port       12366
     private-ip        10.1.14.14
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     bfd-status        up
     domain-id         not set
     site-id           400
     overlay-id        not set
     preference        0
```

```
 region-id          None
 tag                not set
 stale              not set
 weight             1
 version            3
gen-id              0x80000000
 carrier            default
 restrict           0
 on-demand           0
 groups             [ 0 ]
 bandwidth          0
 qos-group          default-group
 border              not set
 unknown-attr-len   not set
```

Related Topics

clear omp tlocs, on page 604
show control connections, on page 788
show omp peers, on page 910
show omp routes, on page 914
show omp services, on page 919
show omp summary, on page 921

show omp verify-routes

To verify if a route prefix is available, use the **show omp verify-routes** command in privileged EXEC mode.

show omp verify-routes vpn *vpn-id prefix/length*

Syntax Description

vpn	Lists the Overlay Management Protocol (OMP) routes for the specified VPN.
vpn-id	Specifies the VPN ID to be verified.
prefix/length	Specifies route prefix and length. Lists OMP route information for the specified route prefix.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.8.1	This command was introduced.

Usage Guidelines

This command helps to reduce the number of steps needed for troubleshooting an OMP prefix by verifying the received and installed RIB and FIB entries, corresponding TLOCs, and BFD sessions.

Examples

The following is a sample output from the **show omp verify-routes** command displaying a prefix table with the prefix's verification details:

```
Device# show omp verify-routes vpn 1 10.2.2.0/24
Codes Route/TLOC Status:
C    -> chosen
I    -> installed
Red  -> redistributed
Rej  -> rejected
L    -> looped
R    -> resolved
S    -> stale
Ext  -> extranet
Inv  -> invalid
Stg  -> staged
O    -> On-demand inactive
U    -> TLOC unresolved
Codes Rib Status:
    F -> fib, S -> selected, I -> inactive,
    B -> blackhole, R -> recursive, L -> import

               PATH                      ATTRIBUTE
STATUS      BFD      RIB
FROM PEER       ID     LABEL  STATUS      TYPE       TLOC IP         COLOR  ENCAP   TLOC
PREFERENCE  STATUS  STATUS
--------------------------------------------------------------------------------------------
172.16.255.19    8      1005   C,I,R    installed    172.16.255.11   lte   ipsec   C,I,R
    -        up      F,S
172.16.255.19    9      1005   C,R      installed    172.16.255.11   3g    ipsec   C,R
    -        up       -
```

Table 22: show omp verify-routes Field Descriptions

Field	Description
FROM PEER	Displays the IP address of the peer from which the route is received.
PATH ID	Displays the ID of the OMP path.
LABEL	Displays the service label.
STATUS	Displays the status information codes of routes.
ATTRIBUTE TYPE	Displays the attribute type information regarding the route installation in RIB.
TLOC IP	Displays the TLOC IP address.
TLOC COLOR	Displays the TLOC color information.
TLOC ENCAP	Displays the TLOC encapsulation information.
TLOC STATUS	Displays the status information codes of TLOC.
PREFERENCE	Displays the preference information of TLOC.
BFD STATUS	Displays the connectivity status of a BFD session of a route.
RIB STATUS	Displays the code information of routes installed in RIB.

show orchestrator connections

show orchestrator connections—List the Cisco SD-WAN devices that have active DTLS connections to the vBond orchestrator (on vBond orchestrators only).

Command Syntax

show orchestrator connections [**vsmart** [*site-id*]] [**detail**]

Syntax Description

	None: List information about all the Cisco SD-WAN devices that have active DTLS connections to the vBond orchestrator.
vsmart [*site-id*]	Connections to vSmart Controllers: List information about the vSmart controllers that have active DTLS connections to the vBond orchestrator or about a vSmart controller at a specific site in the Cisco SD-WAN network.
detail	Detailed Information: Display information about the vBond connections and about the handshaking packets that are exchanged when a connection is being established, maintained, and torn down.

Output Fields

For the State columen, the operational state can be one of the following: challenge, challenge_ack, challenge_resp, connect, down, handshake, tear_down, trying, and up.

The remaining output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Examples

Example 1

```
vBond# show orchestrator connections
                                                                                PEER                    PEER
PEER     PEER     PEER             SITE        DOMAIN      PEER               PRIVATE  PEER              PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP         PORT     PUBLIC IP         PORT    REMOTE COLOR
  STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------
vsmart   dtls     172.16.255.19    100         1           10.0.5.19          12346    10.0.5.19         12346   default
  up              0:03:26:04
```

```
vsmart   dtls     172.16.255.19    100         1           10.0.5.19        12446    10.0.5.19        12446   default
  up              0:03:26:04
vsmart   dtls     172.16.255.20    200         1           10.0.12.20       12346    10.0.12.20       12346   default
  up              0:03:26:10
vsmart   dtls     172.16.255.20    200         1           10.0.12.20       12446    10.0.12.20       12446   default
  up              0:03:26:10
vmanage  dtls     172.16.255.22    200         0           10.0.12.22       12346    10.0.12.22       12346   default
  up              0:03:26:09
vmanage  dtls     172.16.255.22    200         0           10.0.12.22       12446    10.0.12.22       12446   default
  up              0:03:26:09
```

Example 2

```
vBond# show orchestrator connections  detail

----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 172.16.255.19   PEER-PERSONALITY- vsmart
----------------------------------------------------------------------------------------------
site-id             100
domain-id           1
protocol            dtls
private-ip          10.0.5.19
private-port        12346
public-ip           10.0.5.19
public-port         12346
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:03:26:48
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   12408
    connects                780
    registers               0
    register-replies        365
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0

  Rx Statistics-
  --------------
    hello                   12408
    connects                0
    registers               365
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    vmanage-to-peer         0
    register-to-vmanage     0
...
```

Related Topics

show control connections, on page 788
show orchestrator local-properties, on page 935
show orchestrator statistics, on page 937

show orchestrator connections-history

show orchestrator connections-history—List the history of connections and connection attempts made by the vBond orchestrator (on vBond orchestrators only).

Command Syntax

show orchestrator connections-history [*index*] [**detail**]

show orchestrator connections-history *connection-parameter* [**detail**]

Syntax Description

	None: List the history of connections and connection attempts between Cisco vEdge devices and the vBond orchestrator.
detail	Detailed Output: List detailed connection history information and information about the handshaking packets that are exchanged when a connection is being established, maintained, and torn down.
connection-parameter	Specific Connection Parameter: List the connection history only for those items match the connection parameter. *connection-parameter* can be one of the following: **domain-id, peer-type**, **private-ip**, **private-port**, **public-ip**, **public-port**, **site-id**, and **system-ip**. These values corresponds to the column headers in the output of the show orchestrator connections-history command.
index	Specific History Item: List the connection history only for the specific item in the history list.

Output Fields

Field	Explanation
Domain ID	Administrative state of the interface: • state-down—The interface has not been configured. state-up—The interface has been configured.
Index	Index counter of the connection operation. The initial operation has an index of 0. The newest operation is listed first.

Field	Explanation
Peer Type	Type of Cisco SD-WAN device: • vmanage—vManage management configuration system. vsmart—vSmart controller.
Private IP	Private IP address of the connected Cisco SD-WAN device. If the Cisco SD-WAN device is behind a NAT device, the private and public IP addresses are different.
Private Port	Private UDP port number used to connect to the vBond orchestrator. If the Cisco SD-WAN device is behind a NAT device, the private and public UDP port numbers are likely different.
Public IP	Public IP address of the connected Cisco SD-WAN device.
Public Port	Public UDP port number used to connect to the vBond orchestrator.
Site ID	Identifier of the Cisco SD-WAN administrative site where the connected Cisco SD-WAN device is located.
State	Operational state of the connection to the Cisco SD-WAN device. It can be one of the following: challenge, challenge_ack, challenge_resp, connect, down, handshake, tear_down, trying, and up.
System IP	System IP address of the Cisco SD-WAN device.
Uptime	How long the connection between the Cisco SD-WAN device and the vBond orchestrator has been up and operational.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vEdge# show orchestrator connections-history
Legend for Errors
BDSGVERFL  - Board ID signature verify failure        ORPTMO    - Remote client peer timeout
```

```
BIDNTPR    - Board ID not initialized                RMGSPR    - Remove global saved peer
BIDNTVRFD  - Peer board ID certificate not verified  RXTRDWN   - Received teardown
CRTREJSER  - Challenge response rejected by peer     RDSIGFBD  - Read signature from board ID failed
CRTVERFL   - Fail to verify peer certificate         SSLNFAIL  - Failure to create new SSL context
CTORGNMMIS - Certificate organization name mismatch  SERNTPRES - Serial number not present
DCONFAIL   - DTLS connection failure                 TMRALC    - Memory failure
DEVALC     - Device memory allocation failures       TUNALC    - Memory failure
DHSTMO     - DTLS handshake timeout                  UNMSGBDRG - Unknown message type or bad register message
DISCVBD    - Disconnect vBond after register reply   UNAUTHEL  - Recd hello from unauthenticated peer
DISTLOC    - TLOC disabled                           VBDEST    - vDaemon process terminated
DUPSER     - Duplicate serial number                 VECRTREV  - vEdge certification revoked
IP_TOS     - Socket options failure                  VSCRTREV  - vSmart certificate revoked
LISFD      - Listener socket FD error                VB_TMO    - Peer vBond timed out
MEMALCFL   - Memory allocation failure               VM_TMO    - Peer vManage timed out
NOACTVB    - No active vBond found to connect to     VP_TMO    - Peer vEdge timed out
NOERR      - No error                                VS_TMO    - Peer vSmart timed out
NOSLPRCRT  - Unable to get peer's certificate        XTVSTRDN  - Extra vSmart teardown
```

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	LAST TIME WHEN STATE	LOCAL/REMOTE	LAST CHANGED
vedge	dtls	172.16.255.14	400	1	10.1.14.14	12350	10.1.14.14	12350	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:23:14
vedge	dtls	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:23:14
vedge	dtls	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:23:00
vedge	dtls	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:22:44
vedge	dtls	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:22:43
vedge	dtls	172.16.255.14	400	1	10.1.14.14	12350	10.1.14.14	12350	lte	trying	RXTRDWN/DISCVBD	2014-07-21T18:22:28
vmanage	dtls	172.16.255.22	200	0	10.0.12.22	12346	10.0.12.22	12346	default	tear_down	VM_TMO/NOERR	2014-07-21T18:22:28
vedge	dtls	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:47
vedge	dtls	172.16.255.14	400	1	10.1.14.14	12350	10.1.14.14	12350	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:46
vedge	dtls	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:46
vedge	dtls	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:31
vedge	dtls	172.16.255.14	400	1	10.1.14.14	12350	10.1.14.14	12350	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:31
vedge	dtls	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:31
vsmart	dtls	172.16.255.20	100	1	10.0.12.20	12346	10.0.12.20	12346	default	up	RXTRDWN/DISTLOC	2014-07-21T13:39:15
vedge	dtls	172.16.255.16	600	1	10.1.16.16	12346	10.1.16.16	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:10
vedge	dtls	172.16.255.14	400	1	10.1.14.14	12350	10.1.14.14	12350	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:10
vedge	dtls	172.16.255.15	500	1	10.1.15.15	12346	10.1.15.15	12346	lte	trying	RXTRDWN/DISCVBD	2014-07-21T13:39:10

Example 2

```
vEdge# show orchestrator connections-history 0 detail
-------------------------------------------------------------------------------
 REMOTE-COLOR- lte SYSTEM-IP- 172.16.255.15   PEER-PERSONALITY- vedge
-------------------------------------------------------------------------------
site-id             500
domain-id           1
protocol            dtls
private-ip          10.1.15.15
private-port        12346
```

```
public-ip           10.1.15.15
public-port         12346
state               trying [Local Err: ERR_RX_TEAR_DOWN] [Remote Err: ERR_DISCONNECT_VBOND]
downtime            2014-07-21T13:39:10

  Tx Statistics-
  --------------
    hello                   0
    connects                0
    registers               0
    register-replies        1
    challenge               1
    challenge-response      0
    challenge-ack           1
    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     0

  Rx Statistics-
  --------------
    hello                   0
    connects                0
    registers               1
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                1
    vmanage-to-peer         0
    register-to-vmanage     0
```

Related Topics

show control connections, on page 788
show orchestrator local-properties, on page 935
show orchestrator statistics, on page 937

show orchestrator local-properties

show orchestrator local-properties—Display the basic configuration parameters of a vBond orchestrator (on vBond orchestrators only).

Command Syntax

show orchestrator local-properties [*parameter*]

Syntax Description

	None: Display the basic vBond configuration parameters.
parameter	Information about a Specific Parameter: Display configuration information about a specific parameter. *parameter* can be one of the following: **board-serial**, **certificate-not-valid-after**, **certificate-note-valid-before,** **certificate-status**, **certificate-validity**, **device-type**, **number-active-wan-interfaces**, **organization-name**, **protocol**, **root-ca-chain-status**, **system-ip**, **uuid**, and **wan-interface-list**.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.
Cisco Catalyst SD-WAN Control Components Release 26.2.1 Cisco Catalyst SD-WAN Control Components Release 26.1.2 Cisco Catalyst SD-WAN Control Components Release 20.18.3	In case of an expired certificate, the **certificate-validity** field in the command output shows **Valid - Expired**. Previously it showed only **Expired**.

Usage Guidelines

From Cisco Catalyst SD-WAN Control Components Release 26.2.1 and other releases shown in the modification history, if a certificate is expired, the **certificate-validity** field in the command output shows **Valid - Expired**.

Example

```
vBond# show orchestrator local-properties
personality                   vbond
organization-name             Cisco, Inc.
system-ip                     172.16.255.14
certificate-status            Installed
root-ca-chain-status          Installed

certificate-validity          Valid
certificate-not-valid-before  Feb 16 21:07:01 2016 GMT
certificate-not-valid-after   Feb 15 21:07:01 2017 GMT
chassis-num/unique-id         8155a210-9342-459c-b404-5904895236e0
serial-num                    1234560B

number-active-wan-interfaces 1
protocol                      dtls
                                                      ADMIN    OPERATION
INDEX  IP               PORT  VSMARTS  VMANAGES  STATE    STATE
------------------------------------------------------------------------
0      10.1.14.14       12346 4        1         up        up
```

Related Topics

show control local-properties, on page 794
show orchestrator connections, on page 930
show system status, on page 1019

show orchestrator reverse-proxy-mapping

show orchestrator reverse-proxy-mapping—Display the proxy IP addresses and port numbers that are configured for use by reverse proxy (on vBond orchestrators only).

Command Syntax

show orchestrator reverse-proxy-mapping

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
18.2	Command introduced.

Example

```
vBond# show orchestrator reverse-proxy-mapping
                                                    PRIVATE               PROXY
UUID                                  PRIVATE IP    PORT      PROXY IP    PORT
------------------------------------------------------------------------------
00096956-7471-471b-99b6-15e1ba6cb187  10.0.12.19    23456     10.0.37.19  23456
00096956-7471-471b-99b6-15e1ba6cb187  10.0.12.19    23556     10.0.37.19  23556
63636bc5-b0fc-4b42-a6e8-d122357b0431  10.0.12.20    23456     10.0.37.20  23456
63636bc5-b0fc-4b42-a6e8-d122357b0431  10.0.12.20    23556     10.0.37.20  23556
cb8d64af-59bb-4c58-900a-267089977eb8  10.0.12.22    23456     10.0.37.22  23456
cb8d64af-59bb-4c58-900a-267089977eb8  10.0.12.22    23556     10.0.37.22  23556
```

Related Topics

clear reverse-proxy context, on page 616
show certificate reverse-proxy, on page 771
show control connections, on page 788
show control local-properties, on page 794

show orchestrator statistics

show orchestrator statistics—Display statistics about the packets that a vBond orchestrator has transmitted and received in the process of establishing and maintaining secure DTLS connections to Cisco SD-WAN devices in the overlay network (on vBond orchestrators only).

Command Syntax

show orchestrator statistics [*counter-name*]

Syntax Description

	None: Display statistics about handshaking packets sent and received by the vBond orchestrator as it establishes, maintains, and tears down DTLS connections to the Cisco SD-WAN devices in the overlay network.
counter-name	Statistics about a Specific Counter: Display the statistics for the specific counter.

Output Fields

Rx Statistics: Statistics about received handshaking packets.

Tx Statistics: Statistics about transmitted handshaking packets.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vBond# show orchestrator statistics

Tx Statistics:
--------------
Packets                   3180
Octets                    357705
Error                     0
Blocked                   0
Connects                  1599
Registers                 0
Register Replies          1581

DTLS Handshake            0
DTLS Handshake Failures   0
DTLS Handshake Done       0

Challenge                 25
Challenge Response        0
Challenge Ack             25
Challenge Errors          0
Challenge Response Errors 0
Challenge Ack Errors      0
Challenge General Errors  0

Rx Statistics:
--------------
Packets                   48297
Octets                    2207567
```

```
Errors                    0
Connects                  0
Registers                 1581
Register Replies          0

DTLS Handshake            74
DTLS Handshake Failures   0
DTLS Handshake Done       25

Challenge                 0
Challenge Response        25
Challenge Ack             0
Challenge Failures        0
```

Related Topics

show orchestrator connections, on page 930
show orchestrator local-properties, on page 935

show orchestrator summary

show orchestrator summary—Display a count of the Cisco vEdge devices, vManage Network Management Systems (NMSs), and vSmart controllers in the overlay network (on vBond orchestrators only). For vBond orchestrators running on virtual machines (VMs) that have more than one core, this command shows the number of devices that each vdaemon process is handling.

Command Syntax

show orchestrator summary [*instance*]

Syntax Description

	None: Display a count of all the Cisco vEdge devices, vManage NMSs, and vSmart controllers in the overlay network.
instance	Devices for a Specific vdaemon Process: Display a count of devices for a specific instance of a vdaemon process. Cisco SD-WAN devices that run on VMs that have more than one core automatically spawn one vdaemon process for each core, to load-balance the Cisco SD-WAN software functions across all the CPUs in the VM server.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.
15.4	Add support for multiple vdaemon processes.

Release	Modification
16.3	Add support for IPv6.

Example

```
vBond# show orchestrator summary

          VMANAGE  VSMART  VEDGE             LISTENING   LISTENING  LISTENING
INSTANCE  COUNTS   COUNTS  COUNTS  PROTOCOL  IP          IPV6       PORT
-------------------------------------------------------------------------------
0         2        4       0       dtls      10.1.14.14  ::         12346
```

Related Topics

show control summary, on page 800
show orchestrator connections, on page 930

show orchestrator valid-vedges

show orchestrator valid-vedges—List the chassis numbers of the valid Cisco vEdge devices in the overlay network (on vBond orchestrators only).

Command Syntax

show orchestrator valid-vedges

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.
14.2	Command renamed from **show orchestrator valid-devices**.

Example

```
vBond# show orchestrator valid-vedges

                SERIAL
CHASSIS NUMBER  NUMBER    VALIDITY
----------------------------------
11OD113140004   10000266  valid
11OD145130082   10000142  staging
11OD252130046   100001FF  valid
```

```
11OD252130049   1000020B  valid
11OD252130057   1000020C  staging
R26OC126140004  10000369  valid
```

Related Topics

show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator connections, on page 930
show orchestrator valid-vmanage-id, on page 941
show orchestrator valid-vsmarts, on page 942

show orchestrator valid-vmanage-id

show orchestrator valid-vmanage-id—List the chassis numbers of the valid vManage NMSs in the overlay network (on vBond orchestrators only).

Command Syntax

show orchestrator valid-vmanage-id [*serial-number*]

Syntax Description

	None: Display the chassis numbers of all valid vManage NMSs in the overlay network.
serial-number	Serial Number: List whether a specific vManage chassis number is valid.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3.1	Command introduced.

Example

```
vBond# show orchestrator valid-vmanage-id

CHASSIS NUMBER
--------------------------------------
72d0229c-7bb6-4bfd-b7f3-648fc78392c7
db51d941-9055-44a3-8f9f-09e305e0d60e
f23cfb69-8485-4e95-b02a-f5b27c9809b7
```

Related Topics

show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator connections, on page 930
show orchestrator valid-vedges, on page 940
show orchestrator valid-vsmarts, on page 942

show orchestrator valid-vsmarts

show orchestrator valid-vsmarts—List the serial numbers of the valid vSmart controllers in the overlay network (on vBond orchestrators only).

Command Syntax

show orchestrator valid-vsmarts [*serial-number*]

Syntax Description

	None: Display the serial numbers of all valid vSmart controllers in the overlay network.
serial-number	Serial Number: List whether a specific vSmart serial number is valid.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vBond# show orchestrator valid-vsmarts

SERIAL
NUMBER
----------
12345601
12345602
```

Related Topics

show control valid-vedges, on page 801
show control valid-vsmarts, on page 802
show orchestrator connections, on page 930

show orchestrator valid-vedges, on page 940
show orchestrator valid-vmanage-id, on page 941
show orchestrator valid-vsmarts, on page 942

show ospf database

show ospf database—List the entries in the OSPF Link-State Advertisement (LSA) database (on Cisco vEdge devices only).

Command Syntax

show ospf database [**vpn** *vpn-id*] [*ospf-parameter*] [**detail**]

Syntax Description

	None: List all the entries in the OSPF LSA database.
detail	Detailed Information: List detailed information about the entries in the OSPF LSA database.
ospf-parameter	Specific OSPF Property: List information about a specific OSPF property. *ospf-property* can be one of the following: **adv-route**, **area**, **area-local-opaque**, **as-external-opaque**, **asbr-summary**, **external**, **group-member**, **link-id**, **link-local-opaque**, **network**, **nssa-external**, **router**, **summary**, and **type-ext-attributes**.
vpn *vpn-id*	VPN-Specific Routes List the OSPF routing process information for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vEdge# show ospf database
             LSA               LINK            ADVERTISING
VPN    AREA  TYPE              ID              ROUTER          AGE      CHECKSUM  SEQ#
-------------------------------------------------------------------------------------
0      51    router            172.16.255.11   172.16.255.11   624      0xe19f    0x80000004
```

```
0       51    router            172.16.255.13    172.16.255.13    622      0x2dd9    0x80000010
0       51    router            172.16.255.14    172.16.255.14    622      0xb6ad    0x80000004
0       51    router            172.16.255.15    172.16.255.15    623      0xca94    0x80000004
0       51    router            172.16.255.16    172.16.255.16    625      0xde7b    0x80000004
0       51    router            172.16.255.21    172.16.255.21    623      0xcb96    0x80000005
0       51    network           10.0.5.13        172.16.255.13    623      0x8f7c    0x80000002
0       51    network           10.1.14.13       172.16.255.13    622      0xa134    0x80000001
0       51    network           10.1.15.13       172.16.255.13    623      0xa42f    0x80000001
0       51    network           10.1.16.13       172.16.255.13    625      0xa72a    0x80000001
1       0     router            172.16.255.11    172.16.255.11    699      0xc5bd    0x80000003
1       0     router            172.16.255.12    172.16.255.12    699      0xce55    0x80000007
1       0     router            172.16.255.21    172.16.255.21    704      0x2238    0x80000003
1       0     network           10.2.2.12        172.16.255.12    700      0xf9ec    0x80000001
1       0     network           10.2.3.21        172.16.255.21    704      0xe6e2    0x80000001
```

Example 2

```
vEdge# show ospf database area 0 detail

      OSPF Router with ID - <172.16.255.11>

      Router Link States <VPN 1 AREA 0>

LS age - 489
Options - 0x2 <E>
LS Flags - 0x3
Flags - 0x2 <ASBR>
LS Type - router-LSA
Link State ID - 172.16.255.11
Advertising Router - 172.16.255.11
LS Seq Number - 0x8000001c
Checksum - 0x93d6
Length - 36
  Number of Links - 1

      Link connected to - a transit Network
       (Link Id) Designated Router address - 10.2.2.12
       (Link Data) Router Interface Address - 10.2.2.11
        Number of TOS metrics - 0
        TOS 0 Metric - 10
...
```

Related Topics

clear ospf database, on page 607
show ospf database-summary, on page 944
show ospf interface, on page 945
show ospf neighbor, on page 947
show ospf process, on page 948
show ospf routes, on page 950

show ospf database-summary

show ospf database-summary—List how many of each type of LSA is present in the OSPF database, along with the total number of LSAs in the database (on Cisco vEdge devices only).

Command Syntax

show ospf database-summary [**vpn** *vpn-id*] [*ospf-lsa*]

Syntax Description

	None: List a summary of all the LSAs in the OSPF LSA database.
ospf-lsa	Specific OSPF LSA Type: List information about a specific OSPF LSA. *ospf-lsa* can be one of the following: **as-external-lsa**, **network-lsa**, **nssa-lsa**, **router-lsa**, **summary-lsa**, and **total-lsa**.
vpn *vpn-id*	VPN-Specific Routes List the OSPF routing process information for the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show ospf database-summary

                                        AS
            ROUTER  NETWORK  SUMMARY  EXTERNAL  NSSA  TOTAL
VPN  AREA   LSA     LSA      LSA      LSA       LSA   LSA
-------------------------------------------------------------
0    51     6       4        0        0         0     10
```

Related Topics

show ospf database, on page 943
show ospf interface, on page 945
show ospf neighbor, on page 947
show ospf process, on page 948
show ospf routes, on page 950

show ospf interface

show ospf interface—Display information about interfaces that are running OSPF (onCisco vEdge devices only).

Command Syntax

show ospf interface [**vpn** *vpn-id*]

show ospf route vpn *vpn-id*[*ip-address* [*interface-index* [*ospf-property*]]]

Syntax Description

	None: List standard information about all interfaces that are running OSPF.
if-name *interface-name*	OSPF Interface: Display interface-specific OSPF information.
vpn *vpn-id ip-address* [*interface-index*[*ospf-property*]]	Specific OSPF Interface Information: Display information about the OSPF interface in the specified VPN and with the specified IP address, and optionally for a specific interface index and a specific OSPF property on that interface. *ospf-property* can be one of the fields in the **show ospf interface** command output.
vpn *vpn-id*	VPN-Specific Interfaces: Display information about the OSPF interfaces in the specified VPN.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show ospf interface vpn 1
ospf interface vpn 1 10.2.2.11/24 0
 if-name                     ge0/0
 mtu                         1500
 bandwidth                   0
 area-addr                   0
 mtu-mismatch                true
 router-id                   172.16.255.11
 if-type                     broadcast
 cost                        10
 delay                       1
 ospf-if-state               if-backup
 priority                    1
 designated-router-id        172.16.255.12
 backup-designated-router-id 172.16.255.11
 designated-router-ip        10.2.2.12
 backup-designated-router-ip 10.2.2.11
 members                     designated
 hello-timer                 10
```

```
dead-interval               40
retransmit-timer            5
neighbor-count              1
adj-neighbor-count          1
hello-due-time              5
oper-state                  true
```

Related Topics

show ospf database, on page 943
show ospf database-summary, on page 944
show ospf neighbor, on page 947
show ospf routes, on page 950

show ospf neighbor

show ospf neighbor—List information about OSPF neighbors (on vEdge routers only).

Command Syntax

show ospf neighbor [**detail**] [**vpn** *vpn-id*]

show ospf route vpn *vpn-id* [*ip-address*[*ospf-property*]]

Syntax Description

	None: List standard information about OSPF neighbors.
detail	Detailed Information: List detailed information about OSPF neighbors.
vpn *vpn-id ip-address* [*ospf-property*]	Specific OSPF Route Information: List the information about entries for specific OSPF route and, optionally, for a specific interface index and a specific OSPF property on that interface. For a list of OSPF properties, see the fields in the **show ospf neighbor detail** command output, shown below.
vpn *vpn-id*	VPN-Specific Routes: List only the OSPF neighbors in the specified VPN.

Command History

Release	Modification
14.1	Command introduced.

Examples

Example 1

```
vEdge# show ospf neighbor
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List
                INTERFACE  IF                                    DEAD

VPN  ADDRESS    INDEX      NAME   NEIGHBOR ID    STATE    PRI   TIMER  DBsmL  RqstL  RXmtL

-------------------------------------------------------------------------------------------
0    10.0.5.13  0          ge0/2  172.16.255.13  full     13    36     0      0      0

0    10.0.5.21  0          ge0/2  172.16.255.21  two-way  0     36     0      0      0

1    10.2.2.12  0          ge0/0  172.16.255.12  full     1     36     0      0      0
```

Example 2

```
vEdge# show ospf neighbor vpn 1 detail
ospf neighbor vpn 1 neighbor 10.2.2.12 interface-index 0
 if-name                     ge0/0
 router-id                   172.16.255.12
 if-address                  10.2.2.12
 area                        0
 area-type                   regular
 neighbor-state              full
 interface-state             if-dr
 priority                    1
 state-changes               6
 progressive-change-time     504
 designated-router-id        10.2.2.12
 backup-designated-router-id 10.2.2.11
 dead-timer                  30
 db-summary-list             0
 link-state-req-list         0
 link-state-retrans-list     0
 options                     E
```

Related Topics

show ospf database, on page 943
show ospf database-summary, on page 944
show ospf interface, on page 945
show ospf process, on page 948
show ospf routes, on page 950

show ospf process

show ospf process—Display information about each OSPF routing process running on the vEdge router (on vEdge routers only).

Command Syntax

show ospf process [**vpn** *vpn-id*] [*ospf-property*]

show ospf process area *area-id* [*ospf-property*]

Syntax Description

	None: List information about the OSPF routing process.
area *area-id* [*ospf-property*]	Specific OSPF Property: List information about a specific OSPF property. *ospf-property* can be one of the fields in the **show ospf process** command output, shown below.
vpn *vpn-id*	VPN-Specific Routes: List the OSPF routing process information for the specified VPN.

Command History

Release	Modification
14.1	Command introduced.

Examples

```
vEdge# show ospf process
ospf process vpn 0
 router-id             172.16.255.11
 rfc1583-compatible    true
 spf-delay             200
 spf-holdtime          1000
 spf-max-holdtime      10000
 spf-hold-multiplier   3
 spf-last-exec-time    1030
 lsa-refresh-interval  10
 external-lsa-count    0
 external-lsa-checksum 0
 number-areas          1
 ignore-down-bit       false
 hello-received        230
 hello-sent            116
 dbd-received          4
 dbd-sent              6
 ls-req-received       2
 ls-req-sent           2
 ls-upd-received       24
 ls-upd-sent           8
 ls-ack-received       9
 ls-ack-sent           11
 area 51
  num-interfaces       1
  num-full-adj-routers 2
  spf-exec-count       12
  lsa-count            10
  router-lsa-count     6
```

```
  router-lsa-checksum  277194
  network-lsa-count    4
  network-lsa-checksum 162825
  summary-lsa-count    0
  summary-lsa-checksum 0
  asbr-lsa-count       0
  asbr-lsa-checksum    0
  nssa-lsa-count       0
  nssa-lsa-checksum    0
ospf process vpn 1
 router-id             172.16.255.11
 rfc1583-compatible    true
 spf-delay             200
 spf-holdtime          1000
 spf-max-holdtime      10000
 spf-hold-multiplier   3
 spf-last-exec-time    1030
 lsa-refresh-interval  10
 external-lsa-count    15
 external-lsa-checksum 464360
 number-areas          1
 ignore-down-bit       false
 hello-received        122
 hello-sent            123
 dbd-received          3
 dbd-sent              3
 ls-req-received       1
 ls-req-sent           1
 ls-upd-received       27
 ls-upd-sent           24
 ls-ack-received       6
 ls-ack-sent           8
 area 0
  backbone-area        true
  num-interfaces       1
  num-full-adj-routers 1
  spf-exec-count       8
  lsa-count            5
  router-lsa-count     3
  router-lsa-checksum  112202
  network-lsa-count    2
  network-lsa-checksum 122064
  summary-lsa-count    0
  summary-lsa-checksum 0
  asbr-lsa-count       0
  asbr-lsa-checksum    0
  nssa-lsa-count       0
  nssa-lsa-checksum    0
```

Related Topics

show ospf database, on page 943
show ospf database-summary, on page 944
show ospf interface, on page 945
show ospf neighbor, on page 947
show ospf routes, on page 950

show ospf routes

Display the entries that the route table has learned from OSPF (on vEdge routers only).

show ospf routes [**detail**] [*prefix*/*length*] [**vpn** *vpn-id*]**show ospf routes vpn** *vpn-id* [*route-type* [*prefix*/*length*]]

Syntax Description

None	List standard information about the entries the route table has learned from OSPF.
Detailed Information	**detail** List detailed information about the entries the route table has learned from OSPF.
Route Prefix	*prefix*/*length prefix* **vpn** *vpn-id* List route information for the specified route prefix learned from OSPF. If you omit the prefix length, you must specify a VPN identifier so that the Cisco SD-WAN software can find the route that best matches the prefix.

Specific OSPF Route Type	*route-type* [*prefix*/*length*] List the information about entries for specific OSPF route types and optionally learned from the specified IP prefix. For a list of route types, see the Output Fields table below.
VPN-Specific Routes	**vpn** *vpn- id* List only the route table entries for the specified VPN.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show ospf routes

```
vEdge# show ospf routes

     ROUTE                                                          DEST               IF
VPN  TYPE      PREFIX             ID  AREA  COST  PATH TYPE   TYPE     NEXT HOP   NAME
-------------------------------------------------------------------------------------------
0    router    172.16.255.13/32   0   51    10    intra-area  router   10.0.5.13  ge0/2
0    network   10.0.5.0/24        0   51    10    intra-area  network  0.0.0.0    ge0/2
0    network   10.0.12.0/24       0   51    20    intra-area  network  10.0.5.13  ge0/2
0    network   10.1.14.0/24       0   51    20    intra-area  network  10.0.5.13  ge0/2
0    network   10.1.15.0/24       0   51    20    intra-area  network  10.0.5.13  ge0/2
0    network   10.1.16.0/24       0   51    20    intra-area  network  10.0.5.13  ge0/2
1    router    172.16.255.12/32   0   0     10    intra-area  router   10.2.2.12  ge0/0
1    router    172.16.255.21/32   0   0     20    intra-area  router   10.2.2.12  ge0/0
1    network   10.2.2.0/24        0   0     10    intra-area  network  0.0.0.0    ge0/0
1    network   10.2.3.0/24        0   0     20    intra-area  network  10.2.2.12  ge0/0
1    external  172.16.255.112/32  0   -     -     external2   network  10.2.2.12  ge0/0

vEdge# show ospf routes detail

     ROUTE                                                                  DEST          TYPE2
          IF
VPN  TYPE      PREFIX             ID  AREA  COST  FLAGS  PATH TYPE   TYPE     TAG  COST
NEXT HOP   NAME
-------------------------------------------------------------------------------------------------------
0    router    172.16.255.13/32   0   51    10    2      intra-area  router   -    -
10.0.5.13  ge0/2
```

```
0    network   10.0.5.0/24        0   51    10    0      intra-area  network  -    -
0.0.0.0    ge0/2
0    network   10.0.12.0/24       0   51    20    0      intra-area  network  -    -
10.0.5.13  ge0/2
0    network   10.1.14.0/24       0   51    20    0      intra-area  network  -    -
10.0.5.13  ge0/2
0    network   10.1.15.0/24       0   51    20    0      intra-area  network  -    -
10.0.5.13  ge0/2
0    network   10.1.16.0/24       0   51    20    0      intra-area  network  -    -
10.0.5.13  ge0/2
1    router    172.16.255.12/32   0   0     10    2      intra-area  router   -    -
10.2.2.12  ge0/0
1    router    172.16.255.21/32   0   0     20    2      intra-area  router   -    -
10.2.2.12  ge0/0
1    network   10.2.2.0/24        0   0     10    0      intra-area  network  -    -
0.0.0.0    ge0/0
1    network   10.2.3.0/24        0   0     20    0      intra-area  network  -    -
10.2.2.12  ge0/0
1    external  172.16.255.112/32  0   -     -     83     external2   network  0    20
10.2.2.12  ge0/0
```

Related Topics

show ip routes, on page 865
show ospf database, on page 943
show ospf database-summary, on page 944
show ospf interface, on page 945
show ospf neighbor, on page 947
show ospf process, on page 948

show packet-capture

To view details of the packets captured, use the **show packet-capture** command in privileged EXEC mode.

show packet-capture [**details** [**interface** *interface-name* | **packets-captured** *packets* | **session-id** *session-id* | **vpn** *vpn-id*]]

Syntax Description

interface *interface-name*	(Optional) Name of the interface.
packets-captured *packets*	(Optional) Number of packets.
session-id *session-id*	(Optional) Session ID.
vpn *vpn-id*	(Optional) VPN ID.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.6.1	This command was introduced.

Example

Following is a sample output from the **show packet-capture** command using the keyword **details**.

```
Device# show packet-capture details
SESSION  PACKETS
VPN    INTERFACE       ID      CAPTURED   STATE
1  ipsec1 s123 59 Running
```

show packet-trace

To view detailed packet tracer statistics for the specified trace ID or summary statistics for all the filtered packets, up to 1024 records, use the **show packet-trace** command in privileged EXEC mode.

show packet-trace [**details** *trace-id*] [**statistics** [*trace-id* | **decision** *string* | **destination-ip** *ip-address* | **destination-interface** *interface* | **destination-port** *port* | **duration** *seconds* | **source-interface** *interface* | **source-ip** *ip-address* | **source-port** *port*]]

Syntax Description

details *trace-id*	(Optional) Displays packet trace details for the specified trace ID.
statistics	(Optional) Displays packet trace statistics for the parameter specified.
trace-id	(Optional) Displays packet statistics for the specified trace-id. Range: 0 to 1023.
decision *string*	(Optional) Displays packet drop/forward information.
destination-ip *ip-address*	(Optional) Displays packet trace statistics for the specified destination IPv4 address.
destination-interface *interface*	(Optional) Displays statistics for the specified destination-interface.
destination-port *port*	(Optional) Displays packet trace statistics for the specified destination port. Range: 0 to 65535.
duration *seconds*	(Optional) Displays packet trace statistics for the specified duration in µsecs.
source-interface *interface*	(Optional) Displays packet trace statistics for the specified source interface.
source-ip *ip-address*	(Optional) Displays packet trace statistics for the specified source IPv4 address.
source-port *port*	(Optional) Displays packet trace statistics for the specified source port. Range: 0 to 65535.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.5.1	This command was introduced.

Example

This is the sample output for the show packet-trace details command, which is displayed for the specified trace ID 10.

```
Device# show packet-trace details 10
=========================================================================================================
Pkt-id     src_ip(ingress_if)     dest_ip(egress_if)     Duration     Decision
=========================================================================================================
10         10.1.15.15:0 (ge0_0)   192.168.255.5:0 (ge0_0)     15 us          PUNT
INGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f 0f
e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00 00
00 00 00 00 00
EGRESS_PKT:
01 00 5e 00 00 05 52 54 00 6b 4b fa 08 00 45 c0 00 44 f8 60 00 00 01 59 c7 2b 0a 01 0f 0f
e0
00 00 05 02 01 00 30 ac 10 ff 0f 00 00 00 33 8d 1b 00 00 00 00 00 00 00 00 00 ff ff ff
00 00 0a 02 00 00 00 00 28 0a 01 0f 0d 00 00 00 00 ac 10 ff 0d 00 00 00 00 00 00 00 00 00
00 00 00 00 00
Feature Data
-------------------------------------
TOUCH : fp_proc_packet
-------------------------------------
TOUCH : fp_proc_packet2
-------------------------------------
TOUCH : fp_send_to_host
-------------------------------------
FP_TRACE_FEAT_PUNT_INFO:
icmp_type : 0
icmp_code : 0
qos : 7
-------------------------------------
TOUCH : fp_hw_x86_pkt_free
```

This is the sample output for the packet trace statistics command, which is displayed for the specified interface, in this case, for the loopback 0 interface.

```
Device# show packet-trace statistics source-interface loop0.0
packet-trace statistics 0
source-ip 10.1.15.13
source-port 0
destination-ip 192.168.255.5
destination-port 0
source-interface ge0_0
destination-interface ge0_0
decision PUNT
duration 40
```

This is the sample output for the packet tracer statistics command, which is displayed for the 10 records.

```
Device# show packet-trace statistics
TRACE            SOURCE  DESTINATION  DESTINATION  SOURCE    DESTINATION
 ID   SOURCE IP    PORT       IP         PORT      INTERFACE  INTERFACE  DECISION DURATION
-------------------------------------------------------------------------------------------
```

```
0     10.1.15.13   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       40
1     10.1.15.15   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       12
2     10.20.24.15  0    192.168.255.5    0        ge0_1       ge0_1       PUNT       66
3     10.1.15.13   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       14
4     10.1.15.15   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       11
5     10.20.24.15  0    192.168.255.5    0        ge0_1       ge0_1       PUNT       64
6     10.1.15.13   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       14
7     10.1.15.15   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       27
8     10.20.24.15  0    192.168.255.5    0        ge0_1       ge0_1       PUNT       97
9     10.1.15.13   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       12
10    10.1.15.15   0    192.168.255.5    0        ge0_0       ge0_0       PUNT       15
```



Note Packet tracer displays statistics for up to 1024 records.

show parser dump

Display all CLI operational commands and their syntax.

show parser dump [*command-name*]

Syntax Description

None	Display all CLI operational commands and their syntax.
Command	*command-name* Display the specific CLI operational command or command hierarchy and the syntax of those commands.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show parser dump

```
vEdge# show parser dump
autowizard [true/false]
clear arp
clear arp WORD
clear arp WORD interface WORD
clear arp WORD interface WORD vpn WORD
clear arp WORD vpn WORD
clear arp WORD vpn WORD interface WORD
clear arp interface WORD
clear arp interface WORD WORD
clear arp interface WORD WORD vpn WORD
clear arp interface WORD vpn WORD
clear arp interface WORD vpn WORD WORD
```

```
clear arp vpn WORD
...
```

Related Topics

help, on page 638
show parser dump, on page 1093

show pim interface

List interfaces that are running PIM (on vEdge routers only).

show pim interface [**vpn** *vpn- id*]

Syntax Description

None	List standard information about interfaces that are running PIM.

VPN-Specific Interfaces	**vpn** *vpn-id* List only the PIM interfaces in the specified VPN.

Command History

Release	Modification
14.2.	Command introduced.

Examples

Show pim interface

```
vEdge# show pim interface

                                                                          JOIN
     IF                    NEIGHBOR  HELLO                              PRUNE
VPN  NAME   IF ADDR        COUNT     INTERVAL  PRIORITY  DR ADDRESS      INTERVAL
-------------------------------------------------------------------------------
1    ge0/0  10.2.2.11/24   1         30        1         10.2.2.12       60
1    ge0/5  10.0.9.11/24   1         30        1         10.0.9.14       60
1    ge0/6  10.0.10.11/24  1         30        1         10.0.10.14      60
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900

show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim neighbor, on page 957
show pim rp-mapping, on page 958
show pim statistics, on page 959

show pim neighbor

List PIM neighbors (on vEdge routers only).

show pim neighbor [**vpn** *vpn-id*]

Syntax Description

None	List standard information about PIM neighbors.

VPN-Specific Neighbors	**vpn** *vpn-id* List only the PIM neighbors in the specified VPN.

Command History

Release	Modification
14.2.	Command introduced.

Examples

Show pim neighbor

```
vEdge# show pim neighbor

                                                                    HOLD
VPN  IF NAME  NBR ADDR    UP TIME     EXPIRES     PRIORITY  TIME  DR ADDRESS
-------------------------------------------------------------------------------
1    ge0/0.1  10.0.9.11   0:08:19:01  0:00:01:44  1         105   10.0.9.14
1    ge0/1.1  10.0.10.11  0:08:19:01  0:00:01:44  1         105   10.0.10.14
2    ge0/0.2  20.0.9.11   0:08:19:01  0:00:01:44  1         105   20.0.9.14
2    ge0/1.2  20.0.10.11  0:08:19:01  0:00:01:44  1         105   20.0.10.14
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901

show omp multicast-routes, on page 909
show pim interface, on page 956
clear pim protocol, on page 609
show pim rp-mapping, on page 958
show pim statistics, on page 959

show pim rp-mapping

Display the mappings of multicast groups to RPs (on vEdge routers only).

show pim rp-mapping [**vpn** *vpn-id*]

Syntax Description

None	Display all group-to-RP mappings.
VPN	**vpn** *vpn-id* Display the group-to-RP mappings for a specific VPN.

Command History

Release	Modification
14.3.	Command introduced.

Examples

Show pim rp-mapping

```
vEdge# show pim rp-mapping

VPN  TYPE     GROUP         RP ADDRESS
---------------------------------------
1    Auto-RP  225.0.0.0/24  60.0.1.100
1    Auto-RP  226.0.0.0/24  59.0.1.100
2    Auto-RP  227.0.0.0/24  58.0.2.100
2    Auto-RP  228.0.0.0/24  57.0.2.100
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897
show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909

show pim interface, on page 956
show pim neighbor, on page 957
show pim statistics, on page 959

show pim statistics

Display all PIM-related statistics on the router (on vEdge routers only).

show pim statistics [**vpn** *vpn-id*]**show pim statistics** *parameter*

Syntax Description

None	Display all PIM statistics.
Specific Statistic	*parameter* Display the counters for a single PIM counter. *parameter* can be **assert-rx**, **assert-tx**, **auto-rp-announce-rx**, **auto-rp-mapping-rx**, **bad-rx**, **hello-rx**, **hello-tx**, **join-prune-rx**, **join-prune-tx**, **unknown-rx**, and **unsupported-rx**.

VPN	**vpn** *vpn-id*Display the PIM statistics in the specified VPN.

Command History

Release	Modification
14.2.	Command introduced.

Examples

Show pim statistics

```
vEdge# show pim statistics
VPN 1 STATISTICS
------------------------------------------
MESSAGE TYPE         RECEIVED          SENT
------------------------------------------
Hello                    2455          2528
Join-Prune                115            82
AutoRP Announce             0             -
AutoRP Mapping              0             -
Unsupported                 0             -
Unknown                     0             -
Bad                      1440             -
```

Related Topics

clear pim interface, on page 607
clear pim neighbor, on page 608
clear pim protocol, on page 609
clear pim rp-mapping, on page 610
clear pim statistics, on page 611
show multicast replicator, on page 897

show multicast rpf, on page 899
show multicast topology, on page 900
show multicast tunnel, on page 901
show omp multicast-routes, on page 909
show pim interface, on page 956
show pim neighbor, on page 957
show pim rp-mapping, on page 958

show platform resources

Table 23: Feature History

Feature Name	Release Information	Description
Crypto Utilization in Show Platform Resources Command	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This feature adds information about crypto utilization to the **show platform resources** command on the supported routers.

To monitor system resources, including crypto utilization, use the **show platform resources** command in privileged EXEC mode.

show platform resources

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	The command is modified. The command output is enhanced to include crypto-utilization information on the supported routers.

Usage Guidelines

Crypto utilization is displayed only for the following supported routers:

- Cisco ASR 1000-ESP100 - CN6870 (15-13063-01)
- Cisco ASR 1000-ESP200 - 2x CN6880 (15-13062-01)
- Cisco ASR 1001-X - CN6645 (15-14203-01)
- Cisco ASR 1002-X - CN6335 (15-13267-01)
- Cisco ASR 1001-HX - CN6870-800 (15-13063-01)
- Cisco ASR 1002-HX - CN6880-1200 (15-13062-01)
- Cisco ASR1000-ESP100-X
- Cisco ASR 1000-ESP200-X

- Cisco Catalyst 8500-12X
- Cisco Catalyst 8500-12X4QC

Note Some of the supported routers above have a "- CN6XXX" designation trailing the Cisco product name, indicating the part number of the particular Cavium/Marvell network processor used.

The following is a sample output from the **show platform resources** command that is run on a Cisco ASR 1000 Series router:

```
# show platform resources
**State Acronym: H - Healthy, W - Warning, C - Critical
Resource                Usage                Max             Warning         Critical        State
-------------------------------------------------------------------------------------------------
RP0 (ok, active)                                                                             H
 Control Processor      1.45%                100%            80%             90%             H
  DRAM                  2979MB(18%)          15912MB         88%             93%             H
  bootflash             968MB(52%)           1858MB          88%             93%             H
  harddisk              6453MB(8%)           75058MB         88%             93%             H
ESP0(ok, active)                                                                             H
 Control Processor      3.05%                100%            80%             90%             H
  DRAM                  1037MB(13%)          7861MB          88%             93%             H
 QFP                                                                                         H
  TCAM                  14cells(0%)          524288cells     65%             85%             H
  DRAM                  108655KB(10%)        1048576KB       85%             95%             H
  IRAM                  13013KB(9%)          131072KB        85%             95%             H
  CPU Utilization       0.00%                100%            90%             95%             H
  Crypto Utilization    0.00%                100%            90%             95%             H
  Pkt Buf Mem           2003KB(0%)           262144KB        85%             95%             H
SIP0                                                                                         H
 Control Processor      1.50%                100%            80%             90%             H
  DRAM                  518MB(55%)           941MB           88%             93%             H
```

show platform software trace level

To view the binary trace levels for the modules of a Cisco SD-WAN process executing on a specific hardware slot, issue the command **show platform software trace level** in the Privileged EXEC mode.

show platform software trace level *process* *slot*

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'.
slot	Hardware slot from which process messages must be logged.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Support introduced for select Cisco SD-WAN processes. See the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.

Usage Guidelines

Table 24: 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

```
Device# show platform software trace level fpmd r0
Module Name                      Trace Level
-------------------------------------------------
binos                            Notice
bipc                             Notice
btrace                           Notice
btrace_ra                        Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
chmgr_api                        Notice
config                           Notice
cyan                             Notice
dassist                          Notice
dbal                             Notice
dpi                              Notice
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
flash                            Notice
fpmd                             Notice
green-be                         Notice
ios-avl                          Notice
mqipc                            Notice
policy                           Notice
prelib                           Notice
procstlib                        Notice
service-dir                      Notice
services                         Notice
syshw                            Notice
tdl_cdlcore                      Notice
tdl_dbal_root                    Notice
tdl_mem_stats_ui                 Notice
tdl_og_config                    Notice
tdl_plat_main                    Notice
tdl_plat_trail                   Notice
tdl_sdwan_policy                 Notice
```

```
tdl_service_directory           Notice
tdl_tdl_toc                     Notice
tdl_ui                          Notice
tdl_uipeer_comm_ui              Notice
tdlgc                           Notice
tdllib                          Notice
trans_avl                       Notice
trans_gbt                       Notice
ttm                             Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
vconfd                          Notice
vipcommon                       Notice
vista                           Notice
vs_flock                        Notice
```

show policer

Display information about the policers that are in effect (on vEdge routers only).

show policer [**burst** *bytes*] [**oos-action** *action*] [**oos-pkts** *number*] [**rate** *bps*]

Syntax Description

None	Display information about all policers.
Specific Burst Size	**burst** *bytes* Display information about policers that match the specified burst size.*Range:* 0 through 2^{64} – 1 bytes
Specific Out-of-Specification Action	**oos-action** *action* Display information about policers that match the specified OOS action. A policed packet is out of specification when the policer does not allow it to pass. Depending on the policer configuration, these packets are either dropped or they are remarked, which sets the packet loss priority (PLP) value on the egress interface to high.*Action:* **drop**, **remark**
Specific Out-of-Specification Packet Count	**oos-pkts** *number* Display information about policers that match the specified OOS packet count.*Range:* 0 through 2^{64} – 1
Specific Bandwidth	**rate** *bps* Display information about policers that match the specified bandwidth.*Range:* 0 through 2^{64} – 1 bps

Command History

Release	Modification
14.1.	Command introduced.
16.3	Added **burst**, **oos-action**, **oos-pkts**, and **rate** options.

Examples

Display the policers that are in effect on the router:

Show policer

```
vEdge# show policer
                                                          OOS      OOS
NAME       INDEX  DIRECTION  RATE          BURST  ACTION   PKTS
-----------------------------------------------------------------
ge0_0_llq  10     out        200000000000  15000  drop     0
ge0_3_llq  11     out        200000000000  15000  drop     0
```

Related Topics

clear policer statistics, on page 612
show policy data-policy-filter, on page 968
show policy from-vsmart, on page 971

show policy access-list-associations

Display the IPv4 access lists that are operating on each interface (on vEdge routers only).

show policy access-list-associations [*access-list-name*]

Syntax Description

None	Display all access lists operating on the vEdge router's interfaces.
Specific Access List	*access-list-name* Display the interfaces on which the specific access list is operating.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show policy access-list-associations

```
vEdge# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!
```

```
vEdge# show policy access-list-associations

                    INTERFACE  INTERFACE
NAME                NAME       DIRECTION
-----------------------------------------
ALLOW_OSPF_PACKETS  ge0/0      in
```

Related Topics

access-list, on page 30
show ipv6 policy access-list-associations, on page 882
show policy access-list-counters, on page 965
show policy access-list-names, on page 966
show policy access-list-policers, on page 967
show policy data-policy-filter, on page 968

show policy access-list-counters

Display the number of packets counted by IPv4 access lists configured on the vEdge router (on vEdge routers only).

show policy access-list-counters [*access-list-name*]

Syntax Description

None	Display the count of packets that have been collected by all data policies on the local vEdge router.
Specific Access List	*access-list-name* Display the count of packets that have been collected by the specified data policy on the local vEdge router.

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show policy access-list-counters

```
vEdge# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
```

```
 !
!
vEdge# show policy access-list-counters

NAME                 COUNTER NAME         PACKETS  BYTES
------------------------------------------------------------
ALLOW_OSPF_PACKETS   count_OSPF_PACKETS   1634     135940
```

Related Topics

access-list, on page 30
show ipv6 policy access-list-counters, on page 883
show policy access-list-associations, on page 964
show policy access-list-names, on page 966
show policy access-list-policers, on page 967
show policy data-policy-filter, on page 968

show policy access-list-names

Display the names of the IPv4 access lists configured on the vEdge router (on vEdge routers only).

show policy access-list-names

Syntax Description

Syntax Description

None

Command History

Release	Modification
14.1.	Command introduced.

Examples

Show policy access-list-names

```
vEdge# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!
vEdge# show policy access-list-names

NAME
```

```
--------------------
ALLOW_OSPF_PACKETS
```

Related Topics

access-list, on page 30
show ipv6 policy access-list-names, on page 884
show policy access-list-associations, on page 964
show policy access-list-counters, on page 965
show policy access-list-policers, on page 967
show policy data-policy-filter, on page 968

show policy access-list-policers

Display information about the policers configured in IPv4 access lists (on vEdge routers only).

show policy access-list-policers

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
16.2.5	Add the policy sequence number to the policer name.

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.

```
vEdge# show 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
```

Related Topics

clear policer statistics, on page 612
show ipv6 policy access-list-policers, on page 885
show policer, on page 963

show policy data-policy-filter

Display information about data policy filters for configured counters and policers, and for out-of-sequence packets (on vEdge routers only).

show policy data-policy-filter

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
16.2.5	Add the policy sequence number to the policer name
17.1	Add out-of-specification bytes (OOS Btytes) column to command output.

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 2

Display packet information for policers. This output shows that the policer named "police" was applied in sequences 10, 20, and 30 in the data policy "dp1" and in sequence 10 in the "dp2" data policy.

```
vEdge# show 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
dp2         vpn_1_list                                   10.police    0
```

Example 3

For a data policy that includes a policer, display the policers:

```
vEdge# 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

vEdge# show 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
```

Related Topics

clear policer statistics, on page 612
show ipv6 policy access-list-policers, on page 885
show policer, on page 963
show policy from-vsmart, on page 971

show policy ef-stats

To display elephant-flow statistics, use the **show policy ef-stats** command in privileged exec mode.

show policy ef-stats

Syntax Description

ef-stats	Displays elephant-flow statistics.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco SD-WAN Release 20.9.1	This command was introduced.

Examples

The following is a sample output from the **show policy ef-stats** command:

```
vEdge2k# show policy ef-stats
-------------------------------------------------------------------------------------------------

                                ADD
      ADD    DEL    CUR    SUPER                                                          CUR
CORE  SUPER  SUPER  SUPER  BLOCK   ADD   DEL   CUR   SCAN     EF   CUSTOM  HASH       CPU
NUM   BLOCK  BLOCK  BLOCK  FAILED  FLOW  FLOW  FLOW  COUNTER  NUM  MATCH   COLLISION  USAGE
-------------------------------------------------------------------------------------------------
2     1      0      1      0       0     0     0     20523    0    0       0          00.04
3     1      0      1      0       1     0     1     20523    0    0       0          00.01
4     1      0      1      0       0     0     0     20523    0    0       0          00.00
5     1      0      1      0       0     0     0     20523    0    0       0          00.01
6     1      0      1      0       0     0     0     20523    0    0       0          00.01
7     1      0      1      0       0     0     0     20523    0    0       0          00.01
```

```
8     1     0     1     0     0     0     0     20523     0     0     0          00.02
9     1     0     1     0     1     0     1     20523     0     0     0          00.02
10    1     0     1     0     0     0     0     20523     0     0     0          00.01
11    1     0     1     0     0     0     0     20523     0     0     0          00.01
12    1     0     1     0     0     0     0     20523     0     0     0          00.00
13    1     0     1     0     1     0     1     20523     0     0     0          00.01
14    1     0     1     0     0     0     0     20523     0     0     0          00.01
15    1     0     1     0     0     0     0     20523     0     0     0          00.01
16    1     0     1     0     0     0     0     20523     0     0     0          00.02
17    1     0     1     0     0     0     0     20523     0     0     0          00.00
18    1     0     1     0     0     0     0     20523     0     0     0          00.01
19    1     0     1     0     0     0     0     20523     0     0     0          00.01
20    1     0     1     0     0     0     0     20523     0     0     0          00.01
```

Table 25: show policy ef-stats Field Descriptions

Field	Description
CORE NUM	Core Number
EF NUM	Number of elephant flows identified at present.
CUSTOM MATCH	Number of elephant flows identified at present because of a matched sequence.
CUR CPU USAGE	Current CPU usage.

show policy from-vsmart

Display a centralized data policy, an application-aware policy, or a cflowd policy that a vSmart controller has pushed to the vEdge router (on vEdge routers only). The vSmart controller pushes the policy via OMP after it has been configured and activated on the controller.

show policy from-vsmart

show policy from-vsmart [**app-route-policy**] [**cflowd-template** [*template-option*]] [**data-policy**] [**lists** (**data-prefix-list** | **vpn-list**)] [**policer**] [**sla-class**]

Syntax Description

None	None: Display all the data policies that the vSmart controller has pushed to the vEdge router.
app-route-policy	Application Route Policies: Display only the application-aware routing policies that the vSmart controller has pushed to the vEdge router.
cflowd-template [*template-option*]	cflowd Templates: Display only the cflowd template information that that vSmart controller has pushed to the vEdge router. *template-option* can be one of **collector**, **flow-active-timeout**, **flow-inactive-timeout**, and **template-refresh**.
data-policy	Data Policies: Display only the data policies that the vSmart controller has pushed to the vEdge router.

lists (**data-prefix-list** | **vpn-list**)	Lists: Display only the policy-related lists that the vSmart controller has pushed to the vEdge router.
policer	Policers: Display only the policers that the vSmart controller has pushed to the vEdge router.
sla-class	SLA Classes: Display only the SLA classes for application-aware routing that the vSmart controller has pushed to the vEdge router.

Command History

Release	Modification
14.1	Command introduced.
14.2	Command renamed from **show omp data-policy** to **show policy from-vsmart**.
14.3	**cflowd-template** option added.

Examples

Example 1

```
vEdge# show 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
  sequence 4
   match
    source-port 8000
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 5
   match
    dscp 10
   action
    count app-route-dscp
```

```
    sla-class test_sla_class
    no sla-class strict
  sequence 7
   match
    protocol 6
   action
    sla-class test_sla_class
    sla-class strict
  sequence 8
   match
    protocol 17
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 9
   match
    protocol 1
   action
    count app-route-icmp
    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
```

Example 2

```
vEdge# show 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
vm5# show policy from-vsmart cflowd-template collector
from-vsmart cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.15 port 13322
```

Related Topics

cflowd-template, on page 121
policy, on page 382
show app cflowd template, on page 727
show policy data-policy-filter, on page 968

show policy service-path

Determine the next-hop information for an IP packet that a vEdge router sends out a service-side interface (on vEdge routers only). You identify the IP packet by specifying fields in the IP header. You can use this command when using application-aware routing, to determine that path taken by the packets associated with a DPI application.

show policy service-path vpn-id *vpn-id* **interface** *interface-name* **source-ip** *ip-address* **dest-ip** *ip-address* **protocol** *number* **source-port** *port-number* **dest-port** *port-number* [**all** | **app** *application-name* | **dscp** *value*]

Syntax Description

all	All Possible Paths: Display all possible paths for a packet.
dest-ip *ip-address* **dest-port** *port-number*	Destination IP Address and Port Number: IP address and port number of the remote end of the IPsec tunnel.
app *application-name*	DPI Application: Display the packets associated with the specified DPI application.
dscp *value*	DSCP Value: DSCP value being used on the IPsec tunnel.*Range:* 0 through 63
interface *interface-name*	Interface: Name of the local interface being used for the IPsec tunnel.
protocol *number*	Protocol: Number of the protocol being used on the IPsec tunnel.
source-ip *ip-address* **source-port** *port-number*	Source IP Address and Port Number: IP address and port number of the local end of the IPsec tunnel.
vpn-id *vpn-id*	VPN: Identifier of the service VPN.

Command History

Release	Modification
15.1	Command introduced.
15.3	**all** and **app** options added.

Example

```
vEdge# show policy service-path vpn 0 interface ge0/0 source-ip 172.0.101.15
dest-ip 172.0.101.16 protocol 1 source-port 1 dest-port 1 all
Number of possible next hops: 1
Next Hop: Svc_GRE
Source: 10.1.15.15 Destination: 10.1.16.16
```

Related Topics

show app-route sla-class, on page 742
show app-route stats, on page 744
show ip fib, on page 854
show ip routes, on page 865
show policy tunnel-path, on page 974

show policy tunnel-path

Determine the next-hop information for an IP packet that a vEdge router sends out a WAN transport tunnel interface (on vEdge routers only). You identify the IP packet by specifying fields in the IP header. You can use this command when using application-aware routing, to determine that path taken by the packets associated with a DPI application.

show policy service-path vpn-id *vpn-id* **interface** *interface-name* **source-ip** *ip-address* **dest-ip** *ip-address* **protocol** *number* **source-port** *port-number* **dest-port** *port-number* [**all** | **app** *application-name* | **dscp** *value*]

Syntax Description

all	All Possible Paths: Display all possible paths for a packet.
dest-ip *ip-address* **dest-port** *port-number*	Destination IP Address and Port Number: IP address and port number of the remote end of the IPsec tunnel.
app *application-name*	DPI Application: Display the packets associated with the specified DPI application.
dscp *value*	DSCP Value: DSCP value being used on the IPsec tunnel.
interface *interface-name*	Interface: Name of the local interface being used for the IPsec tunnel.
protocol *number*	Protocol: Number of the protocol being used on the IPsec tunnel.
source-ip *ip-address* **source-port** *port-number*	Source IP Address and Port Number: IP address and port number of the local end of the IPsec tunnel.
vpn-id *vpn-id*	VPN: Identifier of the transport VPN.

Command History

Release	Modification
15.2	Command renamed from **show app-route path** and introduced.
15.3	**all** and **app** options added.

Example

```
vEdge# show policy tunnel-path vpn 0 interface ge0/2 source-ip 10.0.5.11 dest-ip 10.0.5.21
 protocol 6
source-port 12346 dest-port 12346
Nexthop: Direct
Interface ge0/2 index: 3
```

Related Topics

show app-route stats, on page 744
show app-route sla-class, on page 742
show policy service-path, on page 973

show policy zbfw filter-statistics

Display a count of the packets that match a zone-based firewall's match criteria and the number of bytes that match the criteria (on vEdge routers only).

show policy zbfw filter-statistics

Syntax Description

None

Command History

Release	Modification
18.2	Command introduced.

Example

For the configured zone-based firewalls, display the number of packets and the number of bytes that match the match criteria in the firewalls:

```
vEdge# show policy zbfw filter-statistics

NAME           COUNTER NAME   PACKETS  BYTES
-----------------------------------------------
ZONE-POLICY-1  counter_seq_1  2        196
```

Related Topics

clear policy zbfw filter-statistics, on page 613
clear policy zbfw global-statistics, on page 614

show policy zbfw global-statistics

Display statistics about the packets processed by zone-based firewalls (on vEdge routers only).

show policy zbfw global-statistics

Syntax Description

None

Command History

Release	Modification
18.2	Command introduced.

Example

Display statistics about packets that the router has processed with zone-based firewalls:

```
vEdge# show policy zbfw global-statistics
         Total zone-based firewall packets   : 0
        Fragments                           : 0
        Fragment failures                   : 0
        State check failures                : 0
        Flow addition failures              : 0
        Unsupported protocol                : 0
        Number of flow entries              : 0
        Exceeded maximum TCP half-open      : 0
```

```
Mailbox message full               : 0

Packets Implicitly Allowed         :
  No pair in same zone             : 0
  No-zone-to-no-zone packets       : 0
  Zone-to-no-zone internet         : 0

  TCP Stats                        :
    TCP retransmitted segments     : 0
    TCP out-of-order segments      : 0

Packets Implicitly Dropped         :
  During policy change             : 0
  Invalid filter                   : 0
  No pair for different zone       : 0
  Zone-to-no-zone packets          : 0
  Zone-to-no-zone internet         : 0

  TCP Drops                        :
    Internal invalid tcp state     : 0
    Stray seg                      : 0
    Invalid flags                  : 0
    Syn with data                  : 0
    Invalid win scale option       : 0
    Invalid seg synsent state      : 0
    Invalid ack num                : 0
    Invalid ack flag               : 0
    Reset to Responder             : 0
    Retrans invalid flags          : 0
    Reset in window                : 0
    Invalid sequence number        : 0
    Invalid seg synrcvd state      : 0
    Syn in window                  : 0
    Unexpected TCP payload         : 0
    Invalid seg pkt too old        : 0
    Invalid seg pkt win overflow   : 0
    Invalid seg pyld after fin send : 0
    No syn in listen state         : 0
    Internal TCP invalid direction  : 0
```

Table 26: Statistics Information

Statistics	Description
Total zone-based firewall packets	The total number of packets passing through firewall.
Self zone packets	Packets that are directed to/going out from the router (not pass through traffic).
Fragments	Packet Fragments counter.
Fragment failures	Failure to reassemble fragments.
State check failures	Any TCP state check failures found during flow add or flow inspect process, will be counted towards this counter.
Fragment state check failures	For fragmented packets, if the first packet has failed state check and dropped, drop other fragments and increment the counter.
Flow addition failures	Failed to add a flow record for a given traffic flow.

Statistics	Description
Unsupported protocol	Packets where the protocol number not supported by firewall.
Number of flow entries	Points to the number of sessions created.
Exceeded maximum TCP half-open	After the max half open TCP connections have reached (which is set by tcp-syn-flood-limit), this counter gets incremented.
Mailbox message full	SMTP 554, mailbox full.
No pair in same zone	Packets belonging to same zones and no zone pair. Basically packets across interfaces belonging to same zone.
No-zone-to-no-zone packets	None of the VPN's (source/destination) are part of any zones, then allow the packets to go through.
Zone-to-no-zone internet	When one VPN is part of a zone, and other VPN is a Internet VPN0 AND its not part of the zone, then if "zone-to-nozone-internet" is **allow**, this counter will be incremented.
Umbrella registration packets	Initial Umbrella registration packets.
No pair Self zone packets	If no zone pair found and if its a self-zone packet allow the packet.
TCP retransmitted segments	TCP retransmitted segments.
TCP out-of-order segments	Out of order segments that arrive during ESTAB, CLOSEWAIT OR LASTACK, are allowed implicitly.
During policy change	Packets dropped during policy change due to reconfig.
Invalid filter	No longer a valid policy filter, then increment this counter.
No pair for different zone	No zone pair between different zones, then drop the packet and increment the counter.
Zone-to-no-zone packets	All traffic from Zone to a No-Zone will be dropped.
Zone-to-no-zone internet	When one VPN is part of a zone, and other VPN is a Internet VPN0 AND its not part of the zone, then if "zone-to-nozone-internet" is **deny**, this counter will be incremented.
Internal invalid tcp state	If the TCP state check for the flow, does not match any of the valid states such as LISTEN, SYNSENT, SYNRCVD, ESTABLISHED, CLOSEWAIT, LASTACK OR TIMEWAIT.
Stray seg	A TCP segment is received that should not have been received through the TCP state machine such as a TCP SYN packet being received in the listen state from the responder.

Statistics	Description
Invalid flags	This can be caused by: **1.** During LISTEN state, a TCP peer receives a RST or an ACK **2.** Expected SYN/ACK is not received from the responder. **3.** TCP initial SYN packet has flags other than SYN.
Syn with data	If the SYN packet contains payload for some reason, then drop the packet.
Invalid win scale option	Caused by incorrect window scale option byte length.
Invalid seg synsent state	An invalid TCP segment in SYNSENT state is caused by: **1.** SYN/ACK has payload. **2.** SYN/ACK has other flags (PSH, URG, FIN) set. **3.** Receive a non-SYN packet from initiator.
Invalid ack numif	This drop could be caused by one of these reasons: **1.** ACK not equals to the next_seq# of the TCP peer. **2.** ACK is greater than the most recent SEQ# sent by the TCP peer.
Invalid ack flag	Drop the packet if **1.** Expecting ACK flag , but not set during different TCP states. **2.** ACK flag is set and other flags (such as RST) is set.
Reset to Responder	Send RST to responder in SYNSENT state when ACK# is not equal to ISN+1.
Retrans invalid flags	If this is retransmitted packet and already ACKed drop the packet.
Reset in window	A RST packet is observed within the window of an already established TCP connection.
Invalid sequence number	In SYNRCVD state, drop the packet if, • If Seq number is less than ISN • If receiver window is zero, then drop any segment with Data and drop any out-of-order segments. • If receiver window is non-zero, then drop any segment whose SEQ falls beyond the window.
Invalid seg synrcvd state	In SYNRCVD state, drop the packet if, receive a retransit SYN with payload from initiator.
Syn in window	If a SYN is received in an already established connection, then drop the packet.

Statistics	Description
Unexpected TCP payload	In SYNRCVD state, if a packet with payload from responder to initiator direction is received, drop the packet.
Invalid seg pkt too old	Packet is too old - one window behind the other side's ACK. This could happen in ESTABLISHED, CLOSEWAIT and LASTACK state.
Invalid seg pkt win overflow	This occurs when incoming segment size overflows receiver's window. This check is done during TCP ESTAB, CLOSEWAIT and LASTACK state processing.
Invalid seg pyld after fin send	Payload received after FIN sent. This could happen in CLOSEWAIT state.
No syn in listen state	During TCP LISTEN state processing, if the packet received is not SYN packet, then drop the packet.
Internal TCP invalid direction	Packet direction undefined.

Related Topics

clear policy zbfw global-statistics, on page 614

show policy zbfw sessions

Display the session flow information for all zone pairs configured with a zone-based firewall policy (on vEdge routers only).

show policy zbfw sessions

Syntax Description

None

Command History

Release	Modification
18.2	Command introduced.

Example

For the configured zone-based firewalls, display the number of packets and the number of bytes that match the match criteria in the firewalls:

```
vEdge# show policy zbfw sessions

ZONE PAIR      SOURCE IP    DESTINATION  SOURCE  DESTINATION           SOURCE  DESTINATION  IDLE        OUTBOUND  OUTBOUND  INBOUND  INBOUND  FILTER
NAME      VPN  ADDRESS      IP ADDRESS   PORT    PORT         PROTOCOL VPN     VPN          TIMEOUT     PACKETS   OCTETS    PACKETS  OCTETS   STATE
-------------------------------------------------------------------------------------------------------------------------------------------------
zp1       1    10.20.24.17  10.20.25.18  44061   5001         TCP      1       1            0:00:59:59  12552     17581337  6853     463590   established
zp1       1    10.20.24.17  10.20.25.18  44062   5001         TCP      1       1            0:01:00:00  10151     14217536  5561     375290   established
zp1       1    10.20.24.17  10.20.25.18  44063   5001         TCP      1       1            0:00:59:59  7996      11198381  4262     285596   established
zp1       1    10.20.24.17  10.20.25.18  44064   5001         TCP      1       1            0:00:59:59  7066      9895451   3826     257392   established
zp1       1    10.20.24.17  10.20.25.18  44065   5001         TCP      1       1            0:00:59:59  13471     18868856  7440     504408   established
zp1       1    10.20.24.17  10.20.25.18  44066   5001         TCP      1       1            0:00:59:59  8450      11834435  4435     295718   established
```

Related Topics

clear policy zbfw sessions, on page 614

show ppp interface

Display PPP interface information (on vEdge routers only).

show ppp interface

Syntax Description

None

Command History

Release	Modification
15.3.3	Command introduced.
17.1	Add Auth Type field to command output.

Example

```
vEdge# show ppp interface

              PPPOE       INTERFACE                PRIMARY   SECONDARY        AUTH
VPN   IFNAME  INTERFACE   IP          GATEWAY IP   DNS       DNS         MTU  TYPE
-------------------------------------------------------------------------------
0     ppp10   ge0/1       11.1.1.1    115.0.1.100  8.8.8.8   8.8.4.4     1150 pap
```

Related Topics

clear pppoe statistics, on page 615
show pppoe session, on page 981
show pppoe statistics, on page 982

show pppoe session

Display PPPoE session information (on vEdge routers only).

show pppoe session

Syntax Description

None

Command History

Release	Modification
15.3.3	Command introduced.

Example

```
vEdge# show pppoe session

             SESSION                                          PPP                    SERVICE
VPN  IFNAME  ID       SERVER MAC         LOCAL MAC          INTERFACE  AC NAME     NAME
-------------------------------------------------------------------------------------------
0    ge0/1   1        00:0c:29:2e:20:1a  00:0c:29:be:27:f5  ppp1       branch100  -

0    ge0/3   1        00:0c:29:2e:20:24  00:0c:29:be:27:13  ppp2       branch100  -
```

Related Topics

clear pppoe statistics, on page 615
show ppp interface, on page 981
show pppoe statistics, on page 982

show pppoe statistics

Display statistics for PPPoE sessions (on vEdge routers only).

show pppoe statistics

Syntax Description

None

Command History

Release	Modification
15.3.3	Command introduced.

Example

```
vEdge# show pppoe statistics
      pppoe_tx_pkts              :      73
      pppoe_rx_pkts              :      39
      pppoe_tx_session_drops     :      0
      pppoe_rx_session_drops     :      0
      pppoe_inv_discovery_pkts   :      0
      pppoe_ccp_pkts             :      12
      pppoe_ipcp_pkts            :      16
      pppoe_lcp_pkts             :      35
      pppoe_padi_pkts            :      4
      pppoe_pado_pkts            :      2
      pppoe_padr_pkts            :      2
      pppoe_pads_pkts            :      2
      pppoe_padt_pkts            :      2
```

Related Topics

clear pppoe statistics, on page 615
show pppoe session, on page 981
show ppp interface, on page 981

show 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 reboot history

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show 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
```

Related Topics

reboot, on page 652
show system status, on page 1019

show running-config

Display the active configuration that is running on the Cisco vEdge device. Use the **details** filter with this command to display the default values for configured components.

show running-config [*configuration-hierarchy*]

show running-config [*configuration-hierarchy*] | **details**

Syntax Description

None	Display the full active configuration.
| details	Default Values in Running Configuration: Display the default values for the components configured in the running configuration.
configuration-hierarchy	Specific Configuration Hierarchy: Display the active configuration for a specific hierarchy in the configuration.

Command History

Release	Modification
14.1	Command introduced.
Cisco SD-WAN Release 20.8.1	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.

Examples

Example 1

```
vEdge# show running-config system
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

```
vEdge# show 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
 !
!
vEdge# show running-config vpn 1 | details
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
 !
!
```

Example 3

```
vEdge(config-snmp)# show running-config snmp
snmp
 no shutdown
 view v3
  oid 1.3.6.1
!
 group groupAuthPriv auth-priv
  view v3
!
 user v3userAuthPriv-sha-aes
  auth sha-256
  auth-password 1234567890
  priv aes-256-cfb-128
  priv-password 1234567890
  group groupAuthPriv
 !
!
```

Related Topics

config, on page 623

show sdwan

Display SD-WAN related information about the IOS XE router.

show sdwan app-fwd

show sdwan app-route

show sdwan bfd

show sdwan certificate

show sdwan confd-logs

show sdwan control

show sdwan crash

show sdwan debugs

show sdwan ipsec

show sdwan nat-fwd

show sdwan notification

show sdwan omp

show sdwan policy

show sdwan running-config

show sdwan security-info

show sdwan software

show sdwan transport

show sdwan tunnel

show sdwan version

show sdwan zbfw

show sdwan zonebfwdp

Syntax Description

The options for the **show sdwan** commands are the same as for the equivalent vEdge router commands.

Command History

Release	Modification
16.9.1	Command introduced.

Example

The example output for the **show sdwan** commands is the same as for the equivalent vEdge router commands. Below is an example output for the **show sdwan app-route** command.

```
ISR4K# show sdwan app-route stats
app-route statistics 10.239.136.233 35.164.167.186 ipsec 12366 12366
 remote-system-ip 172.16.100.6
 local-color      custom2
 remote-color     3g
 mean-loss        0
 mean-latency     20
 mean-jitter      0
 sla-class-index  0
       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      662      0     21       0        0        0
1      663      0     21       0        0        0
2      663      1     20       0        0        0
3      663      0     20       0        0        0
4      662      0     20       0        0        0
5      664      1     20       0        0        0
app-route statistics 10.239.136.233 64.71.131.98 ipsec 12366 59448
 remote-system-ip 172.16.255.210
 local-color      custom2
 remote-color     default
 mean-loss        100
 mean-latency     0
 mean-jitter      0
 sla-class-index  0
       TOTAL          AVERAGE  AVERAGE  TX DATA  RX DATA
INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS     PKTS
-----------------------------------------------------------
0      661      661   0        0        0        0
1      662      662   0        0        0        0
2      661      661   0        0        0        0
3      662      662   0        0        0        0
4      661      661   0        0        0        0
5      664      664   0        0        0        0
```

Related Topics

show sdwan policy, on page 1001

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 flow closed

To view the closed appqoe flows, use the **show sdwan appqoe flow closed** command in privileged EXEC mode.

show sdwan appqoe flow closed { **all** | **detail** | **flow-id** *flow-id* | **server-port** *port-number* | **server-ip** *server-ip* [**server-port** *port-number*] | **client-ip** *client-ip* [**server-port** *port-number*] | **server-port** *port-number* | **error** [**detail** | **flow-id**] }

Syntax Description

all	Displays all flows
detail	Displays flow details for all flows
flow-id *flow-id*	Filters flows by flow-id
server-ip *server-ip*	Filters flows by the server IP address
client-ip *client-ip*	Filters flows by the client IP address
server-port *port-number*	Filters flows by server port number. Range: 1 to 65535
error	Displays the latest flows with errors.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	A new keyword **error** was introduced.

The following is a sample out from the **show sdwan appqoe flow closed all** command:

```
Device# show sdwan appqoe flow closed all
Current Historical Optimized Flows: 6

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD
```

```
Flow ID           VPN    Source IP:Port        Destination IP:Port      Service

52590946740086387 101    192.0.2.254:52895     198.51.100.77:443        TSU
52592155669963238 101    192.0.2.254:53394     198.51.100.10:443        TSU
52592460109050976 101    192.0.2.254:53465     198.51.100.22:443        TSU
52592469869036268 101    192.0.2.254:53467     198.51.100.55:443        TSU
52592624888356116 101    192.0.2.254:56293     198.51.100.78:443        TSU
52592627585006471 101    192.0.2.254:56294     198.51.100.99:443        TSU
```

The following is sample out from the **show sdwan appqoe flow closed error** command:

```
Device# show sdwan appqoe flow closed error
Current Historical Optimized Flows: 1
Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, RR:DRE Reduction Ratio
Flow ID      VPN  Source IP:Port        Destination IP:Port    T:S:U:D   RR%      Error
2267354182    1   192.0.2.254:37492     198.51.100.77:6000     1:1:0:0             T:Closed
 by SSL-S:Unsupported cipher
```

show sdwan appqoe flow flow-id

To view the closed appqoe flows, use the **show sdwan appqoe flow flow-id** command in privileged EXEC mode.

show sdwan appqoe flow *flow-id* [**debug** { **all** | **SSL** | **TCP** | **UTD** }]

Syntax Description

all	Displays all debug statistics
SSL	Displays debug statistics for SSL
TCP	Displays debug statistics for TCP
UTD	Displays debug statistics for UTD
DRE	Displays debug statistics for DRE

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command introduced.

Usage Guidelines

Run this command in privileged EXEC mode.

```
Device# show sdwan appqoe flow flow-id 52590946740086387
Flow ID: 52590946740086387

VPN: 101  APP: 0 [Client 192.0.2.254:52895 - Server 198.51.100.77:443]

TCP stats
---------
Client Bytes Received   : 1702
```

```
Client Bytes Sent       : 2877
Server Bytes Received   : 4102
Server Bytes Sent       : 1511
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
TCP Flow Bytes Consumed : 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 FIN/RST Sent        : 0x0
Flow Cleanup State      : 0x0
TCP Flow Events
   1. time:4024.495732   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:4024.495748   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   3. time:4024.496141   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   4. time:4024.496246   ::   Event:TCPPROXY_EVT_CONNECT_START
   5. time:4024.746338   ::   Event:TCPPROXY_EVT_CONNECT_DONE
   6. time:4024.746351   ::   Event:TCPPROXY_EVT_FLOW_CREATE_UTD_SENT
   7. time:4024.746420   ::   Event:TCPPROXY_EVT_FLOW_CREATE_UTD_RSP_SUCCESS
   8. time:4024.746442   ::   Event:TCPPROXY_EVT_FLOW_CREATE_SSL_DONE
   9. time:4024.746466   ::   Event:TCPPROXY_EVT_FLOW_ENABLE_SSL
  10. time:4024.746491   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS

SSL stats
---------
S-to-C Encrypted Bytes Written  : 638
S-to-C Encrypted Bytes Read     : 638
S-to-C Decrypted Bytes Written  : 319
S-to-C Decrypted Bytes Read     : 319
S-to-C Clear Flow Bytes         : 0
C-to-S Encrypted Bytes Written  : 1059
C-to-S Encrypted Bytes Read     : 1059
C-to-S Decrypted Bytes Written  : 740
C-to-S Decrypted Bytes Read     : 740
C-to-S Clear Flow Bytes         : 0

Proxy Server State Trace
INITIALIZED PRE_SSL HANDSHAKE EXPORT APP_DATA
Event: LWSSL_EVT_PEER_INIT_DONE State: INITIALIZED
Event: LWSSL_EVT_PRE_SSL_DONE State: PRE_SSL
Event: LWSSL_EVT_CCS_FIN_RCV State: HANDSHAKE
Event: LWSSL_EVT_KEY_PACKET_INIT_DONE State: EXPORT

Proxy Client State Trace
INITIALIZED FORWARD FORWARD_HANDSHAKE IMPORT APP_DATA
Event: LWSSL_EVT_PEER_INIT_DONE State: INITIALIZED
Event: LWSSL_EVT_HANDSHAKE_BEGIN State: FORWARD
Event: LWSSL_EVT_CCS_FIN_RCV State: FORWARD_HANDSHAKE
Event: LWSSL_EVT_KEY_PACKET_INIT_DONE State: IMPORT
```

show sdwan appqoe flow vpn-id

To view the appqoe flows using vpn ids, use the **show sdwan appqoe flow vpn-id** command in privileged EXEC mode.

show sdwan appqoe flow vpn-id *vpn-id* { **client-ip** *client-ip* [**server-ip** *server-ip* [**server-port** *port-number*]] | **server-ip** *server-ip* **server-port** *port-number* | **server-port** *port-number* }

Syntax Description

vpn-id	VPN/VRF ID. Range: 1 to 64
client-ip *client-ip*	Filters flows by the client IP address
server-ip *server-ip*	Filters flows by the server IP address
server-port *port-number*	Filters flows by server port number. Range: 1 to 65535

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command introduced.

```
Device# show sdwan appqoe flow vpn-id 101 server-port 443
T:TCP, S:SSL, U:UTD

Flow ID      VPN  Source IP:Port              Destination IP:Port   Service
52590946740086387 101    192.0.2.254:52895     198.51.100.77:443        TSU
52592155669963238 101    192.0.2.254:53394     198.51.100.10:443        TSU
52592460109050976 101    192.0.2.254:53465     198.51.100.22:443        TSU
52592469869036268 101    192.0.2.254:53467     198.51.100.55:443        TSU
52592624888356116 101    192.0.2.254:56293     198.51.100.78:443        TSU
52592627585006471 101    192.0.2.254:56294     198.51.100.99:443        TSU
```

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

None.

Command Mode

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.

Examples

Example

```
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

To display the Quality of Experience (QoS) measurements received from gateway sites, for Cloud onRamp for SaaS, on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan cloudexpress gateway-exits** command in privileged EXEC mode. The output may include entries for branch sites, and for branch sites with direct internet access (DIA).

show sdwan cloudexpress gateway-exits

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.

Examples

Example

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 office365 10.0.0.1
latency      2
loss         50
local-color  lte
remote-color lte
cloudexpress gateway-exits vpn 1 amazon_aws 10.0.0.2
latency      1
loss         0
local-color  lte
remote-color lte
cloudexpress gateway-exits vpn 1 dropbox 10.0.0.2
latency      19
loss         0
local-color  lte
remote-color lte
```

show sdwan cloudexpress local-exits

To display the list of applications enabled for Cloud onRamp for SaaS probing, on Cisco IOS XE Catalyst SD-WAN devices, and the interfaces on which the probing occurs, use the **show sdwan cloudexpress local-exits** command in privileged EXEC mode. Each line of the output applies to a specific application and interface, and includes the average latency and loss for each application and interface. The interfaces may include branch site direct internet access (DIA) interfaces, and gateway site interfaces.

show sdwan cloudexpress local-exits

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.

Examples

Example

```
Device# show sdwan cloudexpress local-exits
VPN  APPLICATION             INTERFACE               LATENCY  LOSS
------------------------------------------------------------------------
```

```
1    office365               GigabitEthernet1         1        43
1    office365               GigabitEthernet5         1        42
```

show sdwan cloudexpress service-area-applications

To display the applications enabled for Cloud onRamp for SaaS and the best path that has been selected for each, use the **show sdwan cloudexpress service-area-applications** command in Privileged EXEC mode.

show sdwan cloudexpress service-area-applications

Command Default

Not applicable.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command is introduced.

Usage Guidelines

The output includes separate sections with the details for each unique combination of:

- Service area (Microsoft Exchange traffic is currently the only possible value)
- VPN
- Application

For each combination, the output includes:

- **exit-type**:
  - **Local**: The application traffic uses the local interface – for example a Direct Internet Access (DIA) interface at a branch site.
  - **Gateway**: The application traffic uses a remote gateway.
  - **None**: Cloud onRamp for SaaS has not determined a best path for the application traffic.
- **interface**: Interface for current best path.
- **latency**: Last measured latency.
- **loss**: Last measured packet loss.
- **override-status**: Score for the path:
  - **OK**: Acceptable for application traffic.
  - **NOT-OK**: Not acceptable for application traffic.
  - **INIT**: Insufficient data.

Example

In the following example, the output snippet shows the best-path information for the office365 application, for VPN 1 only. In the example, Office 365 traffic on VPN 1 is using a local interface (GigabitEthernet0/0/2).

```
Device#show sdwan cloudexpress service-area-applications
cloudexpress service-area-applications Exchange vpn 1 office365
exit-type local
interface GigabitEthernet0/0/2
latency 3
loss 0
override-status OK
```

show sdwan policy

Display information about policy configuration on the IOS XE router.

show sdwan policy app-route-policy filter

show sdwan policy access-list-associations

show sdwan policy access-list-counters

show sdwan policy access-list-names

show sdwan policy data policy filter

show sdwan policy from-vsmart

show sdwan policy from-vsmart lists

Syntax Description

The options for the **show sdwan policy** commands are the same as for the equivalent vEdge router commands.

Command History

Release	Modification
16.9.1	Command introduced.

Note The **show sdwan policy data-policy-filter** commands display in different formats depending on if the counter has a value or not. If the counter has a value, the output for the show sdwan policy data-policy-filter displays in a linear format. If the counter does not have a value, the output displays in a tabular format.

Example

The example output for the **show sdwan policy** commands is the same as for the equivalent vEdge router commands. Below is an example output for the **show sdwan policy app-route-policy-filter** command.

```
ISR4K# show sdwan policy app-route-policy-filter
app-route-policy-filter app_route_policy_pm9008
 app-route-policy-vpnlist all_vpns
  app-route-policy-counter count_appr_pm9008_1001
   packets 15126027
   bytes   15305251759
  app-route-policy-counter count_appr_pm9008_1002
   packets 10364400
   bytes   11151607158
  app-route-policy-counter count_appr_pm9008_1003
   packets 0
   bytes   0
  app-route-policy-counter count_appr_pm9008_1004
   packets 265882
   bytes   34997066
```

```
CSR# show sdwan policy data-policy-filter
                                                          POLICER  OOS      OOS
NAME        NAME  COUNTER NAME          PACKETS  BYTES   NAME     PACKETS  BYTES
-------------------------------------------------------------------------------
TCP_Proxy   1     TCP1                  0        0
                  TCP2                  0        0
                  default_action_count  0        0
```

When counter has some value it has below output pattern.

```
CSR# show sdwan policy data-policy-filter
data-policy-filter TCP_Proxy
data-policy-vpnlist 1
  data-policy-counter TCP1
   packets 764954
   bytes   1009386894
  data-policy-counter TCP2
   packets 163154
   bytes   14693558
  data-policy-counter default_action_count
   packets 22
   bytes   7524
```

Related Topics

show sdwan, on page 987

show sdwan policy service-path

To display the next-hop information for an IP packet that a Cisco IOS XE router received from a service-side interface, use the **show sdwan policy service-path** command in the privileged EXEC mode.

show sdwan policy service-path vpn-id *vpn-id* **interface** *interface-name* **source-ip** *ip-address* **dest-ip** *ip-address* **protocol** *number* **source-port** *port-number* **dest-port** *port-number* [**all** | **app** *application-name* | **dscp** *value*]

Syntax Description

vpn-id *vpn-id*	Identifies the service VPN.
interface *interface-name*	Specifies the name of the local interface being used for the IPsec tunnel.
source-ip *ip-address*	Specifies the source IP address number of the local end of the IPsec tunnel.
dest-ip *ip-address*	Specifies the destination IP address of the remote end of the IPsec tunnel.
protocol *number*	Specifies the number of the protocol being used on the IPsec tunnel.
source-port *port-number*	Specifies the port number of the local end of the IPsec tunnel.
dest-port *port-number*	Specifies the port number of the remote end of the IPsec tunnel.
all	Displays all possible paths for a packet.
app *application-name*	Displays the packets associated with the specified DPI application.
dscp *value*	Specifies the DSCP value being used on the IPsec tunnel.*Range:* 0 through 63

Command Default

NA

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You identify the IP packet by specifying fields in the IP header. You can use this command when using application-aware routing, to determine that path taken by the packets associated with a DPI application.

Example

```
Device#show sdwan policy service-path
vpn 1 interface GigabitEthernet 5 source-ip 10.20.24.17 dest-ip 10.20.25.18
protocol 1 Next Hop: IPsec
Source: 10.1.15.15 12346 Destination: 10.1.16.16 12366
Local Color: lte Remote Color: lte Remote System IP: 172.16.255.16
```

show sdwan policy tunnel-path

To display the next-hop information for an IP packet that a Cisco IOS XE router received from a WAN transport tunnel interface, use the **show sdwan policy tunnel-path** command in the privileged EXEC mode.

show sdwan policy tunnel-path vpn-id *vpn-id* **interface** *interface-name* **source-ip** *ip-address* **dest-ip** *ip-address* **protocol** *number* **source-port** *port-number* **dest-port** *port-number* [**all** | **app** *application-name* | **dscp** *value*]

Syntax Description

vpn-id *vpn-id*	Identifies the service VPN.
interface *interface-name*	Specifies the name of the local interface being used for the IPsec tunnel.
source-ip *ip-address*	Specifies the source IP address number of the local end of the IPsec tunnel.
dest-ip *ip-address*	Specifies the destination IP address of the remote end of the IPsec tunnel.
protocol *number*	Specifies the number of the protocol being used on the IPsec tunnel.
source-port *port-number*	Specifies the port number of the local end of the IPsec tunnel.
dest-port *port-number*	Specifies the port number of the remote end of the IPsec tunnel.
all	Displays all possible paths for a packet.
app *application-name*	Displays the packets associated with the specified DPI application.
dscp *value*	Specifies the DSCP value being used on the IPsec tunnel.*Range:* 0 through 63

Command Default

NA

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You identify the IP packet by specifying fields in the IP header. You can use this command when using application-aware routing, to determine that path taken by the packets associated with a DPI application.

Example

```
Device#show sdwan policy tunnel-path
vpn 0 interface ge0/2 source-ip 10.0.5.11 dest-ip 10.0.5.21 protocol 6
source-port 12346 dest-port 12346
```

```
Nexthop: Direct Interface ge0/2 index: 3
```

show security-info

List the configured security information for IPsec tunnel connections (on vEdge routers only).

show security-info [**authentication-type** | **encryption-supported** | **fips-mode** | **pairwise-keying** | **rekey** | **replay-window**]

Syntax Description

None	Lists information about all configured IPsec tunnel security parameters.
authentication-type	Lists the configured authentication type for IPsec tunnels.
encryption-supported	Lists the supported encryption type.
fips-mode	Displays whether fips mode is enabled or disabled.
pairwise-keying	Displays whether pairwise-keying is enabled or disabled.
rekey	Lists the configured rekeying time for IPsec tunnels, in seconds.
replay-window	Lists the configured replay window size for IPsec tunnels.

Command History

Release	Modification
14.2	Command introduced.
16.2	Added support for displaying authentication negotiation.
17.2	Added FIPS status
Cisco SD-WAN Release 20.6.1	The output of this command was modified to included an additional field, `security-info integrity-type`.

The following is a sample output from the **show security-info** command applicable to Cisco SD-WAN Release 20.6.1 and later.

```
vm4# show security-info
security-info authentication-type deprecated
security-info rekey  86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (for unicast & multicast)"
security-info fips-mode Enabled
security-info pairwise-keying Disabled
security-info integrity-type "ip-udp-esp esp"
```

The following is a sample output from the **show security-info** command applicable to releases before Cisco SD-WAN Release 20.6.1.

```
vEdge# show security-info
security-info authentication-type "SHA1_HMAC / NULL"
security-info rekey 3600000
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 and, for multicast, AES_256_CBC"
security-info fips-mode Enabled
```

Related Topics

ipsec, on page 271

show nms server-proxy ratelimit

To view rate limits for bulk and non-bulk APIs, use the **show nms server-proxy ratelimit** command in the operational mode.

show nms server-proxy ratelimit

Syntax Description

This command has no arguments or keywords.

Command Modes

Operational mode (#)

Command History

Release	Modification
Cisco vManage Release 20.10.1	This command is introduced.

Examples

The following is a sample output of the **show nms server-proxy ratelimit** command on a single Cisco vManage node:

```
vManage# show nms server-proxy ratelimit

Non Bulk API: 100/second (per node)

Bulk API: 48/minute (per node)
```

The following is a sample output of the **show nms server-proxy ratelimit** command on a Cisco vManage node belonging to a three-node cluster:

```
vManage# show nms server-proxy ratelimit
Non Bulk API: 100/second (per node)
Bulk API: 150/minute (across cluster)
```

Related Commands

Command	Description
request nms server-proxy set ratelimit	Configures rate limits for bulk and non-bulk APIs on the Cisco vManage server-proxy.

show software

List the software images that are installed on the local device (on vEdge routers and vSmart controllers).

show software *image-name* [**active** | **confirmed** | **default** | **previous** | **timestamp**]

show software

Syntax Description

None	List information about all software images installed on the local device.
[**active** | **confirmed** | **default** | **previous** | **timestamp**]	Software Image Status: List whether the image is the actively running image, the default image, or the previously running image, when the image was installed, and who confirmed the software installation.
image-name	Specific Software Image: List information about a specific software image.

Command History

Release	Modification
15.3.3	Command introduced for vEdge 100 routers only.
15.4	Command available on all Cisco SD-WAN devices.

Example

```
vEdge# show software

VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
15.3.3    true    true     false     -          2015-10-08T12:54:50-00:00
```

Related Topics

request download, on page 668
request software activate, on page 701
request software install-image, on page 704
request software remove, on page 705
request software reset, on page 706
show version, on page 1036

show support omp peer

To display information about the active OMP peer sessions on the local Cisco SD-WAN Controller or Cisco vEdge device, use the **show support omp peer** command in privilege EXEC mode.

show support omp peer peer-ip *ip-address*

Syntax Description

peer-ip	System-IP address of the connected Cisco Catalyst SD-WAN device.
ip-address	Display configuration OMP peer session information about a specific peer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modifications
Cisco SD-WAN Release 20.8.1	This command was introduced.
Cisco Catalyst SD-WAN Control Components Release 20.11.1	Added the **TLOC color supported list** field in the output.

Usage Guidelines

Detailed information about OMP peer is displayed along with all timers and assigned policies in XML format.

The following is a sample output from the **show support omp peer** command:

```
Device# show support omp peer peer-ip 172.16.255.41
================================
            PEERS for CONTEXT 172.16.255.41
================================
 Local address: 172.16.255.41
 Looking up Peer: 172.16.255.5
 Peer: 172.16.255.5 (0x7fd197ee1800), Type: vSmart, Site: 200, Region-id-set: None, Domain:
 1, Overlay: 1, Legit: yes
        State: Up, version: 1, Control-Up: yes, Staging: no, flags: 0x21
        CAP: BR: no, TGW: no
       Multithreading- down: no, move-marker: no, update-gen: no, work-queue: no, needs_upd:
 0x0
        buffer ev: 0x0x7fd197aca580
        fd: 21
        Hello timer: Enabled (e: 2, c: 20, md: 20 lmd: 0)  Hold timer: Enabled (e: 43 v:
60 c: 60)
        Connect retry: Disabled (e: -1 v: 2 c: 2)  Adv. timer: Enabled (e: 1 v: 1 c: 1)
        Down-pending: Disabled (e: -1 v: 1 c: 1)
    EOR interval: 300 EOR timer: Disabled (e: -1 v: 300)

    Force-Send interval: 2 Force-Send timer: Disabled (e: -1 v: 2)

        Rcv cap: Identity MP GR Refresh Security Overlay
        Neg cap: Identity MP GR Refresh Security Overlay
        Rcv afi-safi: TLOC-IPV4 SRVC-IPV4 SRVC-IPV6 ROUTE-IPV4 ROUTE-IPV6 MCAST-IPV4 (2)
LINK CXP (2)
        Neg afi-safi: TLOC-IPV4 SRVC-IPV4 SRVC-IPV6 ROUTE-IPV4 MCAST-IPV4 (2) LINK CXP (2)
        GR-enabled: Enabled, My GR interval: 43200 GR timer: Disabled (e: -1 v: 43200 c:
43200)
        Enter gr: 0, Exit gr: 0, GR mode: FALSE
        site-pol: None route-pol-in: None route-pol-out: None data-pol-in: None
           data-pol-out: None pfr-pol: None mem-pol: None cflowd:None
        UP time: Wed Feb 16 17:55:50 2022
        Last DOWN time: Thu Jan  1 00:00:00 1970
        Down Event: Invalid, Err code: Invalid, Subcode: 0, Down-pend: no
        UP: 1, DOWN: 0, CONN: 1
        Read before hold: 0, Buf pullups: 13
        Buffer thresholds: 0, upd pkt thresholds: 0
        Nothing Read: 29286, Partial Msg: 132
        Direct pkts: 28429 Direct hello send: 0
        Bad marker: 0 Read error: 0
        Read in down pending: 0, Read in null evbuf: 0
        Enter gr: 0, Exit gr: 0
        Policy received: Complete
       Forwarding policy len: 1346
<app-route-policy>
  <name>_VPN_1_web-ssh-AAR</name>
  <vpn-list>
    <name>VPN_1</name>
    <sequence>
      <seq-value>1</seq-value>
```

```
      <match>
        <source-ip>0.0.0.0/0</source-ip>
        <app-list>SSH_policy</app-list>
      </match>
      <action>
        <sla-class>
          <sla-class-name>TEST1</sla-class-name>
          <preferred-color>biz-internet</preferred-color>
        </sla-class>
      </action>
    </sequence>
    <sequence>
      <seq-value>11</seq-value>
      <match>
        <source-ip>0.0.0.0/0</source-ip>
        <app-list>web_services</app-list>
      </match>
      <action>
        <sla-class>
          <sla-class-name>TEST1</sla-class-name>
          <preferred-color>biz-internet</preferred-color>
        </sla-class>
      </action>
    </sequence>
  </vpn-list>
</app-route-policy>
<sla-class>
  <name>TEST1</name>
  <loss>10</loss>
  <latency>100</latency>
  <jitter>10</jitter>
</sla-class>
<lists><vpn-list>
  <name>VPN_1</name>
  <vpn>
    <id>1</id>
  </vpn>
</vpn-list>
<app-list>
  <name>SSH_policy</name>
  <app>
    <name>ssh</name>
  </app>
</app-list>
<app-list>
  <name>web_services</name>
  <app-family>
    <name>audio_video</name>
  </app-family>
  <app-family>
    <name>instant-messaging</name>
  </app-family>
  <app-family>
    <name>web</name>
  </app-family>
</app-list>
</lists>

        Statistics:

          TLOC-IPV4:
            EOR - TX: 1 RX: 1
            Browse-Done: 1 Force-Send: 0
            received: 20 installed: 0 sent: 2
```

```
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 2121 ri-browsed: 2121 te-changed: 0
  ctx-rib-version: 3150 peer-ro-version: 3150

TLOC-IPV6:
  EOR - TX: 0 RX: 0
  Browse-Done: 0 Force-Send: 0
  received: 0 installed: 0 sent: 0
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
  ctx-rib-version: 0 peer-ro-version: 0

SECURITY:
  EOR - TX: 0 RX: 0
  Browse-Done: 0 Force-Send: 0
  received: 0 installed: 0 sent: 0
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
  ctx-rib-version: 0 peer-ro-version: 0

SRVC-IPV4:
  EOR - TX: 1 RX: 1
  Browse-Done: 1 Force-Send: 0
  received: 0 installed: 0 sent: 4
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 2 ri-browsed: 4 te-changed: 0
  ctx-rib-version: 4 peer-ro-version: 4

SRVC-IPV6:
  EOR - TX: 1 RX: 1
  Browse-Done: 1 Force-Send: 0
  received: 0 installed: 0 sent: 0
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
  ctx-rib-version: 0 peer-ro-version: 0

ROUTE-IPV4:
  EOR - TX: 1 RX: 1
  Browse-Done: 1 Force-Send: 0
  received: 88 installed: 0 sent: 4
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 364 ri-browsed: 4784 te-changed: 0
  ctx-rib-version: 802 peer-ro-version: 802

ROUTE-IPV6:
  EOR - TX: 0 RX: 0
  Browse-Done: 0 Force-Send: 0
  received: 0 installed: 0 sent: 0
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
  ctx-rib-version: 0 peer-ro-version: 0

MCAST-IPV4:
  EOR - TX: 1 RX: 1
  Browse-Done: 1 Force-Send: 0
  received: 0 installed: 0 sent: 0
  ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
  marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
  ctx-rib-version: 0 peer-ro-version: 0

MCAST-IPV6:
  EOR - TX: 0 RX: 0
  Browse-Done: 0 Force-Send: 0
  received: 0 installed: 0 sent: 0
```

```
    ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
    marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
    ctx-rib-version: 0 peer-ro-version: 0

  LINK:
    EOR - TX: 1 RX: 1
    Browse-Done: 1 Force-Send: 0
    received: 6 installed: 0 sent: 0
    ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
    marker-reset: 0 routes-browse: 355 ri-browsed: 355 te-changed: 0
    ctx-rib-version: 744 peer-ro-version: 680

  CXP:
    EOR - TX: 1 RX: 1
    Browse-Done: 1 Force-Send: 0
    received: 0 installed: 0 sent: 0
    ri-cleanup: 0 ro-cleanup: 0 ri-reeval: 0 reeval: 0
    marker-reset: 0 routes-browse: 0 ri-browsed: 0 te-changed: 0
    ctx-rib-version: 0 peer-ro-version: 0

Packet Statistics:

  hello-tx:          28429   hello-rx:          28426
  handshake-tx:          1   handshake-rx:          1
  alert-tx:              0   alert-rx:              0
  update-tx:            32   update-rx:         2217
  inform-tx:             7   inform-rx:             7
  policy-tx:             0   policy-rx:             3
  total-tx:          28469   total-rx:          30654
```

The following example, executed on a Cisco SD-WAN Controller, shows the TLOC colors that the peer device 10.0.0.15 is advertising—in this case, lte and 3g.

```
vsmart# show support omp peer peer-ip 10.0.0.15 | inc color
ed bitmap: 0xc0, TLOC color supported list: lte 3g
```

show system buffer-pool-status

Display statistics about internal data packet buffers, which are used in the forwarding path.

show system buffer-pool-status

Syntax Description

None

Command History

Release	Modification
17.2	Command introduced.

Example

```
vEdge# show system buffer-pool-status
Pool   Block-Size   Max-Blocks Avail-Blocks
  0            0       655209
  1            0       677233
  2            0         3920
  3            0        10201
  4            0         7982
  5            0         8180
  6            0         6140
  7            0            0
```

Related Topics

show interface queue, on page 843
show interface statistics, on page 851
show system statistics, on page 1015

show system netfilter

Display the iptable entries, also called iptable/netfilter entries, on the local device (on vSmart controllers and vManage NMSs only). The netfilter is a kernel module that does packet filtering based on firewall rules.

show system netfilter

Syntax Description

None

Command History

Release	Modification
15.4.3	Command introduced.

Example

```
vSmart# show system netfilter
Chain INPUT (policy ACCEPT 60302 packets, 6353K bytes)
 pkts bytes target     prot opt in     out     source               destination
 4649  391K POLICE     all  --  eth1   *       0.0.0.0/0            0.0.0.0/0
limit: avg 10000/sec burst 1000
 4649  391K POLICE_PROT  all  --  eth1   *       0.0.0.0/0            0.0.0.0/0
 limit: avg 10000/sec burst 1000
   53  5102 LOGGING    all  --  eth1   *       0.0.0.0/0            0.0.0.0/0

Chain POLICE (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain POLICE_PROT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  eth1   *       0.0.0.0/0            0.0.0.0/0
tcp spts:67:68 dpts:67:68
```

```
    0     0 ACCEPT     tcp  --  eth1   *       0.0.0.0/0            0.0.0.0/0
tcp spt:53
    0     0 ACCEPT     udp  --  eth1   *       0.0.0.0/0            0.0.0.0/0
udp spt:53
 4596  386K ACCEPT     icmp --  eth1   *       0.0.0.0/0            0.0.0.0/0

Chain LOGGING (1 references)
 pkts bytes target     prot opt in     out     source               destination
   53  5102 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0
limit: avg 10/sec burst 5 LOG flags 0 level 6 prefix "IPTables-dropped: "
   53  5102 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Related Topics

iptables-enable, on page 272

show system on-demand

To display the status of on-demand tunnels, use the **show system on-demand** command in privileged EXEC mode.

show [**sdwan**] **system on-demand** [**remote-system**] [**system-ip** *ip-address*]

Syntax Description

sdwan	Include **sdwan** only when using the command on a Cisco IOS XE Catalyst SD-WAN device, not on a Cisco vEdge device.
remote-system	Use **remote-system** to include on-demand tunnel information about all connected devices. For example, if device A has numerous on-demand tunnels configured to other devices, and you use (for a Cisco IOS XE Catalyst SD-WAN device) **show sdwan system on-demand remote-system** on device A, the output includes information for each site that device A is connected to. The information for each site includes whether the site has on-demand tunnels enabled, whether the tunnel to the site is active, inactive, or not in on-demand tunnel mode, and so on. Without this keyword, the command provides only the local status of the device on which the command is executed. For example, if you execute this command on device A, without **remote-system**, the output shows only the local on-demand tunnel status of device A.
system-ip *ip-address*	Displays the output only for the specified device.

Command Default

Not applicable.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This command was introduced.

Usage Guidelines

Use this command on a hub or spoke device. The output shows the following:

- **SITE-ID**: Site ID.
- **SYSTEM-IP**: IP address of the device.
- **ON-DEMAND**:
  - **yes**: On-demand tunnels are enabled on the device.
  - **no**: On-demand tunnels are not enabled on the device.
- **STATUS**:
  - **active**: The on-demand tunnel to this device is active.
  - **inactive**: The on-demand tunnel to this device is inactive.
  - **not-on-demand**: On-demand tunnels are enabled on the device, but this tunnel is not in on-demand mode because another device at the same multi-home site does not have on-demand tunnels enabled.
- **IDLE-TIMEOUT-CFG(min)**: Configured on-demand tunnel timeout (minutes) for this device.
- **IDLE-TIMEOUT-EXPIRY(sec)**: Seconds before timeout for this on-demand tunnel.

Example

In the following example, **show sdwan system on-demand** is executed on a Cisco IOS XE Catalyst SD-WAN device, so it includes the **sdwan** keyword.

The output shows the on-demand tunnel configuration of the device on which the command was executed, which is at site 800 in the example. On-demand tunnels are enabled.

```
Device#show sdwan system on-demand
SITE-ID    SYSTEM-IP     ON-DEMAND       STATUS     IDLE-TIMEOUT-CFG(min)
-------------------------------------------------------------------------
800        10.0.0.18        yes          active              10
```

Example

In the following example **show sdwan system on-demand remote-system** is executed on a Cisco IOS XE Catalyst SD-WAN device, so it includes the **sdwan** keyword.

The output shows the status of 5 devices at a total of 4 sites. Site 500 is a multi-home site, with 2 devices. Because one of the devices at site 500 (10.0.0.15) does not have on-demand tunnels enabled, the other device at the site (10.0.016) has a status of not-on-demand even though that device has on-demand tunnels enabled.

```
Device#show sdwan system on-demand remote-system
SITE-ID    SYSTEM-IP     ON-DEMAND       STATUS     IDLE-TIMEOUT-EXPIRY(sec)
-------------------------------------------------------------------------
300        10.0.0.11        yes          inactive            -
200        10.0.0.12        no           -                   -
400        10.0.0.14        yes          active              48
500        10.0.0.15        no           -                   -
500        10.0.0.16        yes          not-on-demand       -
```

In the following example, **system-ip** is used to display the status of a single device.

```
Device#show sdwan system on-demand remote-system system-ip 10.0.0.10
SITE-ID    SYSTEM-IP     ON-DEMAND       STATUS     IDLE-TIMEOUT-EXPIRY(sec)
------------------------------------------------------------------------
400        10.0.0.10       yes           active              33
```

show system statistics

Display system-wide forwarding statistics (on vEdge routers only).

show system statistics [**diff**]

Syntax Description

None	Display all system statistics.
diff	Statistics Changes: Display the changes in statistics since you last issued the **show system statistics** command.

Command History

Release	Modification
14.1	Command introduced.
16.3.2	Add display BFD PMTU statistics.

Example

```
vEdge# show system statistics

                                rx_pkts :      172639782
                               rx_drops :      0
                                 ip_fwd :      123848170
                       ip_fwd_mirror_pkts :      0
                                ip_fwd_arp :      10899
                          ip_fwd_to_egress :      61493879
                         ip_fwd_invalid_oil :      0
                          ip_v6_mcast_drops :      0
                 ip_fwd_mcast_invalid_iif :      0
           ip_fwd_mcast_life_exceeded_drops :      0
                rx_mcast_threshold_exceeded :      0
                     ip_fwd_invalid_tun_oil :      0
                  rx_mcast_policy_fwd_drops :      0
                  rx_mcast_mirror_fwd_drops :      0
                    ip_fwd_null_mcast_group :      0
                           ip_fwd_null_nhop :      210416
                    ip_fwd_unknown_nh_type  :      0
                       ip_fwd_nat_on_tunnel :      0
                              ip_fwd_to_cpu :      25051507
                  ip_fwd_to_cpu_nat_xlates :      0
                ip_fwd_from_cpu_nat_xlates :      0
```

```
          ip_fwd_to_cpu_nat_drops :      0
        ip_fwd_from_cpu_non_local :      0
                  ip_fwd_rx_ipsec :      46576642
                 ip_fwd_mcast_pkts :      0
                     ip_fwd_rx_gre :      0
                nat_xlate_outbound :      63509046
         nat_xlate_outbound_drops :      966598
                nat_xlate_inbound :      31683862
          nat_xlate_inbound_fail :      257
                        rx_bcast :      9724255
                    cflowd_pkts :      769419
                        rx_mcast :      28365292
               rx_mcast_link_local :      28365240
           rx_mcast_filter_to_cpu :      0
  rx_mcast_filter_to_cpu_and_fwd :      0
                     rx_gre_decap :      0
                     rx_gre_drops :      0
             rx_gre_policer_drops :      0
            rx_implicit_acl_drops :      9618739
                   rx_ipsec_decap :      46574988
              rx_ip6_ipsec_drops :      0
               rx_sa_ipsec_drops :      0
              rx_spi_ipsec_drops :      2
                 rx_replay_drops :      545
       rx_replay_integrity_drops :      9
         rx_next_hdr_ipsec_drops :      0
      rx_mac_compare_ipsec_drops :      0
          rx_err_pad_ipsec_drops :      0
          rx_ipsec_policer_drops :      0
               rx_pre_ipsec_pkts :      0
              rx_pre_ipsec_drops :      0
      rx_pre_ipsec_policer_drops :      0
              rx_pre_ipsec_decap :      0
             openssl_aes_decrypt :      0
                 qat_aes_decrypt :      0
             openssl_gcm_decrypt :      46575030
                 qat_gcm_decrypt :      0
              rx_ipsec_bad_inner :      0
                    rx_bad_label :      0
               service_label_fwd :      0
               rx_host_local_pkt :      0
             rx_host_mirror_drops :      0
                 rx_tunneled_pkts :      0
                  rx_cp_non_local :      0
            tx_if_not_preferred :      0
                  tx_vsmart_drop :      0
                 rx_invalid_port :      0
                port_disabled_rx :      0
                  ip_disabled_rx :      0
                rx_invalid_qtags :      44
                 rx_non_ip_drops :      892
                      rx_ip_errs :      0
                  pko_wred_drops :      0
               tx_queue_exceeded :      0
                rx_policer_drops :      0
               rx_policer_remark :      0
                   route_to_host :      0
                     ttl_expired :      0
                  icmp_redirect :      0
                  bfd_rx_non_ip :      0
           bfd_tx_record_changed :      41
           bfd_rx_record_invalid :      0
                bfd_rx_parse_err :      0
        rx_arp_rate_limit_drops :      0
```

```
          rx_arp_non_local_drops :      47220007
                      rx_arp_reqs :      69873
                  rx_arp_replies :      760095
                    arp_add_fail :      38578773
                 unknown_nh_type :      0
                 buf_alloc_fails :      0
                   ecmp_discards :      0
      app_route_policy_discards :      0
                   cbf_discards :      0
                   filter_drops :      0
                invalid_back_ptr :      0
               tunnel_loop_drops :      0
            to_cpu_policer_drops :      28046800
                   mirror_drops :      0
             split_horizon_drops :      0
                   rx_no_tun_if :      0
                        tx_pkts :      155590511
                     tx_errors :      0
                      tx_bcast :      508522
                      tx_mcast :      249169
               port_disabled_tx :      5
                  ip_disabled_tx :      0
             tx_fragment_needed :      0
          tx_mcast_fragment_needed :      0
                 fragment_df_drops :      0
                      tx_fragments :      0
                tx_fragment_drops :      0
                 tx_fragment_fail :      0
            tx_fragment_alloc_fail :      0
               tunnel_pmtu_lowered :      0
                        tx_gre_pkts :      0
                       tx_gre_drops :      0
              tx_gre_policer_drops :      0
                       tx_gre_encap :      0
                     tx_ipsec_pkts :      46694074
               tx_ipsec_mcast_pkts :      0
                tx_ip6_ipsec_drops :      0
           tx_no_out_sa_ipsec_drops :      0
            tx_zero_spi_ipsec_drops :      0
             tx_no_tunn_ipsec_drops :      0
             tx_ipsec_policer_drops :      0
                     tx_ipsec_encap :      46694074
              tx_ipsec_mcast_encap :      0
                 tx_pre_ipsec_pkts :      46694074
      tx_no_out_sa_pre_ipsec_drops :      0
        tx_no_tunn_pre_ipsec_drops :      0
               openssl_aes_encrypt :      0
                   qat_aes_encrypt :      0
               openssl_gcm_encrypt :      46694074
                   qat_gcm_encrypt :      0
        tx_pre_ipsec_policer_drops :      0
                tx_pre_ipsec_encap :      46694074
                    tx_arp_replies :      69899
                       tx_arp_reqs :      508502
                   tx_arp_req_fail :      2
                    tx_no_arp_drop :      4
             tx_arp_rate_limit_drops :      5
               tx_icmp_policer_drops :      0
              tx_icmp_mirrored_drops :      0
                       bfd_tx_fail :      0
                    bfd_alloc_fail :      0
                 bfd_timer_add_fail :      0
                       bfd_tx_pkts :      46385012
                       bfd_rx_pkts :      46278322
```

```
                    bfd_tx_octets :      7107533768
                    bfd_rx_octets :      7104071388
                  bfd_pmtu_tx_pkts :      23522
                  bfd_pmtu_rx_pkts :      23199
                 bfd_pmtu_tx_octets :      29353636
                 bfd_pmtu_rx_octets :      8886087
                       bfd_rec_down :      0
                    bfd_rec_invalid :      0
                      bfd_lkup_fail :      0
               rx_icmp_echo_requests :      0
                rx_icmp_echo_replies :      846060
             rx_icmp_network_unreach :      210414
                rx_icmp_host_unreach :      1109
                rx_icmp_port_unreach :      0
            rx_icmp_protocol_unreach :      0
           rx_icmp_fragment_required :      0
           rx_icmp_dst_unreach_other :      0
                 rx_icmp_ttl_expired :      0
                    rx_icmp_redirect :      0
                 rx_icmp_src_quench :      0
                 rx_icmp_bad_ip_hdr :      0
                rx_icmp_other_types :      4398628
               tx_icmp_echo_requests :      602847
                tx_icmp_echo_replies :      0
             tx_icmp_network_unreach :      210416
                tx_icmp_host_unreach :      0
                tx_icmp_port_unreach :      0
            tx_icmp_protocol_unreach :      0
           tx_icmp_fragment_required :      0
           tx_icmp_dst_unreach_other :      0
                 tx_icmp_ttl_expired :      0
                    tx_icmp_redirect :      0
                 tx_icmp_src_quench :      0
                 tx_icmp_bad_ip_hdr :      0
                tx_icmp_other_types :      2
                     gre_ka_tx_pkts :      0
                     gre_ka_rx_pkts :      0
          gre_ka_tx_ipv4_options_drop :      0
                   gre_ka_tx_non_ip :      0
                gre_ka_tx_parse_err :      0
            gre_ka_tx_record_changed :      0
                     gre_ka_tx_fail :      0
                  gre_ka_alloc_fail :      0
               gre_ka_timer_add_fail :      0
                    gre_ka_rx_non_ip :      0
               gre_ka_rx_rec_invalid :      0
                      dot1x_rx_pkts :      0
                      dot1x_tx_pkts :      0
                    dot1x_rx_drops :      0
                    dot1x_tx_drops :      0
        dot1x_vlan_if_not_found_drops :      0
               dot1x_mac_learn_drops :      0
                      dns_req_snoop :      0
                      dns_res_snoop :      0
                   redirect_dns_req :      0
                      ctrl_loop_fwd :      0
                ctrl_loop_fwd_drops :      0
                rx_replay_drops_tc0 :      0
                rx_replay_drops_tc1 :      0
                rx_replay_drops_tc2 :      545
                rx_replay_drops_tc3 :      0
                rx_replay_drops_tc4 :      0
                rx_replay_drops_tc5 :      0
                rx_replay_drops_tc6 :      0
```

```
                rx_replay_drops_tc7 :      0
                rx_window_drops_tc0 :      0
                rx_window_drops_tc1 :      0
                rx_window_drops_tc2 :      768
                rx_window_drops_tc3 :      0
                rx_window_drops_tc4 :      0
                rx_window_drops_tc5 :      0
                rx_window_drops_tc6 :      0
                rx_window_drops_tc7 :      0
    rx_unexpected_replay_drops_tc0 :      0
    rx_unexpected_replay_drops_tc1 :      0
    rx_unexpected_replay_drops_tc2 :      0
    rx_unexpected_replay_drops_tc3 :      0
    rx_unexpected_replay_drops_tc4 :      0
    rx_unexpected_replay_drops_tc5 :      0
    rx_unexpected_replay_drops_tc6 :      0
    rx_unexpected_replay_drops_tc7 :      0
     rx_replay_integrity_drops_tc0 :      9
     rx_replay_integrity_drops_tc1 :      0
     rx_replay_integrity_drops_tc2 :      0
     rx_replay_integrity_drops_tc3 :      0
     rx_replay_integrity_drops_tc4 :      0
     rx_replay_integrity_drops_tc5 :      0
     rx_replay_integrity_drops_tc6 :      0
     rx_replay_integrity_drops_tc7 :      0
            icmp_redirect_tx_drops :      0
            icmp_redirect_rx_drops :      0
```

Related Topics

clear system statistics, on page 618
show app log flow-count, on page 738
show app log flows, on page 739
show system buffer-pool-status, on page 1011
show tunnel statistics, on page 1033

show system status

Display time and process information for the device, as well as CPU, memory, and disk usage data.

show system status

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
15.3	Changed format of command output for vEdge 100 routers.
15.4	Changed format of command output changed for all devices.
16.3.2	Added system state field to output on vEdge routers.

Release	Modification
17.1	Added CPU-reported reboot field to output on hardware vEdge routers.
17.2	Added CPU allocation field to output on hardware vEdge routers; added FIPS state.

Examples

Example 1

In Releases 17.1 and later:

```
vEdge# show system status

Cisco SD-WAN (tm) vedge Operating System Software
Copyright (c) 2013-2018 by Cisco, Inc.
Version: 17.1.0

System logging to host is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Enabled

Last reboot:             Initiated by user - activate 17.1.0.
CPU-reported reboot:     Warm
Boot loader version:     U-Boot 2013.07-ga9b015 (Build time: May 12 2016 - 13:58:12)

System uptime:           0 days 03 hrs 27 min 26 sec
Current time:            Tue Mar 28 12:59:02 PDT 2017

Load average:            1 minute: 0.11, 5 minutes: 29, 15 minutes: 38
Processes:               241 total
CPU allocation:          32 total,   3 control,   29 data,   1 tcpd
CPU states:              11.00% user,   10.10% system,   78.90% idle
Memory usage:            2973024K total,    752796K used,   1865932K free
                         65348K buffers,  288948K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       3621M  82M  2595M    24%   /

Personality:             vedge
Model name:              vedge-1000
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
```

Example 2

In Releases 16.3.2 and later:

```
vEdge# show system status

Cisco SD-WAN (tm) vedge Operating System Software
Copyright (c) 2013-2018 by Cisco, Inc.
Version: 16.3.1
```

```
System logging to host is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up

Last reboot:             Unknown.
Boot loader version:     Not applicable

System uptime:           0 days 10 hrs 30 min 31 sec
Current time:            Mon Feb 06 20:13:54 PST 2017

Load average:            1 minute: 0.01, 5 minutes: 0.05, 15 minutes: 0.05
Processes:               150 total
CPU allocation:          2 total,   1 control,   1 data
CPU states:              2.40% user,   3.00% system,   94.60% idle
Memory usage:            879624K total,    551036K used,   64176K free
                         88772K buffers,  175640K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       7551M  26M  7099M   0%   /

Personality:             vedge
Model name:              vedge-cloud
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
```

Example 3

In Releases 15.4 and later for all Cisco vEdge devices, and in Release 15.3 for vEdge 100 routers only:

```
vEdge# show system status
Cisco SD-WAN (tm) vedge Operating System Software
Copyright (c) 2013-2016 by Cisco, Inc.
Version: 16.1.0
System logging to host  is disabled
System logging to disk is enabled

Last reboot:             Unknown.
Boot loader version:     Not applicable
System uptime:           0 days 04 hrs 39 min 42 sec
Current time:            Wed May 04 15:56:58 PDT 2016

Load average:            1 minute: 1.05, 5 minutes: 1.11, 15 minutes: 1.18
Processes:               229 total
CPU allocation:          2 total,   1 control,   1 data
CPU states:              83.40% user,   13.30% system,   0.00% idle
Memory usage:            753940K total,    408692K used,   180744K free
                         26412K buffers,  138092K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       7679M  26M  7227M   0%   /

Personality:             vedge
Model name:              vedge-cloud
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
```

```
vSmart# show system status

Cisco SD-WAN (tm) vsmart Operating System Software
Copyright (c) 2013-2016 by Cisco, Inc.
Version: 16.1.0

System logging to host  is disabled
System logging to disk is enabled

Last reboot:             Unknown.
Boot loader version:     Not applicable
System uptime:           0 days 04 hrs 43 min 26 sec
Current time:            Wed May 04 16:00:19 PDT 2016

Load average:            1 minute: 0.01, 5 minutes: 0.06, 15 minutes: 0.08
Processes:               202 total
CPU states:              0.30% user,   1.30% system,   98.20% idle
Memory usage:            496720K total,    208256K used,   173712K free
                         20348K buffers,  94404K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/root       7679M  35M  7218M   0%   /

Personality:             vsmart
Model name:              vsmart
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Policy template:         None
Policy template version: None
```

Example 4

In Releases 15.3 and earlier for all Cisco vEdge devices except vEdge 100 routers:

```
vEdge# show system status

Cisco SD-WAN (tm) vedge Operating System Software
Copyright (c) 2013-2015 by Cisco, Inc.
Version: 15.3.4

System logging to host  is disabled
System logging to disk is enabled

Last reboot:             .
System uptime:           0 days 10 hrs 34 min 41 sec
Current time:            Tue Nov 03 22:11:43 PST 2015

Load average:            1 minute: 0.03   5 minutes: 0.04   15 minutes: 0.05
Processes:               106 total, 4 running
CPU states:              1.70% user,   1.70% system,   96.60% idle
Memory usage:            757304K total,    336244K used,   216656K free
                         83032K buffers,  121372K cache

Disk usage:              Filesystem      Size  Used  Avail  Use%  Mounted on
                         /dev/root       9.0G  895M  8.1G   10%   /

Personality:             vedge
Services:                None
vManaged:                false
```

```
Commit pending:          false

vSmart# show system status

Cisco SD-WAN (tm) vsmart Operating System Software
Copyright (c) 2013-2015 by Cisco, Inc.
Version: 15.3.2

System logging to host  is disabled
System logging to disk is enabled

Last reboot:             .
System uptime:           0 days 06 hrs 52 min 52 sec
Current time:            Wed Sep 23 17:36:45 PDT 2015

Load average:            1 minute: 0.00   5 minutes: 0.01   15 minutes: 0.05
Processes:               88 total, 1 running
CPU states:              0.80% user,   0.70% system,   98.30% idle
Memory usage:            500948K total,    185108K used,   205828K free
                         51808K buffers,  58204K cache

Disk usage:              Filesystem      Size  Used  Avail  Use%  Mounted on
                         /dev/root       5.1G  893M  4.2G   18%   /

Personality:             vsmart
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:  None
Policy template:         None
Policy template version: None
```

Related Topics

show reboot history, on page 983
show uptime, on page 1035
show version, on page 1036

show tech-support

To display general information about the Cisco SD-WAN devices, use the **show tech-support** command in the privileged EXEC mode.

show tech-support

Syntax Description

This command has no arguments or keywords.

Command Default NA

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command introduced to display the admin-tech and memory details.

Usage Guidelines

When a Cisco device reboots, it collects system status information in a compressed tar file to aid in troubleshooting and diagnostics. The tar file is saved in your system's home directory and contains the following information:

- output of commands
- content of files on the local device
- core files
- syslog files for each process
- configuration rollback files

This command is useful for collecting a large amount of information about devices for troubleshooting. The output of this command can be provided to technical support representatives when reporting a problem. The command output displays the output of a number of show commands at once. The output from this command varies depending on your platform and configuration. Where as, the command **request admin-tech** collects all system status information, including core files, log files, and the process (daemon) and operational-related files that are stored in the /var/tech directory on the local device. For more information on **admin-tech** command, see request admin-tech. The **show tech-support** command displays the output from the following **show** commands, as listed in the order below:

- show platform
- show platform software status control-processor brief
- show platform resources
- show memory statistics history
- show memory allocating-process total
- show process memory sorted
- show process memory platform sorted
- show memory lite-chunks totals
- show buffer
- show buffer usage
- show region
- show memory dead totals
- show chunk brief

Example

The following is sample output from the **show tech-support** command. Following are the excerpts from /var/tech/ios file extracted from the admin-tech tar file which shows that the corresponding command output is captured in admin-tech.

```
Device# show tech-support
------------------ show tech-support memory ------------------
```

```
------------------ show clock ------------------


*05:25:59.689 UTC Wed May 29 2019


------------------ show version ------------------

Cisco IOS Software [Gibraltar], Virtual XE Software (X86_64_LINUX_IOSD-UCMK9-M),,
 Experimental Version 17.1.20190425:094712 [polaris_dev-/nobackup/saajanap/polarr
is_Apr25 105]
Copyright (c) 1986-2019 by Cisco Systems, Inc.


Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The



------------------ show sdwan confd-log netconf-trace ------------------

No log to display


------------------ show umbrella config -----------------
```

show tenant-mapping

On a Cisco vBond Orchestrator, to view the mapping of tenants to multitenant Cisco vSmart Controllers, use the **show tenant-mapping** command.

show tenant-mapping [*vSmart-serial-number*]

Syntax Description

[*vSmart-serial-number*]	(Optional) Specify the serial number of a specific Cisco vSmart Controller to view the tenants assigned to it.

Command Default

None

Command Modes

#

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	Command introduced.

Example

```
vBond# show tenant-mapping
VSMART
SERIAL
```

```
NUM       TENANT NAMES                                                                  TENANT COUNT
-------------------------------------------------------------------------------------------------
12345990  [ "multitenancy-Customer6" "multitenancy-Customer4" "multitenancy-Customer3"
"multitenancy-Customer1" ]  4
12345992  -
                        0
12345994  [ "multitenancy-Customer6" "multitenancy-Customer5" "multitenancy-Customer3"
"multitenancy-Customer2" ]  4
12345997  -
                        0
12345998  -
                        0
12346001  [ "multitenancy-Customer5" "multitenancy-Customer4" "multitenancy-Customer2"
"multitenancy-Customer1" ]  4
```

show tenant omp peers

To view information about the OMP peering sessions that are active on the multitenant Cisco vSmart Controller for a particular tenant, use the **show tenant** *tenant-name* **omp peers** command.

show tenant *tenant-name* **omp peers** [*peer-ip-address*] [**detail**]

Syntax Description

tenant-name	Specify the name of a tenant assigned to the multitenant Cisco vSmart Controller.
peer-ip-address	(Optional) View OMP peering session information for a specific peer.
detail	(Optional) View detailed information.

Command Default

None

Command Modes

#

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	Command introduced.

Example

```
vSmart# show tenant multitenancy-Customer1 omp peers
R -> routes received

I -> routes installed

S -> routes sent


                          DOMAIN    OVERLAY   SITE

PEER             TYPE     ID        ID        ID        STATE    UPTIME           R/I/S

-------------------------------------------------------------------------------------------
```

```
172.16.255.14    vedge   1         1         400       up        23:09:40:04       4/0/0
172.16.255.15    vedge   1         1         500       up        0:14:33:55        0/0/0
172.16.255.24    vsmart  1         1         103       up        44:06:36:31       4/0/4
```

show tenant omp routes

To view information about information about OMP routes for a tenant on a multitenant Cisco vSmart Controller, use the **show tenant** *tenant-name* **omp routes** command.

show tenant *tenant-name* **omp routes** [**family** *family-address*] [**vpn** *vpn-id*] [*prefix* | *ip-address*] [**advertised** | **received**] [**detail**]

Syntax Description

tenant-name	Specify the name of a tenant assigned to the multitenant Cisco vSmart Controller.
prefix	(Optional) Lists OMP route information for the specified route prefix.
ip-address	(Optional) Displays IP address of specific route.
family*family-address*	Lists OMP route information for the specified IP family. *family-address* can be **ipv4** or **ipv6**.
vpn*vpn-id*	Lists the OMP routes for the specified VPN.
detail	Lists detailed route information about OMP peering sessions.

Command Default

None

Command Modes

#

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	Command introduced.

Example

```
vSmart# show tenant multitenancy-Customer1 omp routes


-----------------------------------------------------
omp route entries for vpn 1 route 172.16.33.0/24
-----------------------------------------------------
            RECEIVED FROM:
peer            172.16.255.14
```

```
path-id         66

label           1005

status          C,R

loss-reason     not set

lost-to-peer    not set

lost-to-path-id not set

    Attributes:

     originator       172.16.255.14

     type             installed

     tloc             172.16.255.14, mpls, ipsec

     ultimate-tloc    not set

     domain-id        not set

     overlay-id       1

     site-id          400

     region-id        None

     region-path      65534

     preference       not set

     tag              not set

     origin-proto     connected

     origin-metric    0

     as-path          not set

     community        not set

     unknown-attr-len not set

...
```

show tenant-summary

To view information about the tenants assigned to a multitenant Cisco vSmart Controller, use the **show tenant-summary** command.

show tenant-summary [**max-tenants** | **num-active-tenants** | **tenant-org-names** [*tenant-name*] [**detail**] | **detail**]

Syntax Description

max-tenants	View the maximum number of tenants that can be assigned to the Cisco vSmart Controller.

num-active-tenants	View the number of tenants assigned to the Cisco vSmart Controller.
tenant-org-names[*tenant-name*][**detail**]	Enter only the **tenant-org-names** argument to view information on the tenants assigned to the Cisco vSmart Controller, and the tenant and VPN IDs for each tenant. (Optional) Enter a tenant name along with **tenant-org-names** to view information about a specific tenant. (Optional) Enter the **detail** keyword for more detailed information for all or one of the tenants assigned to the Cisco vSmart Controller.
detail	Enter the **detail** keyword for detailed information for all the tenants assigned to the Cisco vSmart Controller.

Command Default

None

Command Modes

#

Command History

Release	Modification
Cisco SD-WAN Release 20.4.1	Command introduced.

Example

```
vSmart# show tenant-summary
tenant-summary max-tenants 24
tenant-summary num-active-tenants 4
                                    TENANT  TENANT
TENANT ORG NAME                     ID      VPN ID
-----------------------------------------------------
multitenancy-Customer1              1       1003
multitenancy-Customer2              2       1004
multitenancy-Customer3              3       1005
multitenancy-Customer4              4       1006
```

show transport connection

Display the status of the DTLS connection to a vBond orchestrator (on vEdge routers and vSmart controllers only).

show transport connection

show transport connection [*ip-address*] [**history** [*index* [**state** *state*]]]

Syntax Description

history [*index*]	Connection History and Index: Display the complete connection history or the connection history of a specific indexed item.

state *state*	Connection State: Display connections with the specified state. *state* can be **up** or **down**.
ip-address	vBond Address: IP address of the vBond orchestrator or the DNS name that points to the vBond orchestrator.

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show transport connection

ADDRESS       HOST                INDEX  TIME                       STATE
-------------------------------------------------------------------------
10.11.12.123  vbond.viptela.com   100    Thu Mar 27 17:35:15 2014   up
                                  99     Thu Mar 27 17:35:13 2014   down
                                  98     Wed Mar 26 11:20:58 2014   up
                                  97     Wed Mar 26 11:16:46 2014   down
                                  96     Wed Mar 26 08:05:24 2014   up
                                  95     Wed Mar 26 08:05:23 2014   down
                                  94     Sun Mar 23 20:20:24 2014   up
                                  93     Sun Mar 23 20:20:22 2014   down
                                  92     Fri Mar 21 16:50:24 2014   up
                                  91     Fri Mar 21 16:50:22 2014   down
50.51.52.111  vbond.viptela.com   76     Thu Mar 27 19:51:51 2014   up
                                  75     Thu Mar 27 19:51:49 2014   down
                                  74     Thu Mar 27 17:35:16 2014   up
                                  73     Thu Mar 27 17:35:14 2014   down
                                  72     Thu Mar 27 14:05:42 2014   up
                                  71     Thu Mar 27 14:05:40 2014   down
                                  70     Thu Mar 27 09:12:54 2014   up
                                  69     Thu Mar 27 09:12:52 2014   down
                                  68     Thu Mar 27 03:25:27 2014   up
                                  67     Thu Mar 27 03:25:25 2014   down
```

Related Topics

track-transport, on page 504

show tunnel gre-keepalives

Display information about the keepalive packets transmitted and received on GRE tunnels that originate on the local router (on vEdge routers only).

show tunnel gre-keepalives [*vpn-id*]

Syntax Description

None	Display keepalive information for all GRE tunnels.

vpn-id	Specific VPN: Display keepalive information for GRE tunnels in a specific VPN.

Command History

Release	Modification
15.4.1	Command introduced.

Example

```
vEdge# show tunnel gre-keepalives

                                                                 REMOTE   REMOTE
     IF                                  ADMIN  OPER   KA       TX       RX       TX       RX       TX       RX
VPN  NAME  SOURCE IP  DEST IP           STATE  STATE  ENABLED  PACKETS  PACKETS  PACKETS  PACKETS  ERRORS   ERRORS  TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------
0    gre1  10.0.5.11  172.168.1.1       up     down   true     0        0        370      0        0        0       0
0    gre2  10.0.5.11  172.168.122.11    up     down   true     0        0        644      0        0        0       0
```

Related Topics

keepalive, on page 279
show interface, on page 827
show tunnel statistics, on page 1033
tunnel-destination, on page 511
tunnel-source, on page 515

show tunnel inbound-connections

Display information about the IPsec tunnel connections that originate on the local router, showing the TLOC addresses for both ends of the tunnel (on vEdge routers only).

In Releases 15.2 and later, this command has been renamed to **show ipsec outbound-connections**.

show tunnel inbound-connections

show tunnel inbound-connections *local-tloc-address* [*local-color* [*remote-tloc-address* [*remote-color* [(**dest-ip** | **dest-port** | **source-ip** | **source-port**)]]]]

Syntax Description

None	Display information for all the IPsec connections that originate on the vEdge router. The tunnel connections are listed in order according to the local TLOC address.
local-tloc-address [*local-color* [*remote-tloc-address* [*remote-color* [(**dest-ip** | **dest-port** | **source-ip** | **source-port**)]]]]	Specific Tunnel Connection: Display information for a specific IPsec connection.

Command History

Release	Modification
14.1	Command introduced.
15.2	Command renamed to **show ipsec outbound-connections**

Example

```
vEdge# show tunnel inbound-connections
SOURCE           SOURCE  DEST             DEST    REMOTE           REMOTE           LOCAL            LOCAL
IP               PORT    IP               PORT    TLOC ADDRESS     TLOC COLOR       TLOC ADDRESS     TLOC COLOR
-------------------------------------------------------------------------------------------------------------------
10.1.14.14       12350   10.0.5.11        12346   172.16.255.14    lte              172.16.255.11    lte
10.1.15.15       12346   10.0.5.11        12346   172.16.255.15    lte              172.16.255.11    lte
10.1.16.16       12346   10.0.5.11        12346   172.16.255.16    lte              172.16.255.11    lte
10.0.5.21        12346   10.0.5.11        12346   172.16.255.21    lte              172.16.255.11    lte
```

Related Topics

show tunnel local-sa, on page 1032
show ipsec outbound-connections, on page 875

show tunnel local-sa

Display the IPsec tunnel security associations for the local TLOCs (on vEdge routers only).

In Releases 15.2 and later, this command has been renamed to **show ipsec local-sa**.

show tunnel local-sa

show tunnel local-sa *tloc-address* [*color* [**spi** [(**auth-key-hash** | **encrypt-key-hash** | **ip** | **port**)]]]]

Syntax Description

None	Display information for all the IPsec tunnels that originate on the router. The tunnel connections are listed in order according to the local TLOC address.
tloc-address [*color* [**spi** [(**auth-key-hash** | **encrypt-key-hash** | **ip** | **port**)]]]]	Specific SA: Display information for a specific security association.

Command History

Release	Modification
14.1	Command introduced.
15.2	Command renamed to **show ipsec local-sa**.

Example

```
vEdge# show tunnel local-sa
                                                SOURCE           SOURCE
TLOC ADDRESS     TLOC COLOR       SPI      IP               PORT    KEY HASH
-------------------------------------------------------------------------------
172.16.255.15    lte              260      10.1.15.15       12346   *****0979
```

Related Topics

rekey, on page 419
request security ipsec-rekey, on page 700
show tunnel inbound-connections, on page 1031
show ipsec outbound-connections, on page 875

show tunnel statistics

Display information about the packets transmitted and received on the data plane tunnels that originate on the local router (on vEdge routers only).

show tunnel statistics

show tunnel statistics bfd

show tunnel statistics dest-ip *ip-address*

show tunnel statistics dest-port *port-number*

show tunnel statistics ipsec

show tunnel statistics source-ip *ip-address*

show tunnel statistics source-port *port-number*

show tunnel statistics tunnel-protocol (**gre** | **ipsec**)

Syntax Description

None	Display statistics for all data plane tunnels, for both IPsec and GRE tunnels. Note that the output fields are specific for IPsec, so for GRE tunnels, the values for all fields are zero or empty.
bfd	BFD Tunnels: Display statistics for all BFD tunnels.
dest-ip *ip-address***dest-port** *port-number*	Destination IP Address or Port: Display statistics for the specified destination address or destination port number.
ipsec	IPsec Tunnels: Display statistics for IPsec tunnels.
source-ip *ip-address***source-port** *port-number*	Source IP Address or Port: Display statistics for the specified source address or source port number.

tunnel-protocol (**gre** | **ipsec**)	Tunnel Protocol: Display tunnel statistics for either GRE or IPsec tunnels. To display the count of data packets, use the **show interface** command. To display the count of only GRE keepalive packets, use the **show tunnel gre-keepalives** command.

Command History

Release	Modification
14.1	Command introduced.
15.4.1	Added support for GRE tunnels.
16.3.2	Added **bfd** option and display BFD hello and PMTU packet statistics.

Example

Example 1

```
vEdge# show tunnel statistics
                                                                                                                                                                TCP
TUNNEL                                  SOURCE  DEST                  LOCAL   REMOTE  TUNNEL                                                                  MSS
PROTOCOL  SOURCE IP   DEST IP     PORT    PORT    SYSTEM IP      COLOR   COLOR   MTU     tx-pkts  tx-octets  rx-pkts  rx-octets  ADJUST
-------------------------------------------------------------------------------------------------------------------------------------------------------------
ipsec     10.1.15.15  10.0.5.11   12366   12366   172.16.255.11  lte     lte     1441    31726    4895251    31723    5341408    1361
ipsec     10.1.15.15  10.0.5.21   12366   12366   172.16.255.21  lte     lte     1441    31712    4896936    31712    5339686    1361
ipsec     10.1.15.15  10.1.14.14  12366   12366   172.16.255.14  lte     lte     1441    31730    4899623    31727    5344598    1361
ipsec     10.1.15.15  10.1.16.16  12366   12366   172.16.255.16  lte     lte     1441    31723    4895980    31723    5338796    1361
```

Example 2

```
vEdge# show tunnel statistics bfd
                                                BFD     BFD                     BFD     BFD     BFD     BFD     BFD
                                                ECHO    ECHO    BFD     BFD     PMTU    PMTU    PMTU    PMTU
TUNNEL                                  SOURCE  DEST    TX      RX      ECHO TX ECHO RX TX      RX      TX      RX
PROTOCOL  SOURCE IP   DEST IP     PORT    PORT    PKTS    PKTS    OCTETS  OCTETS  PKTS    PKTS    OCTETS  OCTETS
-----------------------------------------------------------------------------------------------------------------
ipsec     10.1.15.15  10.0.5.11   12366   12366   32284   32281   2663437 2663186 42      42      33220   31981
ipsec     10.1.15.15  10.0.5.21   12366   12366   32267   32267   2662031 2662024 45      45      37623   32407
ipsec     10.1.15.15  10.1.14.14  12366   12366   32283   32280   2663358 2663100 47      47      37917   35002
ipsec     10.1.15.15  10.1.16.16  12366   12366   32282   32282   2663265 2663265 41      41      34228   29273
```

Related Topics

clear tunnel statistics, on page 620
show interface, on page 827
show system statistics, on page 1015
show tunnel gre-keepalives, on page 1030

show umbrella deviceid

To display the Umbrella registration status, for Cisco IOS XE Catalyst SD-WAN devices, use the **show umbrella deviceid** command.

show umbrella deviceid

Syntax Description

This command has no arguments or keywords.

Command History

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

Examples

The command displays a table with the registration details:

Column	Description
VRF	Virtual routing forwarding (VRF) instance.
Tag	VPN number from which registration is successful.
Status	Created or Unsuccessful.
Device-id	Unique number associated with the registration.

```
Device# show umbrella deviceid
Device registration details
VRF                  Tag             Status          Device-id
1                    vpn1            201 CREATED     ab00f5cee26f962e
```

show uptime

Show how long the system has been running. This command is the same as the UNIX **uptime** command.

show uptime

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

```
vEdge# show uptime
16:34:32 up  6:29,  1 user,  load average: 0.04, 0.05, 0.05
```

Related Topics

show system status, on page 1019

show users

Display the users currently logged in to the device.

show users

vManage Equivalent

For all Cisco vEdge devices:

Monitor > **Network** > **Real Time** > **Users**

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example

```
vEdge# show users

                                          AUTH
SESSION  USER   CONTEXT  FROM      PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------
96       admin  cli      10.0.1.1  ssh    netadmin   2014-07-24T14:57:43+00:00
```

Related Topics

aaa, on page 24

request aaa unlock-user, on page 654

show version

Display the active version of the Cisco SD-WAN software running on the device.

show version

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example

```
vEdge# show version
15.3.3
```

Related Topics

request software install, on page 702

show vrrp

Display information about the configured VRRP interfaces and groups (on vEdge routers only).

show vrrp [**interfaces** *interface-name*] [**groups** *group-number* [*vrrp-parameter*]]

show vrrp vpn *vpn-id* [**interfaces** *interface-name*] [**groups** *group-number* [*vrrp-parameter*]]

Syntax Description

	None: Display information about all VRRP interfaces and groups configured on the local vEdge router, for all VPNs.
interfaces *interface-name*	Interface: Display VRRP information for a specific interface.
vpn *vpn-id*	VPN: Refresh the dynamic ARP cache entries for the specific VPN.
groups *group-number*	VRRP Group: Display information for a specific VRRP group.

groups *group-number vrrp-parameter*	VRRP Parameter: Display information about a specific VRRP parameter in a VRRP group. *vrrp-parameter* can be one of the following, which correspond to the header fields in the **show vrrp** output: • **advertisement-timer** [*number*] • **last-state-change-time** [*ccyy-mm-ddthh:mm:ss*] • **master-down-timer** [*number*] • **omp-state** [**down** | **up**] • **prefix-list-state** [**resolved** | **unresolved**] • **priority** [*number*] • **track-prefix-list** [*prefix-list-name*] • **virtual-ip** [*ip-address*] • **virtual-mac** [*mac-address*] • **vrrp-state** [**backup** | **init** | **master**]

Command History

Release	Modification
14.1	Command introduced.

Related Topics

show interface, on page 827
vrrp, on page 542

show wlan clients

Display information about the clients on the wireless WAN (on vEdge routers only).

show wlan clients [*vap-number*]

Syntax Description

vap-number	Specific VAP: Display information about the clients connected to a specific virtual access point.

Command History

Release	Modification
16.3	Command introduced.

Example

Example

Example

Display information about all clients connected to all VAPs on the WLAN:

```
vEdge# show wlan clients

      CLIENT                                                  CHANNEL    DATA       RX          ASSOC
VAP   ID      MAC                MODE       BAND    CHANNEL  BANDWIDTH  SECURITY   RATE  RSSI  TIME
-------------------------------------------------------------------------------------------------------
vap0  0       50:50:50:50:50:50  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  1       50:50:50:50:50:53  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  2       50:50:50:50:50:56  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  3       50:50:50:50:50:59  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  4       50:50:50:50:50:51  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  5       50:50:50:50:50:54  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  6       50:50:50:50:50:57  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  7       50:50:50:50:50:52  802.11ac   5 GHz   36       80         none       175   11    00:11:43
vap0  8       50:50:50:50:50:55  802.11ac   5 GHz   36       80         none       58    11    00:11:43
vap0  9       50:50:50:50:50:58  802.11ac   5 GHz   36       80         none       58    11    00:11:43
```

Related Topics

show interface, on page 827
show wlan interfaces, on page 1039
show wlan radios, on page 1040

show wlan interfaces

Display information about the virtual access point (VAP) interfaces (on vEdge routers only).

Note The **show interface** command displays no information about VAP interfaces.

show wlan interfaces [**detail**] [*vap-id*]

detail	Detailed VAP Interface Information: Display detailed information about the VAP interfaces.
vap-id	Specific VAP: Display information about a specific virtual access point.

Command History

Release	Modification
16.3	Command introduced.

Examples

Example 1

Display regular and detailed information about all the VAP interfaces on the WLAN:

```
vEdge# show wlan interfaces
                                                                MGMT                    ADMIN   OPER    NUM
VAP   SSID                BSSID             DATA SECURITY       SECURITY  BAND   MODE   STATUS  STATUS  CLIENTS
-------------------------------------------------------------------------------------------------------------
vap0  tb31_pm6_5ghz_vap0  80:b7:09:08:b7:6a  none               none      5 GHz  802.11ac  Up     Up      0
vap1  tb31_pm6_5ghz_vap1  80:b7:09:08:b7:6b  wpa/wpa2-enterprise  none      5 GHz  802.11ac  Up     Up      0
vap2  tb31_pm6_5ghz_vap2  80:b7:09:08:b7:6c  wpa/wpa2-personal    optional  5 GHz  802.11ac  Up     Up      8
vap3  tb31_pm6_5ghz_vap3  80:b7:09:08:b7:6d  wpa2-enterprise      optional  5 GHz  802.11ac  Up     Up      0

vEdge# show wlan interfaces detail
                                                                MGMT                                    BIT   TX     MAX      ADMIN   OPER    NUM
VAP   SSID                BSSID             DATA SECURITY       SECURITY  BAND   MODE      DESCRIPTION   RATE  POWER  CLIENTS  STATUS  STATUS  CLIENTS
-------------------------------------------------------------------------------------------------------------------------------------------------
vap0  tb31_pm6_5ghz_vap0  80:b7:09:08:b7:6a  none               none      5 GHz  802.11ac  -             1300  25     50       Up      Up      0
vap1  tb31_pm6_5ghz_vap1  80:b7:09:08:b7:6b  wpa/wpa2-enterprise  none      5 GHz  802.11ac  -             1300  25     20       Up      Up      0
vap2  tb31_pm6_5ghz_vap2  80:b7:09:08:b7:6c  wpa2-personal        optional  5 GHz  802.11ac  -             1300  25     24       Up      Up      8
vap3  tb31_pm6_5ghz_vap3  80:b7:09:08:b7:6d  wpa2-enterprise      optional  5 GHz  802.11ac  -             1300  25     18       Up      Up      0
```

Example 2

Display information about a specific VAP:

```
vEdge# show wlan interfaces

                                                MGMT                    ADMIN   OPER    NUM
VAP   SSID   BSSID              DATA SECURITY    SECURITY  BAND   MODE   STATUS  STATUS  CLIENTS
-----------------------------------------------------------------------------------------------
vap0  test   80:b7:09:01:39:0a  wpa2-enterprise  none      5 GHz  802.11ac  Up     Up      0
vap1  test2  80:b7:09:01:39:0b  wpa2-personal    none      5 GHz  802.11ac  Up     Up      1

vEdge# show wlan interfaces vap1

vap1 :
      IEEE 802.11ac  5 GHz SSID: test2
      Admin status: Up, Oper status: Up
      BSSID: 80:b7:09:01:39:0b
      Data security: wpa2-personal
      Management security: none
      Description:
      Bit rate: 1300 Mbps
      Transmit power: 25 dBm
      Active clients: 1, Max clients: 25
```

Related Topics

show interface, on page 827
show wlan clients, on page 1038
show wlan radios, on page 1040

show wlan radios

Display information about the WLAN radios (on vEdge routers only).

show wlan radios [*radio-name* [*parameter*]]

Syntax Description

	None: Display information about all WLAN radios.
radio-name [*parameter*]	Specific Radio: Display information about a specific radio and about a specific radio parameter. *parameter* can be one of the column heads in the output of the regular **show wlan radios** command.

Command History

Release	Modification
16.3	Command introduced.

Examples

Example 1

Display information about all WLAN radios:

```
vEdge# show wlan radios

RADIO                                                                  CHANNEL              GUARD
NAME   MODE       BAND   MAC                COUNTRY        CHANNEL  BANDWIDTH  FREQUENCY  INTERVAL  VAPS
-------------------------------------------------------------------------------------------------------
wifi0  802.11ac  5 GHz  80:b7:09:08:b7:6a  United States  36       80         5180       400       4
```

Example 2

Display information about a specific radio:

```
vEdge# show wlan radios wifi0
wifi0 :
      IEEE 802.11ac  5 GHz  80 MHz
      MAC address: 80:b7:09:08:b7:6a
      Channel: 36 Frequency: 5180 MHz
      Regulatory country: United States
      Guard interval: 400 ns
      Number of VAPs: 4

vEdge# show wlan radios wifi0 ?
Description: Display WLAN radio information
Possible completions:
  band                Radio band
  channel             Radio channel
  channel-bandwidth   Channel bandwidth, in MHz
  country             Regulatory country code
  frequency           Frequency, in MHz
  guard-interval      Guard interval, in nanoseconds
  mac                 MAC address in aa:bb:cc:dd:ee:ff format
  mode                Radio mode
  vaps                Number of virtual access point interfaces
  |                   Output modifiers

vEdge# show wlan radios wifi0 country
country "United States"
```

Related Topics

show interface, on page 827
show wlan clients, on page 1038
show wlan interfaces, on page 1039

show wlan radius

Display information about the sessions with RADIUS servers being used for WLAN authentication (on vEdge routers only).

show wlan radius [**vap** *number*] [*tag*]

Syntax Description

tag	Tag Associated with a RADIUS Server: The tag can be from 4 through 16 characters long. You configure it with the **wlan interface vap** *number* **radius-servers** *tag* command.
vap *number*	VAP Interface Virtual access point instance. Range: 0 through 3

Command History

Release	Modification
17.1	Command introduced.

Example

Example 1

Display information about the RADIUS servers that are being used for WLAN authentication:

```
vEdge# show wlan radius
vap1 :
     Primary Server, Tag: tag_dummy1, IP: 10.20.24.15, VPN: 1
     Priority: 0, Source interface:
     Authentication information
        Server Port: 1812, Active: true, Round trip time: 0
        Access requests     :    0, retransmissions    :    0, challenges          : 0
        Access accepts      :    0, rejects            :    0, malformed responses : 0
        Bad authenticators  :    0, pending requests   :    0, timeouts            : 0
        Unknown types       :    0, packets dropped    :    0
     Accounting information
        Server Port:    0, Active: false, Round trip time: 0
        Requests            :    0, retransmissions    :    0, responses           : 0
        Bad authenticators  :    0, pending requests   :    0, timeouts            : 0
        Unknown types       :    0, packets dropped    :    0, malformed responses : 0

vap1 :
     Secondary Server, Tag: tag1, IP: 10.20.24.113, VPN: 1
     Priority: 0, Source interface:
     Authentication information
        Server Port: 1812, Active: false, Round trip time: 0
        Access requests     :    0, retransmissions    :    0, challenges          : 0
        Access accepts      :    0, rejects            :    0, malformed responses : 0
        Bad authenticators  :    0, pending requests   :    0, timeouts            : 0
        Unknown types       :    0, packets dropped    :    0
     Accounting information
        Server Port:    0, Active: false, Round trip time: 0
        Requests            :    0, retransmissions    :    0, responses           : 0
```

```
Bad authenticators  :    0, pending requests   :    0, timeouts           : 0
Unknown types       :    0, packets dropped    :    0, malformed responses : 0
```

Related Topics

clear wlan radius-stats, on page 620
show interface, on page 827
show wlan clients, on page 1038
show wlan interfaces, on page 1039
show wlan radios, on page 1040

show ztp entries

Display a list of the vEdge router chassis numbers that are present in the ZTP table on the vBond orchestrator that is acting as a ZTP server.

show ztp entries

show ztp entries [*row-index*] (**chassis-number** *number* | **organization-name** *name* | **root-cert-path** *path* | **validity** (**valid** | **invalid**) | **vbond-ip** *ip-address* | **vbond-port** *number*)

Syntax Description

	None: List all entries in the ZTP table.
chassis-number *number* | **organization-name** *name* | **root-cert-path** *path* | **validity** (**valid** | **invalid**) | **vbond-ip** *ip-address* | **vbond-port** *number*	Chassis Information: List the entries corresponding to the specific chassis-related information.
row-index	Table Row: List the ZTP entry corresponding to the specified row number in the ZTP table.

Command History

Release	Modification
15.3	Command introduced.

Example

Example 1

```
vBond# request device add chassis-number 12345 serial-number 6789 validity valid vbond
10.1.14.1 org-name viptela
Adding Chassis number 12345 to the database
Successfully added the chassis-number

Creating Serial file ..
Uploading serial numbers via VPN 0
Copying ... /home/admin/vedge_serial_entries via VPN 0
Successfully loaded the vEdge serial numbers
```

```
vBond# show ztp entries
                                                                        ROOT
       CHASSIS  SERIAL                        VBOND  ORGANIZATION     CERT
INDEX  NUMBER   NUMBER  VALIDITY  VBOND IP    PORT   NAME             PATH
-------------------------------------------------------------------------------
1      12345    6789    valid     10.1.14.1   12345  viptela
```

Related Topics

request device, on page 665
request device-upload, on page 666

tcpdump

Print a description of the contents of control plane packets on a network interface that match a boolean expression. This command is the same as the UNIX **tcpdump** command.

tcpdump [**help**] [**interface** *interface-name*] [**options** " *unix-options* "] [**vpn** *vpn-id*]

Syntax Description

interface *interface-name*	Interface to Watch: Name of the interface on which to perform a TCP dump.
options " *unix-options* "	Options: One or more of the UNIX **tcpdump** command options, from among the following: [**–AbdDefhHIJKlLnNOpqStuUv**] [**–B** *size*] [**–c** *count*] [**–E** *algorithm:secret*] [**–j** *timestamp-type*] [**–M** *secret*] [**–T** *type*] [**–y** *data-link-type*] [*expression*] You must enclose *unix-options* in quotation marks. For an explanation of the options, see http://www.tcpdump.org/tcpdump_man.html.
vpn *vpn-id*	VPN to Watch: VPN identifier in which the interface is located.

For an explanation of the remaining standard UNIX options, see http://www.tcpdump.org/tcpdump_man.html.

Command History

Release	Modification
14.1	Command introduced.
16.3	Updated the command options.

Example

Example 1

```
vEdge# tcpdump vpn 1
tcpdump  in vpn 1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 65535 bytes
19:29:49.765224 IP 10.2.2.11 > 224.0.0.5: OSPFv2, Hello, length 48
19:29:49.768263 IP 10.2.2.12 > 224.0.0.5: OSPFv2, Hello, length 48
```

```
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel

vEdge# tcpdump vpn 512 interface eth0 options "-v -n tcp port 22"
tcpdump -i eth0 -s 128 -v -n tcp port 22 in VPN 512
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
14:42:45.077442 IP (tos 0x10, ttl 64, id 50767, offset 0, flags [DF], proto TCP (6), length 184)
    10.0.1.33.22 > 10.0.1.1.53312: Flags [P.], seq 3975104349:3975104481, ack 1536172049, win 218, options [nop,nop,TS val
82477842 ecr 561859671], length 132
14:42:45.077571 IP (tos 0x10, ttl 64, id 8995, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.1.1.53312 > 10.0.1.33.22: Flags [.], cksum 0x1648 (incorrect -> 0xe882), ack 132, win 372, options [nop,nop,TS val
561859682 ecr 82477842], length 0
14:42:45.121925 IP (tos 0x10, ttl 64, id 50768, offset 0, flags [DF], proto TCP (6), length 632)
...
```

test policy match control-policy

To determine the sequence number that matches a particular input variable and a policy name, use the **test policy match control-policy** command in privileged EXEC mode.

test policy match control-policy *policy name input variable*

Syntax Description

policy name	Name of a policy.

input variable	The following are the input variables used to search for policies: • **carrier**: Identifier of the carrier type. It primarily indicates whether the transport is public or private. • **color**: Identifier of the Transport Locator (TLOC) type. • **color-list**: Name of the list of colors defined in policy lists. • **community-list**: Name of the BGP community list defined in policy lists. • **domain-id**: Domain identifier, or ID related to group of devices in the same domain and associated with a TLOC. • **expanded-community-list**: Name of community list of Regex BGP community strings defined in policy lists. • **group-id**: Specific group id of devices. • **ipv4-prefix**: An IPv4 prefix. • **ipv4-prefix-list**: Name of the list of IPv4 prefixes defined in policy lists. • **ipv6-prefix**: An IPv6 prefix. • **ipv6-prefix-list**: Name of the list of IPv6 prefixes defined in policy lists. • **omp-tag**: OMP tag value associated with the TLOC route in the route table on the device. • **origin**: Source of the route, either BGP, OSPF, connected, static. • **originator**: System-ip address of the originating node. • **preference**: OMP path-selection preference. A higher value is a more preferred path. Preference value for a route or prefix in the local site. • **region**: Region ID defined in hierarchical SDWAN. • **region-list**: Name of the region list ids defined in policy lists. • **role**: Search by one of the hierarchical SDWAN roles. • **site-id**: Individual site contributor or more overlay network site identifiers. A site can have multiple nodes or TLOCs. • **site-list**: Name of the site list. Search by the name of list of site ids defined in policy lists. • **tloc**: TLOC used as next hop for the vRoute. Search by individual TLOC address. • **tloc-list**: Name of the list of tlocs defined in policy lists. • **vpn**: VPN to which the vRoute belongs. Search by individual VPN ID. • **vpn-list**: Name of the list of VPN IDs defined in policy lists.

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

For the following, use the **test policy match control-policy** command:

- When there are one or more control policies that are configured on a Cisco SD-WAN Controller.
- When a policy is configured, to check if an entity is assigned correctly under a policy's sequence.
- To troubleshoot large policies with multiple sequence numbers. This command returns the sequence number of the policy that matches input.

Examples

The following sample output shows the sequence in control_policy1 for vpn 2:

```
Device# test policy match control-policy control_policy1 vpn 2
Found: vpn 2 matches policy control_policy1 sequence 111
    sequence: 111
        match route [VPN-ID  (0x100) ]
            vpn-id: 2
        action: reject
        set: [ (0x0) ]
```

The following sample output shows the sequence of the cp1 policy for prefix 10.1.1.1/32:

```
Device# test policy match control-policy cp1 prefix 10.1.1.1/32
Found: prefix 10.1.1.1/32 matches policy cp1 sequence 111
    sequence: 111
        match route [PFX-LIST  (0x10) ]
            IPv4 prefix-list: pf1 (0x7f04292bfa00)
        action: reject
        set: [ (0x0) ]
```

The following sample output shows the sequence of the cp1 policy for ipv6-prefix a:a:a:a:a:a:a:a/128:

```
Device# test policy match control-policy cp1 ipv6-prefix a:a:a:a:a:a:a:a/128
Found: ipv6-prefix a:a:a:a:a:a:a:a/128 matches policy cp1 sequence 600
    sequence: 600
        match route [PFX-LIST  (0x10) ]
            IPv6 prefix-list: pfv61 (0x7ff7be6cb080)
        action: reject
        set: [ (0x0) ]
```

Table 27: test policy match control-policy Field Descriptions

Field	Description
FOUND	Displays a statement informing about the policy's sequence with the search entity.
SEQUENCE	Displays the policy sequence added to the policy name.
VPN-ID	Displays the VPN ID of the policy match that is found.
ACTION	Displays the configured action for the given sequence in a policy.

Field	Description
SET	Displays the configured set actions when a route or a TLOC is accepted.

timestamp

Control the inclusion of timestamp information in command output and logging files.

timestamp (**disable** | **enable**)

Syntax Description

disable	Disable Timestamp Information: Disable the inclusion of timestamp information. This is the default.
enable	Enable Timestamp Information: Enable the inclusion of timestamp information.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vEdge# timestamp enable
vEdge# timestamp disable
Tue Feb  18 19:09:37.112 UTC
vEdge# timestamp enable
vEdge#
```

Related Topics

show clock, on page 779

tools ip-route

Display IP routes and the routing cache. This command is effectively the standard Linux **ip-route** command.

tools ip-route

Syntax Description

None

Command History

Release	Modification
16.1	Command introduced.

Example

Example 1

```
vEdge# tools ip-route
default via 10.0.5.13 dev eth1  proto zebra
10.0.1.0/24 dev eth0  proto kernel  scope link  src 10.0.1.19
10.0.5.0/24 dev eth1  proto kernel  scope link  src 10.0.5.19
172.16.255.11 via 127.0.1.254 dev tun_0_0  src 172.16.255.19
172.16.255.14 via 127.0.1.253 dev tun_1_0  src 172.16.255.19
172.16.255.15 via 127.0.1.254 dev tun_0_0  src 172.16.255.19
172.16.255.16 via 127.0.1.253 dev tun_1_0  src 172.16.255.19
172.16.255.20 via 127.0.1.254 dev tun_0_0  src 172.16.255.19
172.16.255.21 via 127.0.1.254 dev tun_0_0  src 172.16.255.19
```

Related Topics

show ip routes, on page 865

tools iperf

Run tests to display various parameters related to timing, buffers, and the TCP and UDP protocols for IPv4 and IPv6 (on vEdge routers only). This command is similar to the standard **iperf** command.

tools iperf [**options** *options*] [**vpn** *vpn-id*]

tools iperf help

Syntax Description

help	Command Help: Display all the command options.
options *options*	Command Options: See the Example Output below for a list of all the **tools iperf** command options.
vpn *vpn-id*	Specific VPN: Run the command in a specific VPN. Default: VPN 0

Command History

Release	Modification
17.1	Command introduced.

Example

Example 1

```
vEdge# tools iperf helpUSAGE:
 Options:
   help                     Show usage
   vpn                      VPN or namespace
   options                  iperf options

iperf --help in VPN 0
Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Client/Server:
  -f, --format    [kmKM]   format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval  #        seconds between periodic bandwidth reports
  -l, --len       #[KM]    length of buffer to read or write (default 8 KB)
  -m, --print_mss          print TCP maximum segment size (MTU - TCP/IP header)
  -o, --output    <filename> output the report or error message to this specified file
  -p, --port      #        server port to listen on/connect to
  -u, --udp                use UDP rather than TCP
  -w, --window    #[KM]    TCP window size (socket buffer size)
  -B, --bind      <host>   bind to <host>, an interface or multicast address
  -C, --compatibility      for use with older versions does not sent extra msgs
  -M, --mss       #        set TCP maximum segment size (MTU - 40 bytes)
  -N, --nodelay            set TCP no delay, disabling Nagle's Algorithm
  -V, --IPv6Version        Set the domain to IPv6

Server specific:
  -s, --server             run in server mode
  -U, --single_udp         run in single threaded UDP mode
  -D, --daemon             run the server as a daemon

Client specific:
  -b, --bandwidth #[KM]    for UDP, bandwidth to send at in bits/sec
                           (default 1 Mbit/sec, implies -u)
  -c, --client    <host>   run in client mode, connecting to <host>
  -d, --dualtest           Do a bidirectional test simultaneously
  -n, --num       #[KM]    number of bytes to transmit (instead of -t)
  -r, --tradeoff           Do a bidirectional test individually
  -t, --time      #        time in seconds to transmit for (default 10 secs)
  -F, --fileinput <name>   input the data to be transmitted from a file
  -I, --stdin              input the data to be transmitted from stdin
  -L, --listenport #       port to receive bidirectional tests back on
  -P, --parallel  #        number of parallel client threads to run
  -T, --ttl       #        time-to-live, for multicast (default 1)
  -Z, --linux-congestion <algo>  set TCP congestion control algorithm (Linux only)

Miscellaneous:
  -x, --reportexclude [CDMSV]   exclude C(connection) D(data) M(multicast) S(settings)
V(server) reports
  -y, --reportstyle C      report as a Comma-Separated Values
  -h, --help               print this message and quit
  -v, --version            print version information and quit

[KM] Indicates options that support a K or M suffix for kilo- or mega-

The TCP window size option can be set by the environment variable
TCP_WINDOW_SIZE. Most other options can be set by an environment variable
IPERF_<long option name>, such as IPERF_BANDWIDTH.

Report bugs to <iperf-users@lists.sourceforge.net>
```

Determine the data transfer rate and bandwidth available between two vEdge routers. Set up the client side:

```
Client-vEdge# tools iperf vpn 0 options -s
option_list, -s
arg list, -s
iperf -s in VPN 0
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
```

Start the test on the server side:

```
Server-vEdge# tools iperf vpn 0 options "-c 172.16.255.13"
option_list, -c 172.16.255.13
arg list, -c 172.16.255.13
iperf -c 172.16.255.13 in VPN 0
------------------------------------------------------------
Client connecting to 172.16.255.13, TCP port 5001
TCP window size: 22.1 KByte (default)
------------------------------------------------------------
```

View the output on the server vEdge router:

```
[  4] local 10.0.12.26 port 54421 connected with 172.16.255.13 port 5001

[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec   239 MBytes   200 Mbits/sec
Server-vEdge#
```

View the output and terminate the test on the client vEdge router:

```
[  5] local 172.16.255.13 port 5001 connected with 10.0.12.26 port 54421
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-10.1 sec   239 MBytes   200 Mbits/sec

^CClient-vEdge#
```

Related Topics

ping, on page 646
tools nping, on page 1054
tools ss, on page 1062

tools minicom

Connect to the serial console through USB ports (on vEdge 1000, vEdge 2000, and vEdge 5000 routers only). This command is effectively the standard Linux **minicom** command.

tools minicom options *options*

tools minicom help

Syntax Description

help	Command Help: Display all the command options.
options *options*	Command Options: See the Linux **minicom** man page for a list of all the **tools minicom** command options.

Command History

Release	Modification
17.1	Command introduced.

Example

Example 1

Access the serial console of a remote device through the USB port on a vEdge 1000 router:

1. Connect the USB port of a vEdge 1000 or vEdge 200 router to a console port, either on the router or another device.
2. Exit from the CLI to the router's shell:

   ```
   vEdge1000# vshell
   ```

3. Determine which USB port is connected:

   ```
   # ls -lrt /dev/tty*
   ```

4. Return to the CLI:

   ```
   # exit
   ```

5. Set the baud rate on the port:

   ```
   vEdge-1000# tools minicom "-b 115200 /dev/ttyUSB-port
   ```

6. Press Ctrl-a and z, set up the port with the minicom tool, and save the configuration.

Related Topics

console-baud-rate, on page 143

tools netstat

Display information about network connections, routing tables, interface statistics, masquerading connections, and multicast memberships. This command is effectively the standard Linux **netstat** command.

tools netstat [**options** *options*] [**vpn** *vpn-id*]

tools netstat help

Syntax Description

help	Command Help: Display all the command options.
options *options*	Command Options: See the Example Output below for a list of all the **tools netstat** command options.
vpn *vpn-id*	Specific VPN: Run the command in a specific VPN. Default: VPN 0

Command History

Release	Modification
15.4.5	Command introduced.

Examples

Example 1

```
vEdge# tools netstat help
USAGE:
 Options:
   help                    Show usage
   vpn                     VPN or namspace
   options                 Netstat options

Netstat --help in VPN 0
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
        -a, --all, --listening   display all sockets (default: connected)
        -o, --timers             display timers
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB

  <Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) netrom (AMPR NET/ROM)
```

Example 2

```
vEdge# tools netstat vpn 512 options -anr
Netstat -anr in VPN 512
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.99.0       0.0.0.0         255.255.255.0   U         0 0          0 mgmt0
127.1.0.0       0.0.0.0         255.255.255.0   U         0 0          0 loop0.2
vEdge# tools netstat options -anr
```

```
Netstat -anr in VPN 0
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.100.0      0.0.0.0         255.255.255.0   U         0 0          0 ge1_7
127.1.0.0       0.0.0.0         255.255.255.0   U         0 0          0 loop0
127.1.1.0       0.0.0.0         255.255.255.0   U         0 0          0 loop1
```

Example 3

```
vEdge# tools netstat
Netstat  in VPN 0
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost.localdo:39339 localhost.localdom:2424 TIME_WAIT
tcp        0      0 localhost.localdo:39173 localhost.localdom:2424 TIME_WAIT
tcp        0      0 localhost.localdoma:iax localhost.localdo:55613 TIME_WAIT
tcp        0      0 localhost.localdo:39100 localhost.localdom:2424 TIME_WAIT
tcp        0      0 localhost.localdo:39299 localhost.localdom:2424 TIME_WAIT
tcp        0      0 localhost.localdo:51278 localhost.localdom:9300 ESTABLISHED
tcp        0      0 localhost.localdo:60695 localhost.localdom:4565 ESTABLISHED
tcp        0      0 localhost.localdo:39133 localhost.localdom:2424 TIME_WAIT
tcp        0      0 localhost.localdo:50682 localhost.localdom:9300 ESTABLISHED
```

Related Topics

ping, on page 646
tools nping, on page 1054
tools ss, on page 1062

tools nping

Generate network packets, analyze responses, and measure response times. This command is effectively the standard Linux **nping** command.

nping generates network packets of different protocols. You can use the command as a simple ping utility to detect active hosts, and you can use it to generate raw packets to perform network stack stress tests, ARP poisoning, denial-of-service attacks, route tracing, among other things.

nping echo mode displays how generated probes change in transit so that you can track differences between transmitted and received packets.



Note The nping command expects the echo response packet to be received on the same interface as the echo request transmit interface. If it is not the same, nping treats it as a failure.

From Cisco Catalyst SD-WAN Control Components Release 26.2.1, the command syntax is:

tools nping *ip-address* [**count** *probe-packets* | **data-length** *length* | **destination-port** *port* | **df** | **ipv6** | **rapid** | **source-port** *port* | **tos** *service* | **ttl** *time* | **type** *probe-type* | **verbose** | **vpn** *vpn-id*]

tools nping help

In releases earlier than Cisco Catalyst SD-WAN Control Components Release 26.2.1, the command syntax is:

tools nping (*hostname* | *ip-address*) [**options** *options*] [**vpn** *vpn-id*]

Syntax Description

Table 28: Syntax, from Cisco Catalyst SD-WAN Control Components Release 26.2.1

help	Display all the command options.
ip-address	Target destination IP address for nping packets.
count *probe-packets*	Number of probe packets. Range: 1 to 255 Default: 5
data-length *length*	Total length of the packet's IP header. Range: 0 to 4,294,967,295 (2^32-1) Default: 52, 48 for ICMP
destination-port *port*	Destination port for probe packets. Range: 0 to 65,535
df	Set the don't fragment bit. If you use this option, the df bit is set in the packet IP header. If you do not use this option, then the df bit is not set in the IP header.
ipv6	Probe IPv6 endpoint.
rapid	Enable rapid or flood ping. This is a diagnostic test that sends a large volume of Internet Control Message Protocol (ICMP) echo requests quickly, as a stress test to analyze how the infrastructure behaves under an extreme traffic load.
source-port *port*	Source port for probe packets. Range: 0 to 65,535
tos *service*	Type of service (ToS) value in decimal. Default: 192 (hex 0xC0). This corresponds to DSCP class name CS6 (class selector 6).
ttl *time*	Time-to-live (number of hops). Default: 64, 254 for ICMP
type *probe-type*	Type of probes. Values: icmp, tcp, udp Default: icmp
verbose	Enable verbose logging for the nping test.

vpn *vpn-id*	VPN ID. Range: 0 to 512 Default: 0
|	Introduces output modifiers: **begin**: Begin with the line that matches. **count**: Count the number of lines in the output. **exclude**: Exclude lines that match. **include**: Include lines that match. **linnum**: Enumerate lines in the output. **nomore**: Suppress pagination. **save**: Save output text to a file. **until**: End with the line that matches.

Table 29: Syntax, releases earlier than Cisco Catalyst SD-WAN Control Components Release 26.2.1

help	Display all the command options.
options *options*	Command Options: See the Example Output below for a list of all the **tools nping** command options.
hostname | *ip-address*	Host To Check Connectivity To: Name or IP address of host to check connectivity to.
vpn *vpn-id*	Specific VPN: Run the command in a specific VPN. Default: VPN 0

Command History

Release	Modification
16.1	Command introduced.
Cisco Catalyst SD-WAN Control Components Release 26.2.1	Removed the **options** keyword and updated the command syntax.

Examples

This example executes **nping** with:

- Destination IP: 192.168.1.41
- Source interface: eth0

For the **nping** packets in the example:

- The source-ip is the eth0 IP address.
- The packets are transmitted through eth0.
- The packet-length in the IP header is 1500.
- The df bit in the IP address is set.
- **ttl 10** indicates the time-to-live. For the packets, the maximum number of hops to transmit is 10.
- The packets are transmitted in VPN 0.
- The **rapid** option is enabled, for a rapid ping of 50 packets, and a count of 50.

```
sdwan-manager# tools nping 192.168.1.41 source eth0 source-port 12366 destination-port 12366
 data-length 1500 df ttl 10 vpn 0 rapid count 50
Running vping -f -s 192.168.1.1 -p 12366 -o 12366 -M want -T 10 -l 1500 -t icmp -c 50 -N
192.168.1.41

PROBE 192.168.1.41:12366 in VPN 0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Raw packets sent: 50 (76400B) | Rcvd: 50 (76400B) | Lost: 0 (0%)
Nping done: 1 IP address pinged
```

This example executes **nping** with:

- Destination IP: 192.168.1.41
- Source interface: eth0

For the **nping** packets in the example:

- The source IP is the interface eth0 IP address.
- The packets are transmitted through eth0.
- The source port and destination port are set.
- The packet-length in the IP header is 1500.
- The df bit in the IP address is set.
- **ttl 10** indicates the time-to-live. For the packets, the maximum number of hops to transmit is 10.
- The packets are transmitted in VPN 0.
- The **rapid** option is enabled, for a rapid ping of 5 packets.
- The **verbose** option is enabled, to provide detailed output for each packet sent and received.

```
sdwan-manager# tools nping 192.168.1.41 source eth0 source-port 12366 destination-port 12366
 data-length 1500 df ttl 10 vpn 0 rapid verbose
Running vping -f -s 192.168.1.1 -p 12366 -o 12366 -M want -T 10 -dd -l 1500 -t icmp -c 5
-N 192.168.1.41
Starting to monitor 0/192.168.1.41/12366 via none
Binding sockfd: 8 to 192.168.1.1:12366
Successfully created monitor for 0/192.168.1.41/12366 via none
Sending ICMP echo request to 192.168.1.41
```

```
Received ICMP echo response from 192.168.1.41
Monitor attached to 0/192.168.1.41/12366 via none is UP
Monitor attached to 192.168.1.41 is UP

PROBE 192.168.1.41:12366 in VPN 0
!
Sending ICMP echo request to 192.168.1.41
Received ICMP echo response from 192.168.1.41
!
Sending ICMP echo request to 192.168.1.41
Received ICMP echo response from 192.168.1.41
!
Sending ICMP echo request to 192.168.1.41
Received ICMP echo response from 192.168.1.41
!
Sending ICMP echo request to 192.168.1.41
Received ICMP echo response from 192.168.1.41
!

Raw packets sent: 5 (7640B) | Rcvd: 5 (7640B) | Lost: 0 (0%)
Nping done: 1 IP address pinged

 Monitor: 0/192.168.1.41/12366 via none
   Monitor state     : UP (flapped 1 times)
   Ref count         : 1
   Monitor type      : ping
   Probe source IP   : 192.168.1.1 / ::
   DNS source IP     : :: / ::
   Nameserver IP     : ::
   Src Port Base     : 12366
   Num of probes     : 1
   Max Re-transmit   : 0
   First Probe       : 100 msecs
   Probe interval    : 10 msecs
   Probe timeout     : 10 msecs
   DNS TTL           : 0 secs
   DNS query/ok/fail : 0/0/0

   Peer: 192.168.1.41 (UP - flapped 1 times, nretries 0)
     Total requests  : 5           Total responses : 5
     Total Tx errors : 0           Total Rx errors : 0
     Total Tx skipped: 0           Total Rx ignored: 0
     Total timeout   : 0           Connect errors  : 0
     RTT min/avg/max : 0.45/0.48/0.52 ms
     Conn min/avg/max: 0.00/0.00/0.00 ms
```

This example executes **nping** with:

- Destination IP: 192.168.1.41
- Source IP: 192.168.1.3
- Type: UDP
- Destination port: 12346

For the **nping** UDP packets in the example:

- The TOS value in decimal is 192, which is DSCP cs6.

```
sdwan-manager# tools nping 192.168.1.42 source 192.168.1.3 type udp tos 192 destination-port
 12346
Running vping -s 192.168.1.3 -t udp -o 12346 -Q 192 -c 5 -N 192.168.1.42

PROBE 192.168.1.42:12346 in VPN 0
probe=1 rtt: 0.00/0.00/0.00 msec, loss: 100%
probe=2 rtt: 0.00/0.00/0.00 msec, loss: 100%
probe=3 rtt: 0.00/0.00/0.00 msec, loss: 100%
probe=4 rtt: 0.00/0.00/0.00 msec, loss: 100%
probe=5 rtt: 0.00/0.00/0.00 msec, loss: 100%

Max rtt: 0.000ms | Min rtt: 0.000ms | Avg rtt: 0.000ms
Raw packets sent: 5 (120B) | Rcvd: 0 (0B) | Lost: 5 (100%)
Nping done: 1 IP address pinged
All probes failed
```

This example executes **nping** with:

- Destination IP: 10.127.198.9
- Source interface: eth1

For the **nping** packets in the example:

- The source IP is the interface eth1 IP address.
- The packets are transmitted through eth1.
- The packets are transmitted in VPN 512.
- The number of packets is 10.
- The TOS value in decimal is 160, which is DSCP cs5.

```
sdwan-manager# tools nping 10.127.198.9 source eth1 vpn 512 count 10 tos 160
Running vping -v 512 -s 10.127.198.10 -Q 160 -t icmp -c 10 -N 10.127.198.9

PROBE 10.127.198.9:0 in VPN 512
probe=1 rtt: 0.36/0.36/0.36 msec, loss: 0%
probe=2 rtt: 0.43/0.43/0.43 msec, loss: 0%
probe=3 rtt: 0.32/0.32/0.32 msec, loss: 0%
probe=4 rtt: 0.35/0.35/0.35 msec, loss: 0%
probe=5 rtt: 0.45/0.45/0.45 msec, loss: 0%
probe=6 rtt: 0.46/0.46/0.46 msec, loss: 0%
probe=7 rtt: 0.38/0.38/0.38 msec, loss: 0%
probe=8 rtt: 0.36/0.36/0.36 msec, loss: 0%
probe=9 rtt: 0.36/0.36/0.36 msec, loss: 0%
probe=10 rtt: 0.43/0.43/0.43 msec, loss: 0%

Max rtt: 0.459ms | Min rtt: 0.320ms | Avg rtt: 0.391ms
Raw packets sent: 10 (280B) | Rcvd: 10 (280B) | Lost: 0 (0%)
Nping done: 1 IP address pinged
```

Releases earlier than Cisco Catalyst SD-WAN Control Components Release 26.2.1

This example displays help for **nping**.

```
vEdge# tools nping help
```

```
USAGE:
 Options:
   help                     Show usage
   vpn                      VPN or namspace
   options                  Nping options

Nping in VPN 0
Nping 0.6.47 ( http://nmap.org/nping )
Usage: nping [Probe mode] [Options] {target specification}

TARGET SPECIFICATION:
  Targets may be specified as hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.*.1-24
PROBE MODES:
  --tcp-connect                    : Unprivileged TCP connect probe mode.
  --tcp                            : TCP probe mode.
  --udp                            : UDP probe mode.
  --icmp                           : ICMP probe mode.
  --arp                            : ARP/RARP probe mode.
  --tr, --traceroute               : Traceroute mode (can only be used with
                                     TCP/UDP/ICMP modes).
TCP CONNECT MODE:
   -p, --dest-port <port spec>     : Set destination port(s).
   -g, --source-port <portnumber>  : Try to use a custom source port.
TCP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>     : Set destination port(s).
   --seq <seqnumber>               : Set sequence number.
   --flags <flag list>             : Set TCP flags (ACK,PSH,RST,SYN,FIN...)
   --ack <acknumber>               : Set ACK number.
   --win <size>                    : Set window size.
   --badsum                        : Use a random invalid checksum.
UDP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>     : Set destination port(s).
   --badsum                        : Use a random invalid checksum.
ICMP PROBE MODE:
  --icmp-type <type>               : ICMP type.
  --icmp-code <code>               : ICMP code.
  --icmp-id <id>                   : Set identifier.
  --icmp-seq <n>                   : Set sequence number.
  --icmp-redirect-addr <addr>      : Set redirect address.
  --icmp-param-pointer <pnt>       : Set parameter problem pointer.
  --icmp-advert-lifetime <time>    : Set router advertisement lifetime.
  --icmp-advert-entry <IP,pref>    : Add router advertisement entry.
  --icmp-orig-time  <timestamp>    : Set originate timestamp.
  --icmp-recv-time  <timestamp>    : Set receive timestamp.
  --icmp-trans-time <timestamp>    : Set transmit timestamp.
ARP/RARP PROBE MODE:
  --arp-type <type>                : Type: ARP, ARP-reply, RARP, RARP-reply.
  --arp-sender-mac <mac>           : Set sender MAC address.
  --arp-sender-ip  <addr>          : Set sender IP address.
  --arp-target-mac <mac>           : Set target MAC address.
  --arp-target-ip  <addr>          : Set target IP address.
IPv4 OPTIONS:
  -S, --source-ip                  : Set source IP address.
  --dest-ip <addr>                 : Set destination IP address (used as an
                                     alternative to {target specification} ).
  --tos <tos>                      : Set type of service field (8bits).
  --id  <id>                       : Set identification field (16 bits).
  --df                             : Set Don't Fragment flag.
  --mf                             : Set More Fragments flag.
  --ttl <hops>                     : Set time to live [0-255].
  --badsum-ip                      : Use a random invalid checksum.
```

```
  --ip-options <S|R [route]|L [route]|T|U ...> : Set IP options
  --ip-options <hex string>                    : Set IP options
  --mtu <size>                       : Set MTU. Packets get fragmented if MTU is
                                       small enough.
IPv6 OPTIONS:
  -6, --IPv6                         : Use IP version 6.
  --dest-ip                          : Set destination IP address (used as an
                                       alternative to {target specification}).
  --hop-limit                        : Set hop limit (same as IPv4 TTL).
  --traffic-class <class> :          : Set traffic class.
  --flow <label>                     : Set flow label.
ETHERNET OPTIONS:
  --dest-mac <mac>                   : Set destination mac address. (Disables
                                       ARP resolution)
  --source-mac <mac>                 : Set source MAC address.
  --ether-type <type>                : Set EtherType value.
PAYLOAD OPTIONS:
  --data <hex string>                : Include a custom payload.
  --data-string <text>               : Include a custom ASCII text.
  --data-length <len>                : Include len random bytes as payload.
ECHO CLIENT/SERVER:
  --echo-client <passphrase>         : Run Nping in client mode.
  --echo-server <passphrase>         : Run Nping in server mode.
  --echo-port <port>                 : Use custom <port> to listen or connect.
  --no-crypto                        : Disable encryption and authentication.
  --once                             : Stop the server after one connection.
  --safe-payloads                    : Erase application data in echoed packets.
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m, 0.25h).
  --delay <time>                     : Adjust delay between probes.
  --rate  <rate>                     : Send num packets per second.
MISC:
  -h, --help                         : Display help information.
  -V, --version                      : Display current version number.
  -c, --count <n>                    : Stop after <n> rounds.
  -e, --interface <name>             : Use supplied network interface.
  -H, --hide-sent                    : Do not display sent packets.
  -N, --no-capture                   : Do not try to capture replies.
  --privileged                       : Assume user is fully privileged.
  --unprivileged                     : Assume user lacks raw socket privileges.
  --send-eth                         : Send packets at the raw Ethernet layer.
  --send-ip                          : Send packets using raw IP sockets.
  --bpf-filter <filter spec>         : Specify custom BPF filter.
OUTPUT:
  -v                                 : Increment verbosity level by one.
  -v[level]                          : Set verbosity level. E.g: -v4
  -d                                 : Increment debugging level by one.
  -d[level]                          : Set debugging level. E.g: -d3
  -q                                 : Decrease verbosity level by one.
  -q[N]                              : Decrease verbosity level N times
  --quiet                            : Set verbosity and debug level to minimum.
  --debug                            : Set verbosity and debug to the max level.
EXAMPLES:
  nping scanme.nmap.org
  nping --tcp -p 80 --flags rst --ttl 2 192.168.1.1
  nping --icmp --icmp-type time --delay 500ms 192.168.254.254
  nping --echo-server "public" -e wlan0 -vvv
  nping --echo-client "public" echo.nmap.org --tcp -p1-1024 --flags ack

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

vEdge# tools nping 10.1.15.15
Nping in VPN 0
```

```
Starting Nping 0.6.47 ( http://nmap.org/nping ) at 2016-04-02 19:41 PDT
SENT (0.0113s) ICMP [10.0.12.22 > 10.1.15.15 Echo request (type=8/code=0) id=62519 seq=1]
IP [ttl=64 id=9510 iplen=28 ]
RCVD (0.0120s) ICMP [10.1.15.15 > 10.0.12.22 Echo reply (type=0/code=0) id=62519 seq=1] IP
 [ttl=63 id=37514 iplen=28 ]
SENT (1.0114s) ICMP [10.0.12.22 > 10.1.15.15 Echo request (type=8/code=0) id=62519 seq=2]
IP [ttl=64 id=9510 iplen=28 ]
RCVD (1.0123s) ICMP [10.1.15.15 > 10.0.12.22 Echo reply (type=0/code=0) id=62519 seq=2] IP
 [ttl=63 id=38306 iplen=28 ]
vEdge#
```

Related Topics

ping, on page 646
tools netstat, on page 1052
traceroute, on page 1066

tools ss

Display socket statistics for a Cisco vEdge device. This command is effectively the standard Linux **ss** command. The output of the **tools ss** command is similar to the output of the **tools netstat** command, but more state and TCP information is displayed.

tools ss [**options** *options*] [**vpn** *vpn-id*]

tools ss help

Syntax Description

help	Command Help: Display all the command options.
options *options*	Command Options: See the Example Output below for a list of all the **tools netstat** command options.
vpn *vpn-id*	Specific VPN: Run the command in a specific VPN. Default: VPN 0

Command History

Release	Modification
16.2	Command introduced.

Examples

Example 1

```
vEdge# tools ss help
USAGE:
 Options:
   help                    Show usage
   vpn                     VPN or namespace
```

```
   options                 ss options

Netstat --help in VPN 0
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
        -a, --all, --listening   display all sockets (default: connected)
        -o, --timers             display timers
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB

  <Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) netrom (AMPR NET/ROM)
```

Example 2

```
vEdge# tools ss vpn 512
ss  in VPN 512
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
u_dgr  ESTAB      0      0                    * 25172                 * 0
u_dgr  ESTAB      0      0                    * 33267                 * 0
u_dgr  ESTAB      0      0                    * 38346                 * 0
u_dgr  ESTAB      0      0                    * 44878                 * 0
u_dgr  ESTAB      0      0                    * 45056                 * 0
u_dgr  ESTAB      0      0                    * 443913                * 0
u_dgr  ESTAB      0      0                    * 443914                * 0
u_dgr  ESTAB      0      0                    * 444218                * 0
u_str  ESTAB      0      0                    * 25494                 * 0
u_str  ESTAB      0      0      /var/run/quagga/zebra_protobuf_monitor.api.512 25495                 * 0

u_str  ESTAB      0      0                    * 25831                 * 0
u_str  ESTAB      0      0      /var/run/quagga/zebra_protobuf_notify.api.512 26426                * 0
u_str  ESTAB      0      0                    * 27306                 * 0
u_str  ESTAB      0      0      /var/run/.ftmd.512 27310                 * 0
u_str  ESTAB      0      0                    * 33268                 * 0
u_str  ESTAB      0      0                    * 33269                 * 0
u_str  ESTAB      0      0                    * 38347                 * 0
u_str  ESTAB      0      0                    * 38348                 * 0
u_str  ESTAB      0      0                    * 44879                 * 0
u_str  ESTAB      0      0                    * 44880                 * 0
u_str  ESTAB      0      0                    * 45057                 * 0
```

```
u_str  ESTAB      0      0                    * 45058                * 0
u_str  ESTAB      0      0                    * 443915               * 0
u_str  ESTAB      0      0                    * 443916               * 0
u_str  ESTAB      0      0                    * 443917               * 0
u_str  ESTAB      0      0                    * 443918               * 0
u_str  ESTAB      0      0                    * 444219               * 0
u_str  ESTAB      0      0                    * 444220               * 0
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:40694
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:53044
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:40287
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:39953
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:53051
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:53042
tcp    ESTAB      0      0          10.0.99.15:ssh          10.0.99.1:40707
```

Related Topics

tools netstat, on page 1052

tools stun-client

Discover the local device's external IP address when that device is located behind a NAT device. This command obtains a port mapping for the device and optionally discovers properties about the Network Address Translator (NAT) between the local device and a server. This command is similar to a standard Linux **stun** , **stunc** , and **stun-client** commands.

Device discovery is done using the Session Traversal Utilities for NAT (STUN) protocol, which is defined in RFC 5389 .

tools stun-client [**options** *options*] **server** (*domain-name* | *ip-address*) [**port** *port-number*] [**vpn** *vpn-id*]

tools stun-client help

Syntax Description

help	Command Help: Display all the command options.
options *options*	Command Options: See the Example Output below for a list of all the **tools stun-client** command options.
server (*domain-name* | *ip-address*) [**port** *port-number*]	Remote STUN Server: Remote server to attach to, and port to use to reach the server. The default port number for UDP and TCP is 3478.
vpn *vpn-id*	Specific VPN: Run the command in a specific VPN. Default: VPN 0

Command History

Release	Modification
16.2	Command introduced.

Examples

Example 1

Perform a generic basic binding STUN test against Googles STUN server:

```
vEdge# tools stun-client vpn 0 options "--mode basic stun.l.google.com 19302"
stunclient --mode basic stun.l.google.com 19302 in VPN 0
Binding test: success
Local address: 50.247.64.109:56485
Mapped address: 50.247.64.109:56485
```

Example 2

Perform a full test to detect NAT type against Google's STUN server:

```
vEdge# tools stun-client vpn 0 options "--mode full stun.l.google.com 19302"
stunclient --mode full stun.l.google.com 19302 in VPN 0
Binding test: success
Local address: 50.247.64.109:33760
Mapped address: 50.247.64.109:33760
Behavior test: success
Nat behavior: Direct Mapping
Filtering test: success
Nat filtering: Endpoint Independent Filtering
```

Example 3

Perform a full NAT detection test using UDP source port 12346 (the default DTLS/IPsec port) against Google's STUN server:

```
vEdge# tools stun-client vpn 0 options "--mode full --localport 12346 stun.l.google.com
19302"
stunclient --mode full --localport 12346 stun.l.google.com 19302 in VPN 0
Binding test: success
Local address: 50.247.64.109:12346
Mapped address: 50.247.64.109:12346
Behavior test: success
Nat behavior: Direct Mapping
Filtering test: success
Nat filtering: Endpoint Independent Filtering
```

Example 4

Display help for the **tools stun-client** command:

```
vEdge# tools stun-client help
...
The following options are supported:
    --mode MODE
    --localaddr INTERFACE
    --localport PORTNUMBER
    --family IPVERSION
    --protocol PROTO
    --verbosity LOGLEVEL
    --help

--mode (basic | full)
```

```
"basic" mode is the default and indicates that the client should perform a STUN binding
test
only. "full" mode indicates that the client should attempt to diagnose NAT behavior and
filtering methodologies if the server supports this mode. The NAT filtering test is supported
only for UDP.

--localaddr INTERFACE or IPADDRESS
Name of an interface (such as "eth0") or one of the available IP addresses assigned to a
network interface present on the host. The interface chosen is the preferred address for
sending and receiving responses with the remote server. The default is to let the system
decide
which address to send on and to listen for responses on all addresses (INADDR_ANY).

--localport PORTNUM
PORTNUM is a value between 1 to 65535. It is the UDP or TCP port that the primary and
alternate interfaces listen on as the primary port for binding requests. If not specified,
 the
system randomly chooses an available port.

--family IPVERSION
IPVERSION is either "4" or "6" to specify the usage of IPv4 or IPv6. The default value is
"4".

--protocol (udp | tcp)
"udp" is the default.

--verbosity LOGLEVEL
Set the logging verbosity level. 0 is the default, for minimal output and logging). 1 shows
slightly more, and 2 and higher show even more.

EXAMPLES

stunclient stunserver.org 3478
    Perform a simple binding test request with the server, listening at "stunserver.org".

stunclient --mode full --localport 9999 12.34.56.78
    Perform a full set of UDP NAT behavior tests from local port 9999 to the server, listening

    at IP address 12.34.56.78 (port 3478).

stunclient --protocol tcp stun.selbie.com
    Performs a simple binding test using TCP to server, listening on the default port of
3478
    at stun.selbie.com.
```

traceroute

Display the path that packets take to reach a host or IP address on the network.

traceroute interface *interface-name* [**size** *bytes*] [**options** *options*] (*hostname* | *ip-address*)

traceroute vpn *vpn-id* [**interface** *interface-name*] [**size** *bytes*] [**options "** *options* **"**] (*hostname* | *ip-address*)

Syntax Description

interface *interface-name*	Interface: Interface through which traceroute probe should send packets.

(*hostname* | *ip-address*)	Network Host: Hostname or IPv4 or IPv6 address of a system on the network.
options " *options* "	Options: One or more options for the traceroute probe. *option* can be one or more of the following. Enclose the options in quotation marks (" "). • **–d**: Set the SO_DEBUG options to socket. • **–f** *first-ttl*: Report the traceroute probe results starting with the specified hop in the path. • **–g** *gateway*: Add an IP source route gateway to the outgoing packet. • **–I** (capital letter "i"): Use ICMP echo packets instead of UDP datagrams. • **–i** (lowercase letter "i") *interface-name*: Network interface from which to obtain the source IP address for outgoing traceroute probe packets. • **–m** *maximum-ttl*: Set the maximum time-to-live value, which is the maximum number of hops. • **–n**: Print numeric IP addresses. • **–p** *port*: Base UDP port number to use in traceroute probes. The default port is 33434. • **–q** *probes*: Number of probes to send per TTL. The default is 3. • **–r**: Bypass the normal route tables, and send the traceroute probe directly to a host. • **–s** *source-ip-address*: Source IP address to use in the probe packets. • **–t** *tos*: Type-of-service value to use in the probe packets. The default is 0. • **–v**: Display output in verbose mode. • **–w** *wait-time*: Time, in seconds, to wait for a response. The default is 3 seconds. • **–z** *pause-time*: Time, in milliseconds, to pause between probes. The default is 0 milliseconds.
size *bytes*	Probe Packet Size: Size of the traceroute probe packets, in bytes. The maximum packet size is 32,768 bytes.
vpn *vpn-id*	VPN: VPN in which the network host is located.

Command History

Release	Modification
14.1	Command introduced.
14.2	Added **interface**, **options**, **size**, and **vpn** options.
16.3	Added support for IPv6 host addresses.

Usage Guidelines

When a traceroute packet inside a service VPN arrives on the WAN interface:

- The Cisco vEdge device responds with a source IP of one of the interfaces in the service VPN.

Note For Cisco vEdge devices, the **traceroute** command does not support UDP.

- The Cisco IOS XE Catalyst SD-WAN device responds with a source IP of the WAN interface where the packet is received.

In both cases, the packets are always encapsulated in IPSec.

Examples

Example 1

```
vEdge-112# traceroute vpn 1 192.168.111.30
Traceroute in vpn 1
traceroute to 192.168.111.30 (192.168.111.30), 30 hops max, 46 byte packets
1  172.23.2.2 (172.23.2.2)  0.171 ms  0.196 ms  0.126 ms
2  100.100.100.11 (100.100.100.11)  0.128 ms  0.197 ms  0.127 ms
3  100.100.100.12 (100.100.100.12)  0.165 ms  0.194 ms  0.146 ms
4  172.23.111.2 (172.23.111.2)  0.218 ms  0.227 ms  0.214 ms
5  192.168.111.30 (192.168.111.30)  1.173 ms  0.824 ms  1.239 ms
```

Example 2

```
vEdge# traceroute host 10.2.3.12 size 1000 vpn 1 options "-q1 -w1 -m5"
Traceroute -q1 -w1 -m5 10.2.3.12 in VPN 1
traceroute to 10.2.3.12 (10.2.3.12), 5 hops max, 1000 byte packets
1 10.20.24.15 (10.20.24.15) 0.254 ms
2 10.0.5.21 (10.0.5.21) 1.318 ms
3 10.2.3.12 (10.2.3.12) 1.310 ms
```

Related Topics

ping, on page 646
show interface, on page 827
show ipv6 interface, on page 879
tools nping, on page 1054

vshell

Exit from the Cisco SD-WAN CLI to the Linux shell running on the device. In the shell, the default terminal is xterm.

Use the UNIX **exit** command to return to the CLI. If the shell session is inactive, it times out after 15 minutes, and the device returns to the Cisco SD-WAN CLI.

Once you are in the shell, you can use standard Linux commands to perform standard operations, such as listing files, changing directories, and copying files off the device. To edit a file, use the **vi** editor.

vshell

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
15.4	Idle session timeout added.
15.4.3	Having xterm be default terminal added

Example

Example 1

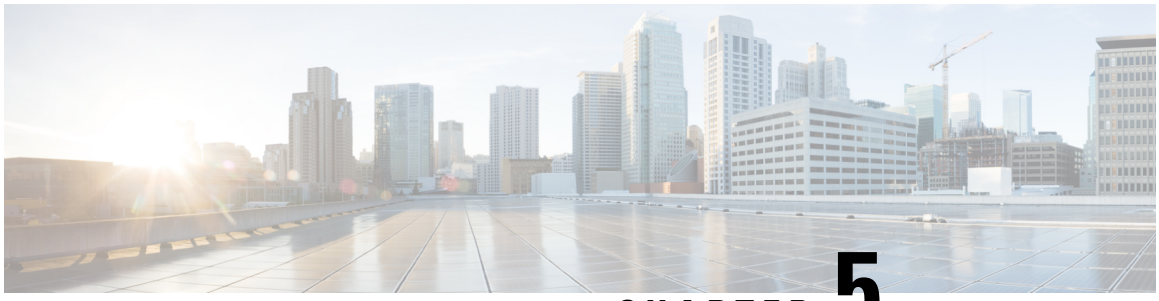
```
vEdge# show version
15.4.3
vEdge# vshell
vEdge$ echo $TERM
xterm
vEdge:~$ exit
exit
vEdge#
```

To open an SSH connection from a vManage NMS to an IOS XE router, you must specify the port number, which is 830:

```
vManage# vshell
vManage:~$ ssh 172.16.255.15 -p 830
admin@172.16.255.15's password:
```

Related Topics

exit, on page 636
quit, on page 652
request execute, on page 669



CHAPTER 5

Configuration Management Commands

Note For a list of Cisco IOS XE SD-WAN commands qualified for use in Cisco vManage CLI templates, see List of Commands Qualified in Cisco IOS XE Release 17.x. For information about specific commands, see the appropriate chapter in Cisco IOS XE SD-WAN Qualified Command Reference Guide.

- Overview of Configuration Management Commands, on page 1072
- abort, on page 1072
- clear, on page 1073
- commit, on page 1074
- describe, on page 1075
- do, on page 1076
- end, on page 1077
- exit, on page 1077
- help, on page 1078
- load, on page 1079
- no, on page 1080
- pwd, on page 1081
- revert, on page 1082
- rollback, on page 1082
- save, on page 1084
- show configuration, on page 1086
- show configuration commit, on page 1087
- show configuration diff, on page 1088
- show configuration merge, on page 1089
- show configuration rollback, on page 1090
- show configuration running, on page 1091
- show full-configuration, on page 1092
- show history, on page 1092
- show parser dump, on page 1093
- top, on page 1094
- validate, on page 1095

Overview of Configuration Management Commands

The configuration management command reference pages describe the CLI commands that you use to manage a configuration on vSmart controllers, vEdge routers, and vBond orchestrators. You know that you are in configuration mode because the CLI prompt changes to include the string **(config)**.

In the CLI, the configuration management commands are grouped together after the functional configuration commands, and they are organized alphabetically. Some of commands are organized into functional hierarchies. The top-level configuration management commands and command hierarchies are:

- abort—End the configuration session.
- clear—Remove all changes to the configuration.
- commit—Activate the configuration.
- describe—Display help about the configuration commands.
- do—Run an operational command without exiting from configuration mode.
- end—End the configuration session.
- exit—Exit from the current configuration level.
- help—Display help information about CLI commands.
- load—Load the configuration from an ASCII text file.
- no—Negate a command.
- pwd—Display the current configuration level.
- revert—Return to the running configuration.
- rollback—Return to a previously committed version of the configuration.
- save—Save the configuration to an ASCII text file.
- show—Display a configuration parameter.
- top—Return to the top level in the configuration.
- validate—Validate the configuration.

The configuration commands themselves are described under Configuration Commands.

abort

Exit configure mode immediately, without displaying a prompt warning you to save uncommitted changes.

abort

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config)# abort
vedge1#
```

Related Topics

clear, on page 1073
commit, on page 1074
rollback, on page 1082

clear

Clear all changes made to the configuration during the current session.

clear

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vvedge1(config)# clear
All configuration changes will be lost. Proceed? [yes, NO] yes
vedge1(config)#
```

Related Topics

abort, on page 1072
rollback, on page 1082

commit

Activate the commands in the configuration on the Cisco vEdge device and make it the running configuration. You issue this **commit** command from configuration mode.

commit (**abort** | **and-quit** | **check** | **confirmed** [*timeout*] [**persist**] | **no-confirm**) [**comment** *text*] [**label** *text*] [**persist-id** *id*] [**save-running** *filename*]

Syntax Description

	None: Activate the commands in the configuration and remain at the same hierarchy in configuration mode.
comment *text*	Add a text comment about the commit operation. If the text string contains spaces, enclose the entire string in quotation marks (" "). Any comments are display in the output of the **show configuration commit list** command.
label *text*	Add a text label that describes the commit operation. If the text string contains spaces, enclose the entire string in quotation marks (" "). Any labels are display in the output of the **show configuration commit list** command.
and-quit	Exit from Configuration Mode: Active the configuration and return to operational mode.
abort	Halt a Commit Operation: Halt a provisional commit operation.
confirmed [*timeout*] [**persist**]	Provisional Commit Operation: Commit the current configuration to the running configuration. If no **commit confirm** command is issued before the timeout period, specified in minutes, expires, the configuration reverts to what was active before the **commit confirmed** command was issued. The default timeout is 10 minutes. The configuration session terminates after you issue this command, because no further editing is possible. This command is available only in **configure exclusive** and **configure shared** mode when the system has been configured with a candidate configuration. If the CLI session is terminated before the **commit confirm** command is issued, the configuration reverts to the previously active configuration. If you include the **persist** option, you can terminate the CLI session before you issue the **commit confirm** command, and you can then confirm the pending commit in a later session by supplying the persist token as an argument to the **commit** command using the **persist-id** option. A **commit confirmed** command is valid only for the candidate datastore where the configuration parameter **/confdConfig/datastores/running/access** is set to **writable-through-candidate** in the confd.conf file and the configuration mode is set to either **configure exclusive** or **configure shared** mode. A candidate datastore provides a temporary work space in which a copy of the running configuration for the Cisco vEdge device is stored. You can create and modify the running configuration before committing the running configuration to the device. On Cisco vEdge devices, we have enabled writable-through-candidate in the confd file, which means that **commit confirmed** works only for **configure exclusive** or **configure shared** modes. By default, the configuration enters **configure private** mode, and therefore, your changes are written directly to the running configuration rather than to the candidate datastore. If you intend to use **commit confirmed**, use **configure exclusive** or **configure shared** modes.

persist-id *id*	Persist Token: If a prior confirming commit operation has been performed with the persist argument, include the **persist-id** option, specifying the same persist token, to modify the ongoing confirming commit process. This allows you, for example, to cancel an ongoing persist commit operation or extend the timeout.
save-running *filename*	Save the Configuration to a File: Save a text copy of the running configuration to the specified file.
check	Validate the Configuration: Validate current configuration and indicate any configuration errors.

Command History

Release	Modification
14.1	Command introduced.
15.2	"system is-vmanaged" warning added

Example

Example 1

```
vedge1(config-system)# commit and-quit
Commit complete.
vedge1#
```

Example 2

```
vm5# config exclusive
Entering configuration mode exclusive
Warning: uncommitted changes will be discarded on exit
vm5(config)# vpn 3
vm5(config-vpn-3)# commit confirmed
Warning: The configuration will be reverted if you exit the CLI without
performing the commit operation within 10 minutes.
vm5(config-vpn-3)# commit
Commit complete. Configuration is now permanent.
vm5(config-vpn-3)# exit
```

Related Topics

commit, on page 622
show configuration commit list, on page 783
validate, on page 1095

describe

Display internal information about how a configuration command is implemented.

describe *command*

Syntax Description

command	Information about a Command: Display internal information about a command's implementation.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm4(config)# describe vpn
Common
    Source           : YANG
    Module           : viptela-vpn
    Namespace        : http://viptela.com/vpn
    Path             : /vpn
    Node             : container
    Revision         : 2013-02-12
    Exported agents  : all
    Checksum         : 5b30372a4dedcad2a01633f79395720
```

Related Topics

show parser dump, on page 955

do

Run an operational command from within configuration mode.

do *command*

Syntax Description

command	Command Name: Run the specified operational-mode command.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config-vpn-0)# do show version
14.0b 20131206-2 build 52
vedge1(config)#
```

Related Topics

Overview of Operational Commands, on page 565

end

Exit configuration mode.

end [**no-confirm**]

Syntax Description

	None: If no changes have been made to the configuration, exit configuration mode immediately. If changes have been made, you are asked to save the changes before existing configuration mode.
no-confirm	Exit Immediately: Exit configuration mode immediately, without committing an changes to the configuration.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config-banner)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] no
vedge1#
```

Related Topics

abort, on page 1072
exit, on page 1077

exit

Exit from the current mode in the configuration, or exit configuration mode altogether.

exit [**configuration-mode**] [**level**] [**no-confirm**]

Syntax Description

	None: Exit from the current level in the configuration, and move up one hierarchy level.
configuration-mode	Exit Configuration Mode: If changes have been made to the configuration, you are prompted to commit them.
no-confirm	Exit Configuration Mode Immediately: Exit configuration mode immediately, without being prompted to commit any changes to the configuration.
level	Exit the Current Level: Exit from the current level in the configuration, and move up one hierarchy level. This is the default behavior if you type the **exit** command with no options.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config)# vpn 0 interface ge0/0
vedge1(config-interface-ge0/0)# exit
vedge1(config-vpn-0)#vedge1(config-banner)# exit configuration-mode
Uncommitted changes found, commit them? [yes/no/CANCEL] no
vedge1#
```

Related Topics

end, on page 1077

help

Display help information about a command.

help *command*

Syntax Description

command	Help about a Command: Display short help information about a command.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config)# help banner
Help for command: banner
    Set banners
```

Related Topics

show parser dump, on page 1093
show parser dump, on page 955

load

Load the configuration from a file.

load (**merge** | **override** | **replace**) *file-path*

Syntax Description

file-path	File Path: Path to the directory and filename of the file containing the configuration. It can be one of the following: • **ftp://** *user:password@host:port/file-path*—Path to a file on an FTP server. • **scp://** *user* **@** *host* **:** *file-path* • **/** *file-path* **/** *filename*—Path to a file on the local Cisco vEdge device.
merge *file-path*	Merge with the Existing Configuration: Merge the configuration in the specified file with the current configuration.
override *file-path*	Override the Existing Configuration: Delete the current configuration and then replace it with a new configuration, which is loaded from the specified file.
replace *file-path*	Replace the Existing Configuration: Replace the corresponding parts of the current configuration with the contents of the specified file. This option differs from the **override** option in that only the parts of the configuration contained in the specified file are replaced. The rest of the configuration is unchanged.

Note **load override** and **load merge** is not supported on Cisco IOS XE devices.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Load the configuration from a file on the router:

```
vm4(config)# load replace test-configuration-file
Loading.
1.18 KiB parsed in 0.09 sec (12.05 KiB/sec)
vm4(config)#
```

Related Topics

file list, on page 637
rollback, on page 1082
save, on page 1084

no

Delete or unset a configuration command or parameter.

no *command*

Syntax Description

command	Delete or Unset a Command: Delete or unset the specified command from the configuration.

Command History

Release	Modification
14.1	Command introduced.

Examples

Example 1

Delete the login banner from the configuration:

```
vm4(config)# banner login "Welcome to vEdge4"
vm4(config-banner)# commit and-quit
Commit complete.
vm4# show running-config banner
banner
```

```
 login "Welcome to vEdge4"
!
vm4# config
Entering configuration mode terminal
vm4(config)# no banner login
vm4(config)# commit and-quit
Commit complete.
vm4# show running-config banner
% No entries found.
```

Example 2

Enable the operation of an interface:

```
vm4# show running-config vpn 0 interface ge0/7vpn 0
 interface ge0/7
  ip address 10.0.100.14/24
  no shutdown
 !
!
```

Related Topics

Overview of Configuration Commands, on page 23

pwd

Display the current path in the configuration hierarchy.

pwd

Syntax Description

None

Command History

Release	Modification
14.1	Commad introduced.

Example

Example 1

```
vedge1(config)# pwd
At top level
vedge1(config)# vpn 0 interface ge0/0
vedge1(config-interface-ge0/0)# pwd
Current submode path:
  vpn vpn-instance 0 \ interface ge0/0
vedge1(config-interface-ge0/0)#
```

Related Topics

exit, on page 1077
top, on page 1094

revert

Copy the running configuration into the current candidate configuration.

revert [**no-confirm**]

Syntax Description

	None: Copy the running configuration into the current candidate configuration, thus losing all configuration changes that have been made during this session. You are prompted to confirm this action.
no-confirm	Return to the Running Configuration Immediately: Immediately copy the running configuration into the current candidate configuration, thus losing all configuration changes that have been made during this session. You are not prompted to confirm this action.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config)# revert
% No configuration changes.
vedge1(config)# no banner
vedge1(config)# revert
All configuration changes will be lost. Proceed? [yes, NO] no
Aborted: by user
vedge1(config)#
```

Related Topics

load, on page 1079
rollback, on page 1082

rollback

Return to a previously committed configuration.

rollback (**configuration** [*number*] | **selective** *number*)

Syntax Description

rollback configuration	Return to the Previously Committed Configuration: Return to the most recently committed configuration. You are not prompted to confirm this action, and you lose all configuration changes that have been made during this session.
rollback configuration [*number*]	Return to an Earlier Committed Configuration: Return to the configuration changes made in all commit operations up to a particular rollback number. If you omit the number, you return to the previously committed configuration, which is rollback 0. Use the **rollback configuration ?** to display the configuration numbers and the dates and times that the configurations were committed. For example, the command **rollback configuration 1** returns to the configuration changes made in rollback versions 0 and 1.
rollbackselective	Return to a Particular Earlier Committed Configuration: Return to the configuration changes made in a specific commit operation. Use the **rollback configuration ?** to display the configuration numbers and the dates and times that the configurations were committed. For example, the command **rollback configuration 1** returns to the configuration changes made in rollback version 1.

Command History

Release	Modification
14.1	Command introduced.

Examples

Example 1

Roll back to the last two sets of configuration changes:

```
vsmart(config)# do show running-config policy
% No entries found.
vsmart(config)# policy lists site-list s site-id 10
vsmart(config-site-list-s)# commit
Commit complete.
config# do show running-config policy
policy
lists
  site-list s
   site-id 10
  !
!
!vsmart(config-lists)# vpn-list v vpn 1
vsmart(config-vpn-list-v)# commit
Commit complete.
vsmart(config-vpn-list-v)#
vsmart(config)# do show running-config policy
policy
lists
  vpn-list v
   vpn 1
  !
  site-list s
```

```
   site-id 10
  !
 !
!
vsmart(config)# rollback configuration
Possible completions:
  0      2013-12-12 12:01:05 by admin via cli
  1      2013-12-12 12:00:50 by admin via cli
  <cr>   latest
vsmart(config)# rollback configuration 1       ========> rollback 0 and 1 are applied
vsmart(config)# show configuration
policy
lists
  no vpn-list v
  no site-list s
 !
!
```

Example 2

Roll back to only the second previous configuration:

```
vsmart(config)# clear
All configuration changes will be lost. Proceed? [yes, NO] yes
vsmart(config)# show configuration
% No configuration changes found.
vsmart(config)# rollback selective
Possible completions:
0 2013-12-12 12:01:05 by admin via cli
1 2013-12-12 12:00:50 by admin via cli
<cr> latest
vsmart(config)# rollback selective 1 ==========> Only rollback 1 applied
vsmart(config)# top show configuration
policy
lists
   no site-list s
!
!
```

Related Topics

load, on page 1079
revert, on page 1082

save

Save the entire current configuration or parts of it to a file.

save *file-path*[*hierarchy*] [**overwrite**]

Syntax Description

file-path	File Path: Path to the directory and filename of the file containing the configuration. It can be one of the following: • **ftp:** *file-path*—Path to a file on an FTP server. • **scp:** *user* **@** *host* **:** *file-path*. • **/** *file-path* **/** *filename*—Path to a file on the local Cisco vEdge device.
overwrite	Overwrite an Existing File: Overwrite the contents of an existing file.
save *filename*	Save the Entire Configuration: Save the entire configuration to a file.
save *filename hierarchy*	Save a Portion of the Configuration: Save the specified configuration hierarchy to a file.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Save the configuration to a file:

```
vedge1(config)# save config-system system
Saving system
vedge1(config)# do file show config-system
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
  !
 !
!
```

Related Topics

file list, on page 637
file show, on page 637
load, on page 1079

show configuration

Display changes that have been made to the configuration during the current editing session. The changes are displayed is the same format as the configuration is displayed when you issue a **show full-configuration** configuration command or a **show running-config** operational command.

show configuration [*hierarchy*]

Syntax Description

	None: Show all configuration changes.
hierarchy	Specific Hierarchy: Show all the changes in a specific configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display all configuration changes:

```
vm4(config)# banner motd "Welcome to vEdge4"
vm4(config-banner)# top
vm4(config)# show configuration
banner
motd "Welcome to vEdge4"
!
```

Related Topics

show configuration commit, on page 1087
show configuration diff, on page 1088
show configuration merge, on page 1089
show configuration running, on page 1091
show full-configuration, on page 1092

show configuration commit

Display the configuration changes that took effect as the result of a previous commit operation.

show configuration commit changes (*rollback-number* | **latest**)

show configuration commit changes diff (*rollback-number* | **latest**)

show configuration commit list [*number*]

Syntax Description

(*rollback-number* | **latest**)	Configuration Changes Since a Specific Commit: List the configuration changes since a specific commit operation. *rollback-number* is the commit identifier. **latest** is the last commit operation. The changes are displayed is the same format as the configuration is displayed when you issue a **show full-configuration** configuration command or a **show running-config** operational command.
diff (*rollback-number* | **latest**)	Configuration Changes Since a Specific Commit, in Diff Format: List the configuration changes since a specific commit operation. *rollback-number* is the commit identifier. **latest** is the last commit operation. The changes are displayed is a UNIX diff-style format.
list [*number*]	Show the Configuration Commit History: List the commit identifiers and information about the previous commit operations.

Command History

Release	Modification
14.1	Command introduced.

Examples

Example 1

Display configuration changes:

```
vm4(config)# show configuration commit changes diff 1
+banner
+ login "Welcome to vEdge4"
+!
```

```
vm4(config)# show configuration commit changes 1
banner
 login "Welcome to vEdge4"
!
```

Example 2

List an abridged commit history:

```
vm4(config)# show configuration commit list 10
2014-03-12 01:00:32
SNo. ID       User       Client      Time Stamp          Label       Comment
0    10042    admin      cli         2014-03-12 00:14:04
1    10041    admin      cli         2014-03-12 00:13:48
2    10040    admin      cli         2014-03-11 18:19:38
3    10039    admin      cli         2014-03-11 18:19:13
4    10038    admin      cli         2014-03-11 14:00:31
5    10037    admin      cli         2014-03-11 13:59:49
6    10036    admin      cli         2014-03-11 13:59:38
7    10035    admin      cli         2014-03-11 13:59:37
8    10034    admin      cli         2014-03-11 13:59:37
9    10033    admin      cli         2014-03-11 13:59:36
```

Related Topics

show configuration, on page 1086
show configuration diff, on page 1088
show configuration merge, on page 1089
show configuration running, on page 1091
show full-configuration, on page 1092

show configuration diff

Display changes that have been made to the configuration during the current editing session. The changes are displayed is UNIX-style diff format.

show configuration diff [*hierarchy*]

Syntax Description

	None: Show all configuration changes.
hierarchy	Specific Hierarchy: Show all the changes in a specific configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display all configuration changes:

```
vm4(config)# show configuration diff
 banner
+ login "Welcome to vEdge4"
 !
```

Related Topics

show configuration, on page 1086
show configuration commit, on page 1087
show configuration rollback, on page 1090
show configuration running, on page 1091
show full-configuration, on page 1092

show configuration merge

Display a combination of the running and target configurations.

show configuration merge [*hierarchy*]

Syntax Description

	None: Show a combination of the running and target configurations for the entire configuration.
hierarchy	Specific Hierarchy: Show a combination of the running and target configurations for the specific configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display the merged configuration for a specific command hierarchy:

```
vm4(config)# show configuration merge banner
banner
 login "Welcome to vEdge4"
 motd  "Welcome to vEdge4"
!
```

Related Topics

show configuration, on page 1086
show configuration commit, on page 1087
show configuration diff, on page 1088
show configuration rollback, on page 1090
show configuration running, on page 1091
show full-configuration, on page 1092

show configuration rollback

Compare the current target configuration to the configuration in a previously committed version, and display the differences.

show configuration rollback changes (*rollback-number* | **latest**)

Syntax Description

(*rollback-number* | **latest**)	Specific Previous Commit: List the configuration differences since a specific commit operation. *rollback-number* is the commit identifier. **latest** is the last commit operation.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display the configuration differences from previously committed configurations:

```
vm4(config)# show configuration rollback changes 1
banner
 login "Welcome to vEdge4"
 no motd "Welcome to vEdge4"
!
vm4(config)# show configuration rollback changes 2
no banner
vm4(config)# show configuration rollback changes 3
no banner
vpn 0
 interface ge0/4
  tunnel-interface
   clear-dont-fragment
  !
 !
!
```

Related Topics

rollback, on page 1082
show configuration, on page 1086
show configuration commit, on page 1087
show configuration diff, on page 1088
show configuration running, on page 1091

show configuration running

Display the running configuration.

show configuration running [*hierarchy*]

Syntax Description

	None: Show the entire configuration.
hierarchy	Specific Hierarchy: Show the running configuration in a specific configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display the running configuration in a hierarchy:

```
vm4(config)# show configuration running banner
banner
 motd "Welcome to vEdge4"
!
```

Related Topics

show configuration, on page 1086
show configuration commit, on page 1087
show configuration diff, on page 1088
show configuration merge, on page 1089
show configuration rollback, on page 1090
show full-configuration, on page 1092

show full-configuration

Display the current configuration, which is a combination of the running and candidate configurations.

show full-configuration [*hierarchy*]

Syntax Description

	None: Show the entire configuration.
hierarchy	Specific Hierarchy: Show the configuration in a specific configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display the running and candidate configuration in a hierarchy:

```
vm4(config)# show full-configuration banner
banner
 login "Welcome to vEdge4"
 motd  "Welcome to vEdge4"
!
```

Related Topics

show configuration, on page 1086
show configuration commit, on page 1087
show configuration diff, on page 1088
show configuration merge, on page 1089
show configuration running, on page 1091

show history

Display the history of the commands issued in the current configuration session.

show history [*number*]

Syntax Description

	None: Display all commands that have been issued in the current configuration session.

number	Specific Number of Commands: Display the specified number of most recent commands that have been issued in the current configuration session.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display a limited number of configuration session commands:

```
vm4(config)# show history 12
02:07:53 -- show configuration merge banner
02:09:45 -- show configuration rollback changes 14
02:10:11 -- show full-configuration
02:14:20 -- show full-configuration banner
02:15:52 -- show configuration running
02:18:18 -- show configuration running banner
02:22:06 -- show configuration rollback changes 1
02:22:13 -- show configuration rollback changes 2
02:22:16 -- show configuration rollback changes 3
02:34:36 -- show configuration this omp
02:34:43 -- show configuration this banner
02:35:32 -- show history 12
vm4(config)#
```

Related Topics

show history, on page 821

show parser dump

Display the syntax of the configuration commands.

show parser dump [*hierarchy*]

Syntax Description

	None: Display the syntax of all configuration commands.
hierarchy	Specific Hierarchy: Display the syntax of the configuration commands in a specified hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

Display a limited number of configuration session commands:

```
vm4(config)# show parser dump banner
banner
banner login <string,-min:-1-chars,-max:-128-chars>
banner login <string,-min:-1-chars,-max:-128-chars> motd
<string,-min:-1-chars,-max:-128-chars>
banner motd <string,-min:-1-chars,-max:-128-chars>

vm4(config)# show parser dump vpn router | include area
vpn router router ospf area <a-num:unsignedInt>
vpn router router ospf area <a-num:unsignedInt> nssa
vpn router router ospf area <a-num:unsignedInt> nssa no-summary
vpn router router ospf area <a-num:unsignedInt> nssa translate [candidate/never/always]
vpn router router ospf area <a-num:unsignedInt> nssa translate [candidate/never/always]
no-summary
vpn router router ospf area <a-num:unsignedInt> range <IPv4-address/prefix-length>
vpn router router ospf area <a-num:unsignedInt> range <IPv4-address/prefix-length> cost
<0..16777215>
vpn router router ospf area <a-num:unsignedInt> range <IPv4-address/prefix-length> cost
<0..16777215> no-advertise
vpn router router ospf area <a-num:unsignedInt> range <IPv4-address/prefix-length>
no-advertise
vpn router router ospf area <a-num:unsignedInt> stub
vpn router router ospf area <a-num:unsignedInt> stub no-summary
vpn router router ospf distance external <1..255> inter-area <1..255>
vpn router router ospf distance external <1..255> inter-area <1..255> intra-area <1..255>
vpn router router ospf distance inter-area <1..255>
vpn router router ospf distance intra-area <1..255>
```

Related Topics

show parser dump, on page 955

top

Move to the top level of the configuration hierarchy.

top [*configuration-command*]

Syntax Description

	None: Move to the top level of the configuration hierarchy.
configuration-command	Execute a Configuration Command: Execute a configuration command from the top level of the configuration hierarchy without actually moving to the top level of the configuration hierarchy.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1(config-interface-ge0/0)# top
vedge1(config)# system aaa usergroup operator
vedge1(config-usergroup-operator)# top banner motd "Welcome"
vedge1(config-usergroup-operator)# top show configuration
banner
 motd Welcome
!
vedge1(config-usergroup-operator)#
```

Related Topics

exit, on page 1077

validate

Verify that the candidate configuration contains no errors.

validate

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.
15.2	"system is-vmanaged" warning added

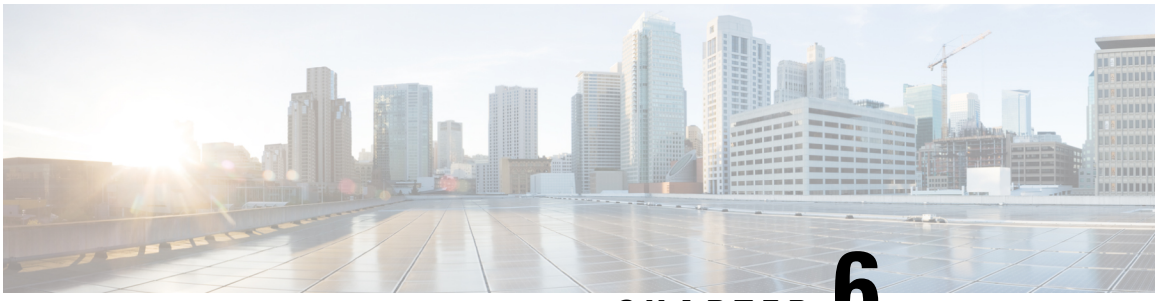
Example

Example 1

```
vm4(config)# validate
Validation complete
vm4(config)#
```

Related Topics

commit, on page 1074



CHAPTER 6

Command Filters for CLI Operational Commands

Overview of Command Filters for CLI Operational Commands	
append	Append the command output to a file.
begin	Display the command output beginning with the line that contains the specified string. The string is case-sensitive.
best-effort	Display the command output or continue loading a file even if some kind of failure has occurred that might interfere with the process.
context-match	Display the upper hierarchy in which a command or string appears in the configuration.
count	Count the number of lines in the command output. The count of lines includes the line on which you type the command.
de-select	Do not display a field in the command output.
details	Display the default values for commands in the running configuration.
display xml	Render the command output as XML.
exclude	Exclude the lines that contain the string defined by the regular expression from the command output.
include	Include only the lines that contain the string defined by the regular expression in the command output.
linnum	Number the lines in the command output. This command effectively counts the numbers of lines in the output.
match-all	Display the command output that matches all command-output filters.
match-any	Display the command output that matches any one of the command-output filters.
more	Paginate the command output. This is the default behavior.

nomore	Do not paginate command output.
notab	Display tabular command output in a list rather than in a table.
repeat	Redisplay the output of a show command periodically.
save	Save the command output to a file.
select	Display fields to display in the command output.
sort-by	Arrange the command output based on the values in a particular field.
tab	Display tabular command output in table even if the table is wider than the width of the screen.
until	Display the command output, ending with the line that contains the specified string. The string is case-sensitive.

- Overview of Command Filters for CLI Operational Commands, on page 1098
- append, on page 1099
- begin, on page 1100
- best-effort, on page 1101
- context-match, on page 1101
- count, on page 1102
- de-select, on page 1103
- details, on page 1104
- display xml, on page 1106
- exclude, on page 1107
- include, on page 1108
- linnum, on page 1109
- match-all, on page 1109
- match-any, on page 1110
- more, on page 1111
- nomore, on page 1112
- notab, on page 1113
- repeat, on page 1114
- save, on page 1114
- select, on page 1115
- sort-by, on page 1116
- tab, on page 1117
- until, on page 1118

Overview of Command Filters for CLI Operational Commands

This section describes the command filters you can use with CLI operational commands to modify operational command output or redirect the output to a file. To enter the filters, type a pipe (|) at the end of the command and then type the filter. You can include multiple filters after a command. Precede each filter with a pipe symbol.

The CLI filter commands are:

- append
- begin
- best-effort
- context-match
- count
- de-select
- details
- display xml
- exclude
- include
- match-all
- match-any
- more
- nomore
- notab
- repeat
- save
- select
- sort-by
- tab
- until

Note that not all filters are available with all commands.

append

Append the command output to a file.

append *filename*

Syntax Description

filename	Name of File: Append the command output to the specified filename.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1# show interface | append interface-file
vedge1# file list
interface-file
vedge1
```

Related Topics

file list, on page 637
file show, on page 637
save, on page 1114

begin

Display the command output beginning with the line that contains the specified string. The string is case-sensitive.

begin *string*

Syntax Description

string	String to Match: Text string to find to start displaying command output. The string is case-sensitive.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge# show ip route
Codes Protocol:                          <-- These 11 lines explain the values in the output.
  C -> connected, S -> static
  O -> ospf, B -> bgp
  M -> omp
Codes Proto-sub-type:
  IA -> ospf-inter-area
```

```
  E1 -> ospf-external1, E2 -> ospf-external2
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2
  e -> bgp-external, i -> bgp-internal
Codes Rstatus flags:
  F -> fib, S -> selected
                              PROTOCOL  NEXTHOP  NEXTHOP
VPN  ROUTE            PROTOCOL  SUB TYPE  IFNAME   ADDR       TLOC IP  COLOR  ENCAP  RSTATUS
-------------------------------------------------------------------------------------------
0    0.0.0.0/0        S         -         ge0/0    10.0.11.3  -        -      -      F,S
0    10.0.11.0/24     C         -         ge0/0    -          -        -      -      F,S
0    10.0.100.0/24    C         -         ge0/7    -          -        -      -      F,S
0    172.16.255.1/32  C         -         system   -          -        -      -      F,S

vedge# show ip route | begin PROTOCOL     <-- Display only the IP routes, without the key.

                              PROTOCOL  NEXTHOP  NEXTHOP
VPN  ROUTE            PROTOCOL  SUB TYPE  IFNAME   ADDR       TLOC IP  COLOR  ENCAP  RSTATUS
-------------------------------------------------------------------------------------------
0    0.0.0.0/0        S         -         ge0/0    10.0.11.3  -        -      -      F,S
0    10.0.11.0/24     C         -         ge0/0    -          -        -      -      F,S
0    10.0.100.0/24    C         -         ge0/7    -          -        -      -      F,S
0    172.16.255.1/32  C         -         system   -          -        -      -      F,S
```

Related Topics

until, on page 1118

best-effort

Display the command output or continue loading a file even if some kind of failure has occurred that might interfere with the process.

best-effort

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

context-match

Display the upper hierarchy in which a command or string appears in the configuration.

context-match *string*

Syntax Description

string	String To Match: Characters from the output to match.

Command History

Release	Modification
14.2	Command introduced.

Example

Example 1

```
vm5# show running-config | context-match ospf
vpn 1
  ospf
```

Related Topics

Overview of Command Filters for CLI Operational Commands, on page 1098

count

Count the number of lines in the command output. The count of lines includes the line on which you type the command.

count

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show ip routes vpn 0
Codes Proto-sub-type:
  IA -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive

                       PATH             PROTOCOL          NEXTHOP
VPN  PREFIX            ID    PROTOCOL   SUB TYPE  METRIC  IFNAME   NEXTHOP ADDR    TLOC IP  COLOR  ENCAP  STATUS
-------------------------------------------------------------------------------------------------------------------
0    0.0.0.0/0         0     Static     -         0       ge0/0    50.197.173.190  -        -      -      F,S
```

```
0    1.1.1.254/32       1     Connected  -         1       system   -              -       -      -      F,S
0    50.197.173.184/29  2     Connected  -         1       ge0/0    -              -       -      -      F,S

hw-vedge# show ip routes vpn 0 | begin 0 | count
Count: 4 lines
```

Related Topics

linnum, on page 1109

de-select

Do not display a field in the command output.

de-select *field*

Syntax Description

field	Column Not To Display: Field not to display in the command output. Use the **de-select ?** command to determine the possible completions for each command.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show ospf neighbor
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List
                   IF     IF                                DEAD
VPN  ADDRESS       INDEX  NAME   NEIGHBOR ID    STATE  PRI  TIME  DBsmL  RqstL  RXmtL
-------------------------------------------------------------------------------------
1    10.10.10.2    0      ge0/3  11.11.11.1     full   1    38    0      0      0

hw-vedge# show ospf neighbor | de-select ?
Description: List of neighbors
Possible completions:
  area                          Area
  area-type                     Area Type
  backup-designated-router-id   Backup designated Router ID
  db-summary-list               Database summary list
  dead-interval-timer           Dead interval timer(Secs)
  designated-router-id          Designated Router ID
  if-address                    Interface address
  if-name                       Interface Name
  interface-state               Interface state
  link-state-req-list           Link state request list
  link-state-retrans-list       Link state retransmission list
  neighbor-state                Neighbor state
```

```
  options                       ospf neighbor options : O|DN|DC|E|EA|MC|T|NP
  priority                      Priority
  progressive-change-time       Progressive change time(Secs)
  regressive-change-reason      Regressive change reason
  regressive-change-time        Regressive change time(Secs)
  router-id                     Neighbor ID
  state-changes                 Number of state changes
```

```
hw-vedge# show ospf neighbor | de-select db-summary-list
DBsmL -> Database Summary List
RqstL -> Link State Request List
RXmtl -> Link State Retransmission List
                    IF     IF                                    DEAD
VPN  ADDRESS        INDEX  NAME   NEIGHBOR ID    STATE   PRI  TIME  RqstL  RXmtL
-------------------------------------------------------------------------------
1    10.10.10.2     0      ge0/3  11.11.11.1     full    1    35    0      0
```

Related Topics

exclude, on page 1107
select, on page 1115

details

Display the default values for commands in the running configuration.

details

Syntax Description

None

Command History

Release	Modification
14.2	Command introduced.

Examples

Example 1

```
vm5# show running-config system logging
system
 logging
  disk
   enable
  !
 !
!
vm5# show running-config system logging | details
system
 logging
  disk
   enable
```

```
   file size 10
   file rotate 10
   priority information
  !
 !
!
```

Example 2

```
vm5# show 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
 !
!
vm5# show running-config vpn 1 | details
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
!
!
```

Related Topics

show running-config, on page 984
Overview of Command Filters for CLI Operational Commands, on page 1098

display xml

Render the command output as XML.

display xml

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1# show control local-properties | display xml
<config xmlns="http://tail-f.com/ns/config/1.0">
  <control xmlns="http://viptela.com/security">
  <local-properties>
    <device-type>vedge</device-type>
    <organization-name></organization-name>
    <certificate-status>Not-Installed</certificate-status>
    <root-ca-chain-status>Not-Installed</root-ca-chain-status>
    <dns-name>10.0.14.4</dns-name>
    <site-id>1</site-id>
    <domain-id>1</domain-id>
    <system-ip>172.16.255.1</system-ip>
    <keygen-interval>0:01:00:00</keygen-interval>
    <number-vbond-peers>0</number-vbond-peers>
    <number-active-wan-interfaces>1</number-active-wan-interfaces>
    <wan-interface-list>
      <index>0</index>
      <public-ip>0.0.0.0</public-ip>
      <public-port>0</public-port>
      <private-ip>10.0.11.1</private-ip>
      <private-port>12346</private-port>
      <num-vsmarts>0</num-vsmarts>
      <weight>1</weight>
      <color>default</color>
      <preference>0</preference>
      <admin-state>unknown</admin-state>
      <operation-state>unknown</operation-state>
    </wan-interface-list>
  </local-properties>
  </control>
</config>
```

exclude

Exclude the lines that contain the string defined by the regular expression from the command output.

exclude *regular-expression*

Syntax Description

regular-expression	String to Match: String to match when excluding lines from the command output.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface vpn 0
                                IF      IF
                                ADMIN   OPER    ENCAP                                                   SPEED                           RX        TX
VPN  INTERFACE  IP ADDRESS      STATUS  STATUS  TYPE    PORT TYPE  MTU   HWADDR             SPEED      MBPS    DUPLEX  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      10.0.0.1/24     Up      Up      null    transport  1500  00:0c:bd:05:df:b7  100     full    11:04:15:07  14549495  12435677
0    ge0/1      -               Down    Down    null    service    1500  00:0c:bd:05:df:b8  -       -       -            0         0
0    ge0/2      -               Down    Down    null    service    1500  00:0c:bd:05:df:b5  -       -       -            0         0
0    ge0/4      -               Down    Down    null    service    1500  00:0c:bd:05:df:bb  -       -       -            0         0
0    ge0/5      -               Down    Down    null    service    1500  00:0c:bd:05:df:bc  -       -       -            0         0
0    ge0/6      -               Down    Down    null    service    1500  00:0c:bd:05:df:b9  -       -       -            0         0
0    ge0/7      -               Down    Down    null    service    1500  00:0c:bd:05:df:ba  -       -       -            0         0
0    system     1.1.1.3/32      Up      Up      null    loopback   1500  00:00:00:00:00:00  10      full    11:04:15:17  0         0

hw-vedge# show interface vpn 0 | exclude IF | exclude ADMIN | exclude VPN | exclude ---
0    ge0/0      10.0.0.1/24     Up      Up      null    transport  1500  00:0c:bd:05:df:b7  100     full    11:04:15:31  14549857  12435986
0    ge0/1      -               Down    Down    null    service    1500  00:0c:bd:05:df:b8  -       -       -            0         0
0    ge0/2      -               Down    Down    null    service    1500  00:0c:bd:05:df:b5  -       -       -            0         0
0    ge0/4      -               Down    Down    null    service    1500  00:0c:bd:05:df:bb  -       -       -            0         0
0    ge0/5      -               Down    Down    null    service    1500  00:0c:bd:05:df:bc  -       -       -            0         0
0    ge0/6      -               Down    Down    null    service    1500  00:0c:bd:05:df:b9  -       -       -            0         0
0    ge0/7      -               Down    Down    null    service    1500  00:0c:bd:05:df:ba  -       -       -            0         0
0    system     1.1.1.3/32      Up      Up      null    loopback   1500  00:00:00:00:00:00  10      full    11:04:15:41  0         0
```

Related Topics

de-select, on page 1103
include, on page 1108

include

Include only the lines that contain the string defined by the regular expression in the command output.

include *regular-expression*

Syntax Description

regular-expression	String to Match: String to match when including lines from the command output.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface vpn 0 | include 10.1.1.8/24
0    ge0/0      10.0.0.1/24     Up      Up      null    transport  1500  00:0c:bd:05:df:b7  100     full    11:04:20:18  14554291  12439750
```

Related Topics

exclude, on page 1107

select, on page 1115

linnum

Number the lines in the command output. This command effectively counts the numbers of lines in the output.

linnum

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface vpn 0 | linnum1:
2:                                IF      IF
3:                                ADMIN   OPER    ENCAP                                                SPEED                        RX        TX
4: VPN  INTERFACE  IP ADDRESS     STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR             MBPS   DUPLEX  UPTIME       PACKETS   PACKETS
5: ------------------------------------------------------------------------------------------------------------------------------------------
6: 0    ge0/0      10.0.0.1/24    Up      Up      null   transport  1500  00:0c:bd:05:df:b7  100    full    11:04:22:04  14555968  12441172
7: 0    ge0/1      -              Down    Down    null   service    1500  00:0c:bd:05:df:b8  -      -       -            0         0
8: 0    ge0/2      -              Down    Down    null   service    1500  00:0c:bd:05:df:b5  -      -       -            0         0
9: 0    ge0/4      -              Down    Down    null   service    1500  00:0c:bd:05:df:bb  -      -       -            0         0
10: 0    ge0/5      -              Down    Down    null   service    1500  00:0c:bd:05:df:bc  -      -       -            0         0
11: 0    ge0/6      -              Down    Down    null   service    1500  00:0c:bd:05:df:b9  -      -       -            0         0
12: 0    ge0/7      -              Down    Down    null   service    1500  00:0c:bd:05:df:ba  -      -       -            0         0
13: 0    system     1.1.1.3/32     Up      Up      null   loopback   1500  00:00:00:00:00:00  10     full    11:04:22:14  0
```

Related Topics

count, on page 1102

match-all

Display the command output that matches all command-output filters.

match-all

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm9# show control connections
                                                                  PEER                    PEER
PEER     PEER             SITE        DOMAIN      PEER            PRIVATE  PEER           PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP      PORT     PUBLIC IP      PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
vedge    172.16.255.11    100         1           10.0.5.11       12346    10.0.5.11      12346   lte              up              0:02:31:49
vedge    172.16.255.21    100         1           10.0.5.21       12346    10.0.5.21      12346   lte              up              0:02:31:49
vedge    172.16.255.14    400         1           10.1.14.14      12350    10.1.14.14     12350   lte              up              0:02:31:52
vedge    172.16.255.15    500         1           10.1.15.15      12346    10.1.15.15     12346   lte              up              0:02:31:51
vedge    172.16.255.16    600         1           10.1.16.16      12346    10.1.16.16     12346   lte              up              0:02:31:50
vsmart   172.16.255.20    200         1           10.0.12.20      12346    10.0.12.20     12346   default          up              0:02:31:40
vbond    -                0           0           10.1.14.14      12346    10.1.14.14     12346   default          up              0:02:31:54
vm9# show control connections | select remote-color default | match-all
                                                                  PEER                    PEER
PEER     PEER             SITE        DOMAIN      PEER            PRIVATE  PEER           PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP      PORT     PUBLIC IP      PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
vsmart   172.16.255.20    200         1           10.0.12.20      12346    10.0.12.20     12346   default          up              0:02:33:42
vbond    -                0           0           10.1.14.14      12346    10.1.14.14     12346   default          up              0:02:33:56
```

Related Topics

match-any, on page 1110
select, on page 1115

match-any

Display the command output that matches any one of the command-output filters. Matching any is the default behavior when matching command output.

match-any

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm9# show control connections
                                                                  PEER                  PEER
PEER     PEER             SITE        DOMAIN      PEER            PRIVATE  PEER         PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP      PORT     PUBLIC IP    PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------
vedge    172.16.255.11    100         1           10.0.5.11       12346    10.0.5.11    12346   lte              up              0:02:31:49
vedge    172.16.255.21    100         1           10.0.5.21       12346    10.0.5.21    12346   lte              up              0:02:31:49
vedge    172.16.255.14    400         1           10.1.14.14      12350    10.1.14.14   12350   lte              up              0:02:31:52
vedge    172.16.255.15    500         1           10.1.15.15      12346    10.1.15.15   12346   lte              up              0:02:31:51
vedge    172.16.255.16    600         1           10.1.16.16      12346    10.1.16.16   12346   lte              up              0:02:31:50
vsmart   172.16.255.20    200         1           10.0.12.20      12346    10.0.12.20   12346   default          up              0:02:31:40
vbond    -                0           0           10.1.14.14      12346    10.1.14.14   12346   default          up              0:02:31:54
vm9# show control connections | select remote-color default | match-any
                                                                  PEER                  PEER
PEER     PEER             SITE        DOMAIN      PEER            PRIVATE  PEER         PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP      PORT     PUBLIC IP    PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------
vsmart   172.16.255.20    200         1           10.0.12.20      12346    10.0.12.20   12346   default          up              0:02:33:38
vbond    -                0           0           10.1.14.14      12346    10.1.14.14   12346   default          up
```

Related Topics

match-all, on page 1109
select, on page 1115

more

Paginate the command output. This is the default behavior.

more

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface | more                                IF      IF
                                ADMIN   OPER    ENCAP                                       SPEED                           RX        TX
VPN  INTERFACE  IP ADDRESS      STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR             MBPS   DUPLEX  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      10.0.0.1/24     Up      Up      null   transport  1500  00:0c:bd:05:df:b7  100    full    11:04:33:54  14566836  12450259
0    ge0/1      -               Down    Down    null   service    1500  00:0c:bd:05:df:b8  -      -       -            0         0
0    ge0/2      -               Down    Down    null   service    1500  00:0c:bd:05:df:b5  -      -       -            0         0
0    ge0/4      -               Down    Down    null   service    1500  00:0c:bd:05:df:bb  -      -       -            0         0
0    ge0/5      -               Down    Down    null   service    1500  00:0c:bd:05:df:bc  -      -       -            0         0
0    ge0/6      -               Down    Down    null   service    1500  00:0c:bd:05:df:b9  -      -       -            0         0
0    ge0/7      -               Down    Down    null   service    1500  00:0c:bd:05:df:ba  -      -       -            0         0
0    system     1.1.1.3/32      Up      Up      null   loopback   1500  00:00:00:00:00:00  10     full    11:04:34:05  0         0
1    ge0/3      10.1.1.1/24     Up      Up      null   service    1500  00:0c:bd:05:df:b6  1000   full    11:04:33:52  277881    231784
--More--
```

Related Topics

nomore, on page 1112

nomore

Do not paginate command output.

nomore

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface | nomore
                                IF      IF
                                ADMIN   OPER    ENCAP                                       SPEED                           RX        TX
VPN  INTERFACE  IP ADDRESS      STATUS  STATUS  TYPE   PORT TYPE  MTU   HWADDR             MBPS   DUPLEX  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      10.0.0.1/24     Up      Up      null   transport  1500  00:0c:bd:05:df:b7  100    full    11:04:33:54  14566836  12450259
0    ge0/1      -               Down    Down    null   service    1500  00:0c:bd:05:df:b8  -      -       -            0         0
```

```
0    ge0/2      -               Down    Down    null   service    1500  00:0c:bd:05:df:b5  -      -      -            0         0
0    ge0/4      -               Down    Down    null   service    1500  00:0c:bd:05:df:bb  -      -      -            0         0
0    ge0/5      -               Down    Down    null   service    1500  00:0c:bd:05:df:bc  -      -      -            0         0
0    ge0/6      -               Down    Down    null   service    1500  00:0c:bd:05:df:b9  -      -      -            0         0
0    ge0/7      -               Down    Down    null   service    1500  00:0c:bd:05:df:ba  -      -      -            0         0
0    system     1.1.1.3/32      Up      Up      null   loopback   1500  00:00:00:00:00:00  10     full   11:04:34:05  0         0
1    ge0/3      10.1.1.1/24     Up      Up      null   service    1500  00:0c:bd:05:df:b6  1000   full   11:04:33:52  277881    231784
hw-vedge#
```

Related Topics

more, on page 1111

notab

Display tabular command output in a list rather than in a table. Note that if tabular command output is wider that the screen width, the output is automatically displayed in a list. Use the **tab** filter to override this display behavior. Use the **screen-width** command to set the screen width, or simply drag the terminal window to the desired size. Changing the screen size by dragging the window overrides the width set by the **screen-width** command.

notab

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface vpn 0 | notab
interface vpn 0 interface ge0/0
 ip-address      10.0.0.1/24
 if-admin-status Up
 if-oper-status  Up
 encap-type      null
 port-type       transport
 mtu             1500
 hwaddr          00:0c:bd:05:df:b7
 speed-mbps      100
 duplex          full
 uptime          11:04:40:13
 rx-packets      14572308
 tx-packets      12455087
interface vpn 0 interface ge0/1
 ip-address      -
 if-admin-status Down
 if-oper-status  Down
 encap-type      null
 port-type       service
```

```
 mtu             1500
 hwaddr          00:0c:bd:05:df:b8
 rx-packets      0
--More--
```

Related Topics

screen-width, on page 716
tab, on page 1117

repeat

Redisplay the output of a **show** command periodically.

repeat *seconds*

Syntax Description

seconds	Repeat Time: How often to repeat the command, in seconds. Type Control-C to terminate the display.

Command History

Release	Modification
14.1	Command introduced.

save

Save the command output to a file.

save *filename* [**overwrite**]

Syntax Description

filename	Name of File: Save the command output in the specified filename.
overwrite	Overwrite the File Contents: Overwrite the contents of an existing file.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vedge1# show interface | save interface-file
vedge1# file list
interface-file
vedge1#
```

Related Topics

append, on page 1099
file list, on page 637
file show, on page 637

select

Display fields to display in the command output.

select *field*

Syntax Description

field	Field To Add: Field to display in the command output. Use the **select ?** command to determine the available fields for each command.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm9# show control connections | select ? Description: Display control connections information
Possible completions:
  local-color           Local Color
  private-ip            Private ip
  private-port          Private port
  remote-color          Remote Color
  rx_challenge          Rx Challenge
  rx_challenge_ack      Rx Challenge Ack
  rx_challenge_resp     Rx Challenge Response
  rx_connects           Rx Connects
  rx_hello              Rx Hello
  rx_register_replies   Rx Register Replies
  rx_registers          Rx Registers
  rx_teardown           Rx Teardown
  state                 State
  system-ip             System IP address
  tx_challenge          Tx Challenge
  tx_challenge_ack      Tx Challenge Ack
  tx_challenge_resp     Tx Challenge Response
  tx_connects           Tx Connects
  tx_hello              Tx Hello
  tx_register_replies   Tx Register Replies
```

```
  tx_registers          Tx Registers
  tx_teardown           Tx Teardown
  tx_teardown_all       Tx Teardown all connections
  uptime                Uptime
vm9# show control connections | select state
                                                                    PEER                    PEER
PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER           PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP      PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
vedge    172.16.255.11    100         1           10.0.5.11        12346    10.0.5.11      12346   lte              up              0:02:32:46
vedge    172.16.255.21    100         1           10.0.5.21        12346    10.0.5.21      12346   lte              up              0:02:32:46
vedge    172.16.255.14    400         1           10.1.14.14       12350    10.1.14.14     12350   lte              up              0:02:32:49
vedge    172.16.255.15    500         1           10.1.15.15       12346    10.1.15.15     12346   lte              up              0:02:32:48
vedge    172.16.255.16    600         1           10.1.16.16       12346    10.1.16.16     12346   lte              up              0:02:32:47
vsmart   172.16.255.20    200         1           10.0.12.20       12346    10.0.12.20     12346   default          up              0:02:32:37
vbond    -                0           0           10.1.14.14       12346    10.1.14.14     12346   default          up              0:02:32:51
```

Related Topics

de-select, on page 1103
match-all, on page 1109
match-any, on page 1110

sort-by

Arrange the command output based on the values in a particular field.

sort-by *field*

Syntax Description

field	Column Not To Display: Field by which to arrange the command output. Use the **sort-by ?** command to determine the possible completions for each command.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm9# show control connections
                                                                    PEER                    PEER
PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER           PUBLIC
TYPE     SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP      PORT    REMOTE COLOR     STATE           UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------------
vedge    172.16.255.11    100         1           10.0.5.11        12346    10.0.5.11      12346   lte              up              0:01:13:09
vedge    172.16.255.21    100         1           10.0.5.21        12346    10.0.5.21      12346   lte              up              0:01:13:09
vedge    172.16.255.14    400         1           10.1.14.14       12350    10.1.14.14     12350   lte              up              0:01:13:07
vedge    172.16.255.15    500         1           10.1.15.15       12346    10.1.15.15     12346   lte              up              0:01:13:09
vedge    172.16.255.16    600         1           10.1.16.16       12346    10.1.16.16     12346   lte              up              0:01:13:07
vsmart   172.16.255.20    200         1           10.0.12.20       12346    10.0.12.20     12346   default          up              0:01:13:21
```

```
vbond    -               0          0          10.1.14.14       12346    10.1.14.14       12346   default         up             0:01:13:23

vm9# show control connections | sort-by site-id
                                                                  PEER                      PEER
PEER     PEER            SITE       DOMAIN     PEER             PRIVATE  PEER             PUBLIC
TYPE     SYSTEM IP       ID         ID         PRIVATE IP       PORT     PUBLIC IP        PORT    REMOTE COLOR    STATE          UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------
vbond    -               0          0          10.1.14.14       12346    10.1.14.14       12346   default         up             0:01:23:51
vedge    172.16.255.11   100        1          10.0.5.11        12346    10.0.5.11        12346   lte             up             0:01:23:37
vedge    172.16.255.21   100        1          10.0.5.21        12346    10.0.5.21        12346   lte             up             0:01:23:37
vsmart   172.16.255.20   200        1          10.0.12.20       12346    10.0.12.20       12346   default         up             0:01:23:50
vedge    172.16.255.14   400        1          10.1.14.14       12350    10.1.14.14       12350   lte             up             0:01:23:35
vedge    172.16.255.15   500        1          10.1.15.15       12346    10.1.15.15       12346   lte             up             0:01:23:37
vedge    172.16.255.16   600        1          10.1.16.16       12346    10.1.16.16       12346   lte             up             0:01:23:35
```

Related Topics

exclude, on page 1107
include, on page 1108

tab

Display tabular command output in table even if the table is wider than the width of the screen. If the command output is wider that the screen width, it wraps onto two or more lines. Use the **screen-width** command to set the screen width, or simply drag the terminal window to the desired size. Changing the screen size by dragging the window overrides the width set by the cli **screen-width** command.

tab

Syntax Description

None

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
vm1# show interface ge0/1
interface vpn 0 interface ge0/1
 ip-address      10.0.26.11/24
 if-admin-status Up
 if-oper-status  Up
 encap-type      null
 port-type       service
 mtu             1500
 hwaddr          00:0c:29:ab:b7:62
 speed-mbps      10
 duplex          full
 uptime          0:00:49:33
 rx-packets      3
 tx-packets      2
vm1# show interface ge0/1 | tab
                              IF      IF
                              ADMIN   OPER    ENCAP  PORT                              SPEED                      RX       TX
VPN  INTERFACE  IP ADDRESS    STATUS  STATUS  TYPE   TYPE     MTU   HWADDR             MBPS   DUPLEX  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/1      10.0.26.11/24 Up      Up      null   service  1500  00:0c:29:ab:b7:62  10     full    0:00:49:46  3        2
```

Related Topics

notab, on page 1113

screen-width, on page 716

until

Display the command output, ending with the line that contains the specified string. The string is case-sensitive.

until *string*

Syntax Description

string	String to Match: Text string to find to start displaying command output. The string is case-sensitive.

Command History

Release	Modification
14.1	Command introduced.

Example

Example 1

```
hw-vedge# show interface | until 10.0.0.1
                                IF      IF
                                ADMIN   OPER    ENCAP                                   SPEED                       RX        TX
VPN  INTERFACE  IP ADDRESS      STATUS  STATUS  TYPE    PORT TYPE  MTU   HWADDR         MBPS   DUPLEX  UPTIME       PACKETS   PACKETS
-------------------------------------------------------------------------------------------------------------------------------------
0    ge0/0      10.0.0.1/24     Up      Up      null    transport  1500  00:0c:bd:05:df:b7  100    full    11:05:10:21  14598208  1247744
```

Related Topics

begin, on page 1100