

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 9
- aaa, on page 10
- aaa netconf-accounting, on page 13
- access-list, on page 14
- access-list, on page 16
- accounting-interval, on page 17
- acct-req-attr, on page 18
- action, on page 20
- action, on page 34
- address-family, on page 36
- address-pool, on page 39
- admin-auth-order, on page 40
- admin-state, on page 41
- admin-tech-on-failure, on page 42
- advertise, on page 43
- age-time, on page 44
- alarms, on page 45
- allow-local-exit, on page 46
- allow-same-site-tunnels, on page 47
- allow-service, on page 49
- api-key, on page 51
- app-probe-class, on page 52
- app-route-policy, on page 53
- app-visibility, on page 55
- applications, on page 57
- apply-policy, on page 58
- archive, on page 61

- area, on page 63
- arp, on page 65
- arp-timeout, on page 66
- auth-fail-vlan, on page 67
- auth-fallback, on page 68
- auth-order, on page 70
- auth-order, on page 71
- auth-reject-vlan, on page 73
- auth-req-attr, on page 74
- authentication, on page 76
- authentication-type, on page 77
- authentication-type, on page 78
- auto-cost reference-bandwidth, on page 80
- auto-sig-tunnel-probing, on page 81
- auto-rp, on page 81
- autonegotiate, on page 82
- bandwidth-downstream, on page 83
- bandwidth-upstream, on page 85
- banner login, on page 87
- banner motd, on page 88
- best-path, on page 89
- bfd app-route, on page 91
- bfd color, on page 92
- bfd app-route color, on page 95
- bgp, on page 96
- bind, on page 98
- block-icmp-error, on page 99
- block-non-source-ip, on page 100
- bridge, on page 101
- capability-negotiate, on page 103
- carrier, on page 104
- cellular, on page 105
- cflowd-template, on page 107
- channel, on page 108
- channel-bandwidth, on page 110
- cipher-suite, on page 111
- class-map, on page 113
- clear-dont-fragment, on page 114
- clock, on page 115
- cloud-qos, on page 116
- cloud-qos-service-side, on page 118
- cloudexpress, on page 121
- collector, on page 122
- color, on page 123
- community, on page 125
- compatible rfc1583, on page 126

- connections-limit, on page 128
- console-baud-rate, on page 129
- contact, on page 130
- container, on page 131
- control, on page 131
- control-connections, on page 132
- control-direction, on page 133
- control-policy, on page 134
- control-session-pps, on page 135
- controller-group-id, on page 136
- controller-group-list, on page 137
- controller-send-path-limit, on page 138
- cost, on page 139
- country, on page 140
- cpu-usage, on page 142
- crypto pki trustpoint, on page 143
- crypto pki authenticate, on page 144
- crypto pki enroll, on page 146
- crypto pki import, on page 147
- custom-eflow, on page 148
- das, on page 149
- data-policy, on page 151
- data-security, on page 154
- dead-interval, on page 156
- dead-peer-detection, on page 157
- default-action, on page 158
- default-information originate, on page 161
- default-vlan, on page 162
- description, on page 164
- device-groups, on page 165
- dhcp-helper, on page 165
- dhcp-server, on page 167
- dialer down-with-vInterface, on page 168
- direction, on page 169
- discard-rejected, on page 170
- disk-speed, on page 171
- disk-usage, on page 172
- distance, on page 174
- dns, on page 175
- domain-id, on page 176
- dot1x, on page 177
- duplex, on page 181
- ebgp-multihop, on page 182
- ecmp-hash-key, on page 183
- ecmp-limit, on page 184
- eco-friendly-mode, on page 185

- eigrp, on page 186
- elephant-flow, on page 187
- encapsulation, on page 188
- exclude, on page 191
- exclude-controller-group-list, on page 193
- flow-active-timeout, on page 194
- flow-control, on page 195
- flow-inactive-timeout, on page 196
- flow-sampling-interval, on page 197
- flow-visibility, on page 198
- gps-location, on page 199
- graceful-restart, on page 200
- group, on page 201
- group, on page 203
- group, on page 204
- guard-interval, on page 205
- guest-vlan, on page 206
- hello-interval, on page 207
- hello-interval, on page 209
- hello-interval, on page 210
- hello-tolerance, on page 211
- hold-time, on page 213
- host, on page 214
- host-mode, on page 215
- host-name, on page 216
- host-policer-pps, on page 217
- icmp-error-pps, on page 218
- icmp-redirect-disable, on page 219
- idle-timeout, on page 220
- igmp, on page 221
- ike, on page 222
- implicit-acl-logging, on page 224
- interface, on page 225
- interface, on page 229
- interface, on page 232
- interface, on page 233
- interface, on page 234
- interface, on page 236
- interface gre, on page 237
- interface ipsec, on page 238
- interface irb, on page 241
- interface ppp, on page 242
- integrity-type, on page 244
- ip address, on page 245
- ip address-list, on page 246
- ip dhcp-client, on page 248

- ip gre-route, on page 250
- ip ipsec-route, on page 251
- ip route, on page 253
- ip secondary-address, on page 255
- ipsec, on page 256
- ipsec, on page 257
- iptables-enable, on page 258
- ipv6 address, on page 258
- ipv6 dhcp-client, on page 260
- ipv6 route, on page 261
- join-group, on page 263
- join-prune-interval, on page 264
- keepalive, on page 265
- last-resort-circuit, on page 267
- lease-time, on page 268
- lists, on page 269
- local-interface-list, on page 278
- location, on page 279
- location, on page 281
- log-frequency, on page 281
- log-translations, on page 283
- logging disk, on page 284
- logging host, on page 289
- logging tls-profile, on page 291
- logging server, on page 291
- logs, on page 294
- low-bandwidth-link, on page 295
- mac-accounting, on page 296
- mac-address, on page 297
- mac-authentication-bypass, on page 298
- match, on page 299
- match, on page 300
- match, on page 302
- max-clients, on page 314
- max-control-connections, on page 315
- max-controllers, on page 317
- max-leases, on page 317
- max-macs, on page 318
- max-metric, on page 319
- max-omp-sessions, on page 320
- memory-usage, on page 322
- mgmt-security, on page 323
- mode, on page 324
- mtu, on page 325
- multicast-buffer-percent, on page 326
- multicast-replicator, on page 327

- name, on page 328
- name, on page 329
- nas-identifier, on page 330
- nas-ip-address, on page 331
- nat, on page 332
- nat-refresh-interval, on page 334
- natpool, on page 335
- neighbor, on page 336
- network, on page 337
- next-hop-self, on page 338
- node-type, on page 339
- nssa, on page 340
- ntp, on page 342
- offer-time, on page 345
- omp, on page 346
- on-demand enable, on page 347
- on-demand idle-timeout, on page 347
- options, on page 348
- organization-name, on page 350
- orgid, on page 350
- ospf, on page 351
- ospfv3 authentication, on page 353
- overlay-as, on page 354
- overload, on page 355
- parameter-map type umbrella global, on page 357
- parent, on page 357
- passive-interface, on page 358
- password, on page 359
- peer, on page 360
- perfect-forward-secrecy, on page 362
- pim, on page 363
- pmtu, on page 364
- policer, on page 365
- policy, on page 368
- policy ipv6, on page 374
- port-forward, on page 376
- port-hop, on page 377
- port-offset, on page 379
- port-scan, on page 380
- ppp, on page 381
- pppoe-client, on page 383
- priority, on page 384
- probe, on page 385
- probe-path branch, on page 387
- probe-path gateway, on page 388
- profile, on page 389

- profile, on page 391
- propagate-aspath, on page 392
- propagate-community, on page 393
- radius, on page 393
- radius-servers, on page 397
- range, on page 400
- reauthentication, on page 401
- redistribute, on page 402
- redistribute leaked routes, on page 404
- refresh, on page 404
- rekey, on page 405
- rekey, on page 407
- remote-as, on page 408
- replay-window, on page 408
- replay-window, on page 409
- replicator-selection, on page 410
- respond-to-ping, on page 411
- retransmit-interval, on page 412
- rewrite-rule, on page 413
- route-consistency-check, on page 415
- route-export, on page 416
- route-import, on page 417
- route-import-service (for route leak), on page 417
- route-map, on page 418
- route-policy, on page 419
- router, on page 421
- router-id, on page 423
- router-id, on page 424
- secret, on page 425
- security, on page 426
- send-community, on page 426
- send-ext-community, on page 427
- send-path-limit, on page 428
- sense level, on page 429
- service, on page 431
- service-insertion appnav-controller-group appqoe, on page 434
- **service-insertion service-node-group** appqoe, on page 435
- set ip next-hop verify-availability, on page 436
- shaping-rate, on page 437
- shutdown, on page 438
- site-id, on page 440
- sla-class, on page 441
- snmp, on page 442
- sp-organization-name, on page 443
- speed, on page 444
- spt-threshold, on page 445

- ssid, on page 446
- static, on page 448
- static-ingress-qos, on page 450
- static-lease, on page 451
- stub, on page 452
- system, on page 453
- system-ip, on page 456
- system-tunnel-mtu, on page 458
- **system patch-confirm**, on page 459
- table-map, on page 460
- tacacs, on page 460
- tcp-mss-adjust, on page 463
- tcp-optimization, on page 465
- tcp-optimization-enabled, on page 465
- tcp-syn-flood-limit, on page 466
- tcp-timeout, on page 467
- technology, on page 469
- template-refresh, on page 470
- timeout inactivity, on page 471
- timer, on page 472
- tracker-dns-cache-timeout, on page 474
- timers, on page 475
- timers, on page 476
- timers, on page 478
- tloc-extension, on page 480
- tloc-extension-gre-from, on page 482
- tloc-extension-gre-to, on page 483
- track, on page 485
- track-default-gateway, on page 486
- track-interface-tag, on page 487
- track-list, on page 489
- track-transport, on page 490
- tracker, on page 491
- trap group, on page 493
- trap target, on page 495
- tunnel-destination, on page 497
- tunnel-destination, on page 498
- tunnel-interface, on page 499
- tunnel-source, on page 500
- tunnel-source, on page 501
- tunnel-source-interface, on page 503
- tunnel-source-interface, on page 504
- tunnel vrf multiplexing, on page 505
- udp-timeout, on page 505
- update-source, on page 506
- upgrade-confirm, on page 507

- usb-controller, on page 509
- user, on page 510
- user, on page 511
- usergroup, on page 513
- vbond, on page 515
- vbond-as-stun-server, on page 518
- view, on page 519
- vlan, on page 521
- vmanage-connection-preference, on page 522
- vpn, on page 523
- vpn-membership, on page 527
- vrrp, on page 528
- wake-on-lan, on page 532
- wlan, on page 533
- wpa-personal-key, on page 535
- zone, on page 536
- zone-based-policy, on page 537
- zone-pair, on page 539
- zone-to-nozone-internet, on page 541

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 177
radius, on page 393
tacacs, on page 460

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 16

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 14

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 18
nas-identifier, on page 330
nas-ip-address, on page 331
radius, on page 393
radius-servers, on page 397

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 74
nas-identifier, on page 330

nas-ip-address, on page 331
radius, on page 393
radius-servers, on page 397

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 58
lists, on page 269
match, on page 302
policy, on page 368
policy ipv6, on page 374

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 368

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 68
auth-order, on page 71
radius, on page 393
tacacs, on page 460
usergroup, on page 513

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
show crash

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 480

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 128
icmp-redirect-disable, on page 219
implicit-acl-logging, on page 224
ntp, on page 342
service, on page 431
vbond-as-stun-server, on page 518

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 441

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
action, on page 34
cflowd-template, on page 107
control-policy, on page 134
data-policy, on page 151
lists, on page 269
match, on page 300
policy, on page 368

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

save

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 73
bridge, on page 101
default-vlan, on page 162
guest-vlan, on page 206
radius, on page 393

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 40
auth-order, on page 71
radius, on page 393
tacacs, on page 460
usergroup, on page 513

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 298
radius, on page 393
radius-servers, on page 397

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 40
auth-fallback, on page 68
radius, on page 393
tacacs, on page 460
usergroup, on page 513

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 67
bridge, on page 101
default-vlan, on page 162
guest-vlan, on page 206

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 18
nas-identifier, on page 330
nas-ip-address, on page 331
radius, on page 393
radius-servers, on page 397

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 324

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 181
speed, on page 444

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 85

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 83

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 88

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 87

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 92

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 91
encapsulation, on page 188
last-resort-circuit, on page 267
mtu, on page 325
pmtu, on page 364
hello-interval, on page 207
hello-tolerance, on page 211

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 241

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 1: 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 391

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 110

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 108

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 16
cloud-qos, on page 116
rewrite-rule, on page 413

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 325
pmtu, on page 364

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 16
class-map, on page 113
cloud-qos-service-side, on page 118
rewrite-rule, on page 413

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 16

class-map, on page 113
cloud-qos, on page 116
rewrite-rule, on page 413

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 188

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 49

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 246

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 2: 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 217
icmp-error-pps, on page 218
policer, on page 365

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 137
exclude-controller-group-list, on page 193
max-control-connections, on page 315
max-omp-sessions, on page 320

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 136
exclude-controller-group-list, on page 193
max-control-connections, on page 315
max-omp-sessions, on page 320

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 108
channel-bandwidth, on page 110
radius, on page 393

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 393

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 527

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 323
radius, on page 393
radius-servers, on page 397
wpa-personal-key, on page 535

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 210

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 67
auth-reject-vlan, on page 73
bridge, on page 101
guest-vlan, on page 206
radius, on page 393

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 328

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 167

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 49
dhcp-helper, on page 165

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 188

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 393

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 82
speed, on page 444

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 92
color, on page 123

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 136
controller-group-list, on page 137
max-control-connections, on page 315
max-omp-sessions, on page 320

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 196

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 194

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 281
location, on page 279

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 478

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 510

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 324

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 67
auth-reject-vlan, on page 73
bridge, on page 101
default-vlan, on page 162
mac-authentication-bypass, on page 298
radius, on page 393

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 92
hello-tolerance, on page 211

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 156

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 92
hello-interval, on page 207

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 393

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 135
icmp-error-pps, on page 218
policer, on page 365

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 135
host-policer-pps, on page 217
policer, on page 365

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 49

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

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 49
log-frequency, on page 281

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 101

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 248
ipv6 address, on page 258
ipv6 dhcp-client, on page 260
system-ip, on page 456
ip secondary-address, on page 255

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 131

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 245
ipv6 address, on page 258
ipv6 dhcp-client, on page 260

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 253
keepalive, on page 265
nat, on page 332

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 250
ip route, on page 253
keepalive, on page 265
nat, on page 332

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 250
ipv6 route, on page 261
nat, on page 332

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 245
ip dhcp-client, on page 248
ipv6 address, on page 258
ipv6 dhcp-client, on page 260
system-ip, on page 456

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 222

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

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 245
ipv6 address, on page 258
ipv6 dhcp-client, on page 260
system-ip, on page 456

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 245
ipv6 address, on page 258

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 253

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 497
tunnel-source, on page 501

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 92

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 20
apply-policy, on page 58
match, on page 302
policy, on page 368
sla-class, on page 441

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 199
location, on page 281

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 199
location, on page 279

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 224

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 188
static, on page 448

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 291
show crash
show logging

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 3: 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 4: 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 284

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 393

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 302

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 20
apply-policy, on page 58
lists, on page 269
match, on page 300
policy, on page 368

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 136
controller-group-list, on page 137
exclude-controller-group-list, on page 193
max-omp-sessions, on page 320

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 136
controller-group-list, on page 137
exclude-controller-group-list, on page 193

max-control-connections, on page 315

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 154

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 204

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 92
pmtu, on page 364
tcp-mss-adjust, on page 463

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 18
auth-req-attr, on page 74
nas-ip-address, on page 331
radius, on page 393
radius-servers, on page 397

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 18
auth-req-attr, on page 74
nas-identifier, on page 330
radius, on page 393
radius-servers, on page 397

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 188
action, on page 34
ip gre-route, on page 250
ip route, on page 253

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 49

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

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 392

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 188

static, on page 448

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 5: 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 6: 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 92
clear-dont-fragment, on page 114
mtu, on page 325

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 135
host-policer-pps, on page 217
icmp-error-pps, on page 218
match, on page 302

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 16
apply-policy, on page 58
policy ipv6, on page 374
redistribute, on page 402

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 368

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 200
port-offset, on page 379
request port-hop

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 377

request port-hop

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 383

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 ge slot/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 381

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 423

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 389

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 354

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 10
admin-auth-order, on page 40
auth-fallback, on page 68
auth-order, on page 71
dot1x, on page 177
tacacs, on page 460
wlan, on page 533

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 393

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 393

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 419

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 200
request security ipsec-rekey
show bfd sessions
timers, on page 478

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 222

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 253
ipv6 route, on page 261

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 368
redistribute, on page 402

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 384
system-ip, on page 456

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 456

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 49
tunnel-destination, on page 497
tunnel-source, on page 501

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

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 82
duplex, on page 181

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 7: 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 8: 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 188
direction, on page 169
natpool, on page 335
overload, on page 355

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 245
router-id, on page 424
router-id, on page 423

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 463

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 10
admin-auth-order, on page 40
auth-fallback, on page 68
auth-order, on page 71
radius, on page 393

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 458

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 465

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 465

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 527
zone, on page 536

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 389

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 393

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 515

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 200
rekey, on page 405

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 47

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 483

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 482

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 9: 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 253

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 487

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 10: 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 332

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

trap target, on page 495

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

trap group, on page 493

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 265
tunnel-source, on page 501

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 222
tunnel-source, on page 500
tunnel-source-interface, on page 503

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 222
tunnel-destination, on page 498
tunnel-source-interface, on page 503

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 265
tunnel-destination, on page 497
tunnel-source-interface, on page 504

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 222
tunnel-destination, on page 498
tunnel-source, on page 500

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 265
tunnel-destination, on page 497
tunnel-source, on page 501

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

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 203

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 68
auth-order, on page 71
radius, on page 393
tacacs, on page 460
usergroup, on page 513

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 393
tacacs, on page 460
user, on page 511

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 377

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 49

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 295

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 151

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 478

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 133
radius, on page 393

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 393

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 154

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 537
zone-pair, on page 539
zone-to-nozone-internet, on page 541

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 536
zone-pair, on page 539
zone-to-nozone-internet, on page 541

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 536
zone-based-policy, on page 537

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 536
zone-based-policy, on page 537
zone-pair, on page 539