Configuration Commands

- Configuration Commands, on page 9
- Overview of Configuration Commands, on page 28
- aaa, on page 29
- access-list, on page 31
- access-list, on page 33
- accounting-interval, on page 35
- acct-req-attr, on page 37
- action, on page 39
- action, on page 53
- address-family, on page 55
- address-pool, on page 59
- admin-auth-order, on page 60
- admin-state, on page 62
- admin-tech-on-failure, on page 64
- advertise, on page 65
- age-time, on page 67
- allow-local-exit, on page 69
- allow-same-site-tunnels, on page 70
- allow-service, on page 72
- app-route-policy, on page 75
- app-visibility, on page 77
- applications, on page 79
- apply-policy, on page 81
- archive, on page 85
- area, on page 87
- arp, on page 89
- arp-timeout, on page 91
- auth-fail-vlan, on page 92
- auth-fallback, on page 94
- auth-order, on page 96
- auth-order, on page 97
- auth-reject-vlan, on page 100
- auth-req-attr, on page 102
- authentication, on page 104
- authentication-type, on page 106
- authentication-type, on page 108
- auto-cost reference-bandwidth, on page 111
- auto-rp, on page 113
- autonegotiate, on page 114
- bandwidth-downstream, on page 116
- bandwidth-upstream, on page 118
- banner login, on page 120
- banner motd, on page 121
- best-path, on page 122
- bfd app-route, on page 124
- bfd color, on page 126
- bgp, on page 129
- bind, on page 131
- block-icmp-error, on page 133
- block-non-source-ip, on page 135
- bridge, on page 136
- capability-negotiate, on page 138
- carrier, on page 139
- cellular, on page 141
- cflowd-template, on page 143
- channel, on page 145
- channel-bandwidth, on page 147
- cipher-suite, on page 149
- class-map, on page 151
- clear-dont-fragment, on page 153
- clock, on page 154
- cloud-qos, on page 155
- cloud-qos-service-side, on page 158
- cloudexpress, on page 161
- collector, on page 162
- color, on page 164
- community, on page 167
- compatible rfc1583, on page 169
- connections-limit, on page 171
- console-baud-rate, on page 173
- contact, on page 174
- container, on page 175
- control, on page 178
- control-connections, on page 179
- control-direction, on page 181
- control-policy, on page 183
- control-session-pps, on page 184
- controller-group-id, on page 185
- controller-group-list, on page 186
• cost, on page 188
• country, on page 189
• das, on page 191
• data-policy, on page 194
• data-security, on page 197
• dead-interval, on page 199
• dead-peer-detection, on page 201
• default-action, on page 203
• default-information originate, on page 206
• default-vlan, on page 208
• description, on page 210
• device-groups, on page 211
• dhcp-helper, on page 212
• dhcp-server, on page 214
• direction, on page 216
• discard-rejected, on page 218
• distance, on page 219
• distance, on page 221
• dns, on page 223
• domain-id, on page 224
• dot1x, on page 225
• duplex, on page 230
• ebgp-multihop, on page 232
• ecmp-hash-key, on page 234
• ecmp-limit, on page 235
• eco-friendly-mode, on page 236
• eigrp, on page 237
• encapsulation, on page 239
• exclude, on page 242
• exclude-controller-group-list, on page 244
• flow-active-timeout, on page 246
• flow-control, on page 248
• flow-inactive-timeout, on page 249
• flow-sampling-interval, on page 251
• flow-visibility, on page 253
• gps-location, on page 254
• graceful-restart, on page 255
• group, on page 256
• group, on page 258
• group, on page 259
• guard-interval, on page 260
• guest-vlan, on page 262
• hello-interval, on page 264
• hello-interval, on page 266
• hello-interval, on page 268
• hello-tolerance, on page 270
• host, on page 272
• host-mode, on page 274
• host-name, on page 276
• host-policer-pps, on page 277
• icmp-error-pps, on page 278
• icmp-redirect-disable, on page 279
• idle-timeout, on page 280
• igmp, on page 281
• ike, on page 283
• implicit-acl Logging, on page 285
• interface, on page 287
• interface, on page 292
• interface, on page 295
• interface, on page 297
• interface, on page 299
• interface, on page 301
• interface gre, on page 303
• interface ipsec, on page 305
• interface irb, on page 307
• interface ppp, on page 309
• ip address, on page 311
• ip address-list, on page 313
• ip dhcp-client, on page 315
• ip gre-route, on page 317
• ip ipsec-route, on page 319
• ip route, on page 321
• ip secondary-address, on page 323
• ipsec, on page 325
• ipsec, on page 326
• iptables-enable, on page 327
• ipv6 address, on page 328
• ipv6 dhcp-client, on page 330
• ipv6 route, on page 332
• join-group, on page 334
• join-prune-interval, on page 336
• keepalive, on page 338
• last-resort-circuit, on page 340
• lease-time, on page 342
• lists, on page 344
• local-interface-list, on page 353
• location, on page 354
• location, on page 356
• log-frequency, on page 357
• log-translations, on page 359
• logging disk, on page 361
• logging server, on page 367
• logs, on page 370
• low-bandwidth-link, on page 372
• mac-accounting, on page 373
• mac-address, on page 374
• mac-authentication-bypass, on page 375
• match, on page 377
• match, on page 380
• max-clients, on page 390
• max-control-connections, on page 392
• max-controllers, on page 394
• max-leases, on page 395
• max-macs, on page 396
• max-metric, on page 397
• max-omp-sessions, on page 399
• mgmt-security, on page 401
• mirror, on page 403
• mode, on page 405
• mtu, on page 406
• multicast-buffer-percent, on page 408
• multicast-replicator, on page 409
• name, on page 411
• name, on page 412
• nas-identifier, on page 413
• nas-ip-address, on page 415
• nat, on page 417
• nat-refresh-interval, on page 419
• natpool, on page 421
• neighbor, on page 422
• network, on page 424
• next-hop-self, on page 426
• node-type, on page 427
• nssa, on page 429
• ntp, on page 431
• offer-time, on page 434
• omp, on page 436
• options, on page 438
• organization-name, on page 440
• ospf, on page 441
• overlay-as, on page 443
• overload, on page 444
• passive-interface, on page 446
• password, on page 447
• perfect-forward-secrecy, on page 449
• pim, on page 451
• pmtu, on page 452
• policer, on page 453
Configuration Commands

- policy, on page 457
- policy ipv6, on page 464
- port-forward, on page 466
- port-hop, on page 468
- port-offset, on page 470
- ppp, on page 472
- pppoe-client, on page 474
- priority, on page 476
- profile, on page 478
- profile, on page 481
- propagate-aspath, on page 483
- qos-map, on page 484
- qos-scheduler, on page 486
- radius, on page 488
- radius-servers, on page 492
- range, on page 496
- reauthentication, on page 497
- redistribute, on page 499
- refresh, on page 501
- rekey, on page 503
- rekey, on page 505
- remote-as, on page 507
- replay-window, on page 508
- replay-window, on page 509
- replicator-selection, on page 510
- respond-to-ping, on page 511
- retransmit-interval, on page 513
- rewrite-rule, on page 515
- route-consistency-check, on page 517
- route-policy, on page 518
- router, on page 520
- router-id, on page 522
- router-id, on page 523
- security, on page 524
- send-community, on page 525
- send-ext-community, on page 526
- send-path-limit, on page 527
- service, on page 528
- shaping-rate, on page 530
- shutdown, on page 532
- site-id, on page 534
- sla-class, on page 535
- snmp, on page 537
- sp-organization-name, on page 538
- speed, on page 539
- spt-threshold, on page 541
• ssid, on page 542
• static, on page 544
• static-ingress-qos, on page 547
• static-lease, on page 548
• stub, on page 550
• system, on page 551
• system-ip, on page 554
• system-tunnel-mtu, on page 556
• tacacs, on page 557
• tcp-mss-adjust, on page 560
• tcp-optimization, on page 562
• tcp-optimization-enabled, on page 563
• tcp-syn-flood-limit, on page 564
• tcp-timeout, on page 566
• technology, on page 568
• template-refresh, on page 570
• timeout inactivity, on page 572
• timer, on page 574
• timers, on page 576
• timers, on page 578
• timers, on page 580
• tloc-extension, on page 583
• tloc-extension-gre-from, on page 585
• tloc-extension-gre-to, on page 587
• track-default-gateway, on page 589
• track-interface-tag, on page 590
• track-transport, on page 592
• tracker, on page 593
• trap group, on page 596
• trap target, on page 599
• tunnel-destination, on page 601
• tunnel-destination, on page 603
• tunnel-interface, on page 605
• tunnel-source, on page 607
• tunnel-source, on page 608
• tunnel-source-interface, on page 610
• tunnel-source-interface, on page 611
• udp-timeout, on page 612
• update-source, on page 614
• upgrade-confirm, on page 616
• usb-controller, on page 618
• user, on page 619
• user, on page 621
• usergroup, on page 624
• vbond, on page 626
• vbond-as-stun-server, on page 629
• view, on page 631
• vlan, on page 633
• vmanage-connection-preference, on page 634
• vpn, on page 636
• vpn-membership, on page 640
• vrrp, on page 642
• wake-on-lan, on page 645
• wlan, on page 646
• wpa-personal-key, on page 648
• zone, on page 650
• zone-based-policy, on page 652
• zone-pair, on page 654
• zone-to-nozone-internet, on page 656
# Configuration Commands

## Overview of Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system aaa</td>
<td>Configure role-based access to a Cisco vEdge device using authentication, authorization, and accounting.</td>
</tr>
<tr>
<td>access-list</td>
<td>Configure or apply an IPv4 access list.</td>
</tr>
<tr>
<td>policy access-list</td>
<td>Configure or apply an IPv4 access list.</td>
</tr>
<tr>
<td>vpn interface access-list</td>
<td>Configure or apply an IPv4 access list.</td>
</tr>
<tr>
<td>policy ipv6 access-list</td>
<td>Configure or apply an IPv6 access list.</td>
</tr>
<tr>
<td>vpn interface access-list</td>
<td>Configure or apply an IPv6 access list.</td>
</tr>
<tr>
<td>accounting-interval</td>
<td>How often to send interim accounting updates during an 802.1X session.</td>
</tr>
<tr>
<td>acct-req-attr</td>
<td>Configure that accounting attributes to send to the RADIUS accounting server during an 802.1X session.</td>
</tr>
<tr>
<td>action</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>policy app-route-policy</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>policy control-policy</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>policy route-policy</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>policy data-policy</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>policy vpn-list sequence</td>
<td>Configure the actions to take when the match portion of an IPv4 policy is met.</td>
</tr>
<tr>
<td>action</td>
<td>Configure the actions to take when the match portion of an IPv6 policy is met.</td>
</tr>
<tr>
<td>address-family</td>
<td>Configure global and per-neighbor BGP address family information.</td>
</tr>
<tr>
<td>vpn router bgp address-family</td>
<td>Configure global and per-neighbor BGP address family information.</td>
</tr>
<tr>
<td>address-pool</td>
<td>Configure the pool of addresses in the service-site network for which the interface acts as DHCP server.</td>
</tr>
<tr>
<td>admin-auth-order</td>
<td>Have the &quot;admin&quot; user use the authentication order configured in the auth-order command.</td>
</tr>
<tr>
<td>admin-state</td>
<td>Enable or disable the DHCP server functionality on the interface.</td>
</tr>
<tr>
<td>admin-tech-on-failure</td>
<td>When a Cisco vEdge device reboots, collect system status information.</td>
</tr>
<tr>
<td>advertise</td>
<td>Advertise routes learned locally by the vEdge router to OMP.</td>
</tr>
<tr>
<td>age-time</td>
<td>Configure when MAC table entries age out.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>allow-local-exit</td>
<td>vpn clouddexpress allow-local-exit—Configure Cloud OnRamp for SaaS to use an interface with Direct Internet Access (DIA).</td>
</tr>
<tr>
<td>allow-same-site-tunnels</td>
<td>system allow-same-site-tunnels—Allow tunnels to be formed between vEdge routers in the same site.</td>
</tr>
<tr>
<td>allow-service</td>
<td>vpn 0 interface tunnel-interface 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.</td>
</tr>
<tr>
<td>app-route-policy</td>
<td>policy app-route-policy—Configure or apply an application-aware routing policy.</td>
</tr>
<tr>
<td>app-visibility</td>
<td>policy app-visibility—Enable application visibility so that a vEdge router can monitor and track the applications running on the LAN.</td>
</tr>
<tr>
<td>applications</td>
<td>vpn clouddexpress applications—Configure applications for which to enable Cloud OnRamp for SaaS.</td>
</tr>
<tr>
<td>apply-policy</td>
<td>apply-policy—Have a policy take effect by applying it to sites within the overlay network.</td>
</tr>
<tr>
<td>archive</td>
<td>system archive—Periodically archive a copy of the full running configuration to an archival file.</td>
</tr>
<tr>
<td>area</td>
<td>vpn router ospf area—Configure an OSPF area within a VPN on a vEdge router.</td>
</tr>
<tr>
<td>arp</td>
<td>vpn interface arp—Configure an ARP table entry for an interface in a VPN.</td>
</tr>
<tr>
<td>arp-timeout</td>
<td>vpn interface arp-timeout—Configure how long it takes for a dynamically learned ARP entry to time out.</td>
</tr>
<tr>
<td>auth-fail-vlan</td>
<td>vpn interface dot1x auth-fail-vlan—Configure a critical VLAN on an interface running IEEE 802.1X.</td>
</tr>
<tr>
<td>auth-fallback</td>
<td>auth-fallback—Configure authentication to fall back to the next authentication method if a higher-priority authentication method fails.</td>
</tr>
<tr>
<td>auth-order</td>
<td>system aaa auth-order—Configure the order in which the Cisco SD-WAN software tries different authentication methods when verifying user access to a Cisco vEdge device.vpn interface dot1x 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 a WAN.</td>
</tr>
<tr>
<td>auth-order</td>
<td>vpn interface dot1x 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 a WAN.</td>
</tr>
<tr>
<td>auth-reject-vlan</td>
<td>vpn interface dot1x auth-reject-vlan—Configure an authentication-reject VLAN to place IEEE 802.1X-enabled clients into if authentication is rejected by the RADIUS server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auth-req-attr</td>
<td>Configure RADIUS authentication attribute-value (AV) pairs to send to the RADIUS accounting server during an 802.1X session.</td>
</tr>
<tr>
<td>authentication</td>
<td>Configure authentication for OSPF protocol exchanges.</td>
</tr>
<tr>
<td>authentication-type</td>
<td>Configure the type of authentication to use during IKE key exchange.</td>
</tr>
<tr>
<td>auto-cost reference-bandwidth</td>
<td>Control how OSPF calculates the default metric for an interface.</td>
</tr>
<tr>
<td>auto-rp</td>
<td>Enable and disable auto-RP for PIM.</td>
</tr>
<tr>
<td>autonegotiate</td>
<td>Configure whether an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>bandwidth-downstream</td>
<td>Generate notifications when the bandwidth of traffic received on a physical interface in the WAN transport VPN exceeds a specific limit.</td>
</tr>
<tr>
<td>bandwidth-upstream</td>
<td>Generate notifications when the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN exceeds a specific limit.</td>
</tr>
<tr>
<td>banner login</td>
<td>Configure banner text to be displayed before the login prompt.</td>
</tr>
<tr>
<td>banner motd</td>
<td>Configure banner text to be displayed after a user logs in to a Cisco vEdge device.</td>
</tr>
<tr>
<td>best-path</td>
<td>Configure how the active BGP path is selected.</td>
</tr>
<tr>
<td>bfd app-route</td>
<td>Configure the Bidirectional Forwarding Protocol timers used by application-aware routing.</td>
</tr>
<tr>
<td>bfd color</td>
<td>Configure the Bidirectional Forwarding Protocol timers used on transport tunnels.</td>
</tr>
<tr>
<td>bgp</td>
<td>Configure BGP within a VPN on a vEdge router.</td>
</tr>
<tr>
<td>bind</td>
<td>Bind a physical WAN interface to a loopback interface.</td>
</tr>
<tr>
<td>block-icmp-error</td>
<td>Prevent a vEdge router that is acting as a NAT device from receiving inbound ICMP error messages.</td>
</tr>
<tr>
<td>block-non-source-ip</td>
<td>Do not allow an interface to forward traffic if the source IP address of the traffic does not match the IP prefix range.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bridge</td>
<td>bridge—Create a bridging domain.</td>
</tr>
<tr>
<td>capability-negotiate</td>
<td>vpn router bgp capability-negotiate—Allow the BGP session to learn about the BGP extensions that are supported by the neighbor.</td>
</tr>
<tr>
<td>carrier</td>
<td>vpn 0 interface tunnel-interface carrier—Associate a carrier name or private network identifier with a tunnel interface.</td>
</tr>
<tr>
<td>cellular</td>
<td>cellular—Configure a cellular module.</td>
</tr>
<tr>
<td>cflowd-template</td>
<td>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.</td>
</tr>
<tr>
<td>channel</td>
<td>wlan channel—Specify the radio channel.</td>
</tr>
<tr>
<td>channel-bandwidth</td>
<td>wlan channel-bandwidth—Specify the IEEE 802.11n and 802.11ac channel bandwidth.</td>
</tr>
<tr>
<td>cipher-suite</td>
<td>vpn interface ipsec ike cipher-suite, vpn interface ipsec ipsec cipher-suite—Configure the type of authentication and integrity to use during IKE key exchange and on the IPsec tunnel being used for IKE key exchange.</td>
</tr>
<tr>
<td>class-map</td>
<td>class-map—Map forwarding classes to output queues.</td>
</tr>
<tr>
<td>clear-dont-fragment</td>
<td>vpn interface clear-dont-fragment—Clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface.</td>
</tr>
<tr>
<td>clock</td>
<td>system clock—Set the timezone to use on the local device.</td>
</tr>
<tr>
<td>cloud-qos</td>
<td>policy cloud-qos—Enable QoS scheduling and shaping for traffic that the router receives from transport-side interfaces.</td>
</tr>
<tr>
<td>cloud-qos-service-side</td>
<td>policy cloud-qos-service-side—Enable QoS scheduling and shaping for traffic that the router receives from service-side interfaces.</td>
</tr>
<tr>
<td>cloudexpress</td>
<td>vpn cloudexpress—Configure Cloud OnRamp for SaaS in a VPN.</td>
</tr>
<tr>
<td>collector</td>
<td>policy cflowd-template collector—Configure the address of a cflowd collector (on vSmart controllers only).</td>
</tr>
<tr>
<td>color</td>
<td>vpn 0 interface tunnel-interface color—Identify an individual WAN transport tunnel.</td>
</tr>
<tr>
<td>community</td>
<td>snmp community—Define an SNMP community.</td>
</tr>
<tr>
<td>compatible rfc1583</td>
<td>vpn router ospf compatible rfc1583—Calculate the cost of summary routes based on RFC 1583 rather than RFC 2328.</td>
</tr>
<tr>
<td>connections-limit</td>
<td>vpn 0 interface tunnel-interface connections-limit—Configure the maximum number of HTTPS connections that can be established to a vManage application server.</td>
</tr>
<tr>
<td>console-baud-rate</td>
<td>system console-baud-rate—Change the baud rate of the console connection on a vEdge router.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>contact</td>
<td>Configure the name of a network management contact person for this Cisco vEdge device.</td>
</tr>
<tr>
<td>container</td>
<td>Configure a vSmart controller as a container with a vContainer host.</td>
</tr>
<tr>
<td>control</td>
<td>Configure the protocol to use on control-plane connections to a vSmart controller.</td>
</tr>
<tr>
<td>control-connections</td>
<td>Attempt to establish a DTLS or TLS control connection for a TLOC.</td>
</tr>
<tr>
<td>control-direction</td>
<td>Configure how the 802.1x interface sends packets to and receive packets from unauthorized hosts.</td>
</tr>
<tr>
<td>control-policy</td>
<td>Configure or apply a centralized control policy.</td>
</tr>
<tr>
<td>control-session-pps</td>
<td>Police the flow of DTLS control session traffic.</td>
</tr>
<tr>
<td>controller-group-id</td>
<td>Configure the identifier of the controller group to which a vSmart controller belongs.</td>
</tr>
<tr>
<td>controller-group-list</td>
<td>List of controller groups to which the vEdge router belongs.</td>
</tr>
<tr>
<td>cost</td>
<td>Configure the cost of an OSPF interface.</td>
</tr>
<tr>
<td>country</td>
<td>Specify the country for the WLAN.</td>
</tr>
<tr>
<td>das</td>
<td>Configure DAS parameters so the router can accept CoA request from a RADIUS server.</td>
</tr>
<tr>
<td>data-policy</td>
<td>Configure or apply a centralized data policy based on data packet header fields.</td>
</tr>
<tr>
<td>data-security</td>
<td>Configure the WPA data security method to use an IEEE 802.11i wireless LAN.</td>
</tr>
<tr>
<td>dead-interval</td>
<td>Set the interval during which at least one OSPF hello packet must be received from a neighbor before declaring that neighbor to be down.</td>
</tr>
<tr>
<td>dead-peer-detection</td>
<td>Configure the parameters for detecting unreachable IKE peers.</td>
</tr>
<tr>
<td>default-action</td>
<td>Configure the default action to take when the match portion of a policy is not met.</td>
</tr>
<tr>
<td>default-information originate</td>
<td>Generate a default external route into an OSPF routing domain.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>default-vlan</td>
<td>Configure the VLAN for 802.1X-compliant clients that are successfully authenticated by the RADIUS server.</td>
</tr>
<tr>
<td>description</td>
<td>Configure a text description for a parameter or property.</td>
</tr>
<tr>
<td>device-groups</td>
<td>Configure one or more groups to which the Cisco vEdge device belongs.</td>
</tr>
<tr>
<td>dhcp-helper</td>
<td>Allow an interface to act as a DHCP helper.</td>
</tr>
<tr>
<td>dhcp-server</td>
<td>Enable DHCP server functionality on a vEdge router so it can assign IP addresses to hosts in the service-side network.</td>
</tr>
<tr>
<td>direction</td>
<td>Configure the direction in which a NAT interface performs address translation.</td>
</tr>
<tr>
<td>discard-rejected</td>
<td>Have OMP discard routes that have been rejected on the basis of policy.</td>
</tr>
<tr>
<td>distance</td>
<td>Define the BGP route administrative distance based on route type.</td>
</tr>
<tr>
<td>domain-id</td>
<td>Configure the identifier for the Cisco SD-WAN overlay network domain.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configure port-level 802.1X parameters on a router interface.</td>
</tr>
<tr>
<td>duplex</td>
<td>Configure whether the interface runs in full-duplex or half-duplex mode.</td>
</tr>
<tr>
<td>ebgp-multihop</td>
<td>Attempt BGP connections to and accept BGP connections from external peers on networks that are not directly connected to this network.</td>
</tr>
<tr>
<td>ecmp-hash-key</td>
<td>Determine how equal-cost paths are chosen.</td>
</tr>
<tr>
<td>ecmp-limit</td>
<td>Configure the maximum number of OMP paths that can be installed in the vEdge router's route table.</td>
</tr>
<tr>
<td>eco-friendly-mode</td>
<td>Configure a vEdge router not to use its CPU minimally or not at all when the router is not processing any packets.</td>
</tr>
<tr>
<td>encapsulation</td>
<td>Set the encapsulation for the tunnel interface.</td>
</tr>
<tr>
<td>exclude</td>
<td>Exclude specific addresses from the pool of addresses for which the interface acts as DHCP server.</td>
</tr>
<tr>
<td>Configuration Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exclude-controller-group-list</td>
<td>Configure the vSmart controllers that the tunnel interface is not allowed to connect to.</td>
</tr>
<tr>
<td>flow-active-timeout</td>
<td>For a cflowd template, how long to collect a set of flows for a flow on which traffic is actively flowing.</td>
</tr>
<tr>
<td>flow-control</td>
<td>Configure flow control, which is a mechanism for temporarily stopping the transmission of data on the interface.</td>
</tr>
<tr>
<td>flow-inactive-timeout</td>
<td>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.</td>
</tr>
<tr>
<td>flow-sampling-interval</td>
<td>For a cflowd template, how many packets to wait before creating a new flow.</td>
</tr>
<tr>
<td>flow-visibility</td>
<td>Enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN.</td>
</tr>
<tr>
<td>gps-location</td>
<td>Set the latitude and longitude of the Cisco vEdge device.</td>
</tr>
<tr>
<td>graceful-restart</td>
<td>Control graceful restart for OMP.</td>
</tr>
<tr>
<td>group</td>
<td>Configure the group number for an IKEv1 session.</td>
</tr>
<tr>
<td>group</td>
<td>Configure an SNMPv3 group.</td>
</tr>
<tr>
<td>guard-interval</td>
<td>Configure the amount of time between symbol transmissions on a wireless WAN.</td>
</tr>
<tr>
<td>guest-vlan</td>
<td>Configure a guest VLAN to provide network access to limited services for non-802.1X-enabled clients.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Set the interval at which the router sends OSPF hello packets. Modify the PIM hello message interval for an interface. Configure the interval between Hello packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Modify the PIM hello message interval for an interface. Configure the interval between Hello packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Configure the interval between Hello packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td>hello-tolerance</td>
<td>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.</td>
</tr>
<tr>
<td>Configuration Commands</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>host</strong></td>
<td><strong>vpn host</strong>—Configure a static mapping between a hostname and an IP address.</td>
</tr>
<tr>
<td><strong>host-mode</strong></td>
<td><strong>vpn interface dot1x host-mode</strong>—Set whether the 802.1X interface grants access to a single client or to multiple clients.</td>
</tr>
<tr>
<td><strong>host-name</strong></td>
<td><strong>system host-name</strong>—Configure a name for the Cisco vEdge device, to be prepended to the device's shell prompt.</td>
</tr>
<tr>
<td><strong>host-policer-pps</strong></td>
<td><strong>system host-policer-pps</strong>—For a policer, configure the rate to deliver packets to the control plane.</td>
</tr>
<tr>
<td><strong>icmp-error-pps</strong></td>
<td><strong>system icmp-error-pps</strong>—For a policer, configure how many ICMP error messages can be generated per second.</td>
</tr>
<tr>
<td><strong>icmp-redirect-disable</strong></td>
<td><strong>vpn interface icmp-redirect-disable</strong>—Disable ICMP redirect message on an interface.</td>
</tr>
<tr>
<td><strong>idle-timeout</strong></td>
<td>Set how long the CLI is inactive before the user is logged out.</td>
</tr>
<tr>
<td><strong>igmp</strong></td>
<td><strong>vpn router igmp</strong>—Configure IGMP.</td>
</tr>
<tr>
<td><strong>ike</strong></td>
<td><strong>vpn interface ipsec ike</strong>—Configure the Internet Key protocol for use on an IPsec tunnel.</td>
</tr>
<tr>
<td><strong>implicit-acl/logging</strong></td>
<td><strong>policy implicit-acl/logging</strong>—Log all flows that are not explicitly configured with an allow-services command.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td><strong>bridge interface</strong>—Associate an interface with a bridging domain. <strong>vpn router igmp interface</strong>—Configure the interfaces that participate in the IGMP domain, and configure the groups for the interface to join. <strong>vpn router pim interface</strong>—Configure the interfaces that participate in the PIM domain, and configure PIM timers for the interfaces. <strong>vpn interface</strong>—Configure an interface within a VPN. <strong>wlan interface</strong>—Configure virtual access points (VAPs) for an IEEE 802.11i wireless LAN. <strong>vpn router ospf area interface</strong>—Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td><strong>vpn router igmp interface</strong>—Configure the interfaces that participate in the IGMP domain, and configure the groups for the interface to join. <strong>vpn router pim interface</strong>—Configure the interfaces that participate in the PIM domain, and configure PIM timers for the interfaces. <strong>vpn interface</strong>—Configure an interface within a VPN. <strong>wlan interface</strong>—Configure virtual access points (VAPs) for an IEEE 802.11i wireless LAN. <strong>vpn router ospf area interface</strong>—Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td><strong>vpn router pim interface</strong>—Configure the interfaces that participate in the PIM domain, and configure PIM timers for the interfaces. <strong>vpn interface</strong>—Configure an interface within a VPN. <strong>wlan interface</strong>—Configure virtual access points (VAPs) for an IEEE 802.11i wireless LAN. <strong>vpn router ospf area interface</strong>—Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td><strong>vpn interface</strong>—Configure an interface within a VPN. <strong>wlan interface</strong>—Configure virtual access points (VAPs) for an IEEE 802.11i wireless LAN. <strong>vpn router ospf area interface</strong>—Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>wlan interface</td>
<td>Configure virtual access points (VAPs) for an IEEE 802.11i wireless LAN.</td>
</tr>
<tr>
<td>vpn router ospf area</td>
<td>Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td>gre</td>
<td>Configure a GRE tunnel interface interface in the transport VPN.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Configure IKE parameters for IPsec tunnels.</td>
</tr>
<tr>
<td>irb</td>
<td>Configure an interface to use for integrated routing and bridging (IRB).</td>
</tr>
<tr>
<td>ospf area</td>
<td>Configure the properties of an interface in an OSPF area.</td>
</tr>
<tr>
<td>ppp</td>
<td>Configure the Point-to-Point Protocol over Ethernet (PPPoE).</td>
</tr>
<tr>
<td>ipsec</td>
<td>Configure the IPsec tunnel to use for IKE key exchange.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Configure parameters for IPsec tunnel connections.</td>
</tr>
<tr>
<td>iptables-enable</td>
<td>Enable the collection of iptable packet-filtering chains for all DTLS peers.</td>
</tr>
<tr>
<td>ip address</td>
<td>Configure an interface's IPv4 address.</td>
</tr>
<tr>
<td>dhcp-client</td>
<td>Configure an interface in VPN 0 to receive its IPv4 address from a DHCP server.</td>
</tr>
<tr>
<td>ip route</td>
<td>Configure an IPv4 static route in a VPN.</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>Configure a static IPv6 address IPv6 on an interface.</td>
</tr>
<tr>
<td>dhcp-client</td>
<td>Configure an interface in the WAN transport VPN (VPN 0) to receive its IPv6 address from a DHCPv6 server.</td>
</tr>
<tr>
<td>ipv6 route</td>
<td>Configure an IPv6 static route in a VPN.</td>
</tr>
<tr>
<td>address-list</td>
<td>Configure the IP addresses reachable by the interfaces on a container.</td>
</tr>
<tr>
<td>gre-route</td>
<td>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.</td>
</tr>
<tr>
<td>ipsec-route</td>
<td>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.</td>
</tr>
<tr>
<td>secondary-address</td>
<td>Configure secondary IPv4 addresses for a service-side interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>join-group</code></td>
<td>Configure an interface on the vEdge router to initiate a request to join a multicast group.</td>
</tr>
<tr>
<td><code>join-prune-interval</code></td>
<td>Modify the PIM join/prune message interval for an interface.</td>
</tr>
<tr>
<td><code>keepalive</code></td>
<td>Configure how often a GRE interface sends keepalive packets.</td>
</tr>
<tr>
<td><code>last-resort-circuit</code></td>
<td>Use this tunnel interface as the gateway of last resort.</td>
</tr>
<tr>
<td><code>lease-time</code></td>
<td>Configure the time period for which a DHCP-assigned IP address is valid.</td>
</tr>
<tr>
<td><code>lists</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>local-interface-list</code></td>
<td>Configure Direct Internet Access (DIA) interfaces for Cloud OnRamp for SaaS.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Configure a text string that describes the location of the device.</td>
</tr>
<tr>
<td><code>log-freQUENCY</code></td>
<td>Configure how often packet flows are logged.</td>
</tr>
<tr>
<td><code>log-translations</code></td>
<td>Log the creation and deletion of NAT flows.</td>
</tr>
<tr>
<td><code>logging disk</code></td>
<td>Log event notification system log (syslog) messages to a file on the local device's hard disk.</td>
</tr>
<tr>
<td><code>logging server</code></td>
<td>Log event notification system logging (syslog) messages to a remote host.</td>
</tr>
<tr>
<td><code>logs</code></td>
<td>Configure the logging of AAA and Netconf system logging (syslog) messages.</td>
</tr>
<tr>
<td><code>low-bandwidth-link</code></td>
<td>Characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td><code>mac-accounting</code></td>
<td>Generate accounting information for IP traffic.</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>Configure a MAC address to associate with the interface in the VPN.</td>
</tr>
<tr>
<td><code>mac-authentication-bypass</code></td>
<td>Authorize clients based on the client's MAC address when IEEE 802.1X authentication times out.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>match</td>
<td>Define the properties that must be matched so that an IPv4 policy action can take effect.</td>
</tr>
<tr>
<td>policy ipv6 access-list sequence match</td>
<td>Define the properties that must be matched so that an IPv6 policy action can take effect.</td>
</tr>
<tr>
<td>max-clients</td>
<td>Configure the maximum number of clients allowed to connect to the wireless LAN.</td>
</tr>
<tr>
<td>max-control-connections</td>
<td>Configure the maximum number of vSmart controllers that the WAN tunnel interface can connect to.</td>
</tr>
<tr>
<td>max-controllers</td>
<td>Configure the maximum number of vSmart controllers that the vEdge router is allowed to connect to.</td>
</tr>
<tr>
<td>max-leases</td>
<td>Configure the maximum number of IP addresses that can be assigned.</td>
</tr>
<tr>
<td>max-macs</td>
<td>Set the maximum number of MAC addresses that a bridging domain can learn.</td>
</tr>
<tr>
<td>max-metric</td>
<td>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 calculation.</td>
</tr>
<tr>
<td>max-omp-sessions</td>
<td>Configure the maximum number of OMP sessions that a vEdge router can establish to vSmart controllers.</td>
</tr>
<tr>
<td>mgmt-security</td>
<td>Configure the encryption of management frames sent on the wireless LAN.</td>
</tr>
<tr>
<td>mirror</td>
<td>Configure or apply a mirror to copy data packets to a specified destination for analysis.</td>
</tr>
<tr>
<td>mode</td>
<td>Configure the mode to use in IKEv1 Diffie-Hellman key exchanges.</td>
</tr>
<tr>
<td>mtu</td>
<td>Set the maximum MTU size of packets on an interface.</td>
</tr>
<tr>
<td>multicast-buffer-percent</td>
<td>Configure the amount of interface bandwidth that multicast traffic can use.</td>
</tr>
<tr>
<td>multicast-replicator</td>
<td>Configure a vEdge router to be a multicast replicator.</td>
</tr>
<tr>
<td>name</td>
<td>Provide a text name for the Cisco vEdge device.</td>
</tr>
<tr>
<td>name</td>
<td>Provide a text description for the VPN.</td>
</tr>
<tr>
<td>nas-identifier</td>
<td>Configure the NAS identifier of the local router, to send to the RADIUS server during an 802.1X session.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>nas-ip-address</td>
<td>vpn interface dot1x nas-identifier—Configure the NAS IP address of the local router, to send to the RADIUS server during an 802.1X session.</td>
</tr>
<tr>
<td>nat</td>
<td>vpn interface nat—Configure a vEdge router to act as a NAT device.</td>
</tr>
<tr>
<td>nat-refresh-interval</td>
<td>vpn 0 interface tunnel-interface nat-refresh-interval—Configure the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td>natpool</td>
<td>vpn interface nat natpool—Configure a pool of addresses to use in NAT translation.</td>
</tr>
<tr>
<td>neighbor</td>
<td>vpn router bgp neighbor—Configure a BGP neighbor.</td>
</tr>
<tr>
<td>network</td>
<td>vpn router ospf area interface network—Set the OSPF network type.</td>
</tr>
<tr>
<td>next-hop-self</td>
<td>vpn router bgp neighbor next-hop-self—Configure the router to be the next hop to the BGP neighbor.</td>
</tr>
<tr>
<td>node-type</td>
<td>vpn cloudexpress node-type—Configure a node type for Cloud OnRamp for SaaS.</td>
</tr>
<tr>
<td>nssa</td>
<td>vpn router ospf area nssa—Configure an OSPF area to be an NSSA (a not-so-stubby area).</td>
</tr>
<tr>
<td>ntp</td>
<td>system ntp—Configure Network Time Protocol (NTP) servers and MD5 authentication keys for the servers.</td>
</tr>
<tr>
<td>offer-time</td>
<td>vpn interface dhcp-server offer-time—Configure how long the IP address offered to a DHCP client is reserved for that client.</td>
</tr>
<tr>
<td>omp</td>
<td>omp, vpn omp—Modify the OMP configuration.</td>
</tr>
<tr>
<td>options</td>
<td>vpn interface dhcp-server options—Configure the DHCP options to send to the client when the DHCP client request them.</td>
</tr>
<tr>
<td>organization-name</td>
<td>system organization-name—Configure the name of your organization.</td>
</tr>
<tr>
<td>ospf</td>
<td>vpn router ospf—Configure OSPF within a VPN on a vEdge router.</td>
</tr>
<tr>
<td>overlay-as</td>
<td>omp overlay-as—Configure a BGP AS number that OMP advertises to the router's BGP neighbors.</td>
</tr>
<tr>
<td>overload</td>
<td>vpn interface nat overload—Control the mapping of addresses on a vEdge router that is acting as a NAT device.</td>
</tr>
<tr>
<td>passive-interface</td>
<td>vpn router ospf area interface passive-interface—Set the OSPF interface to be passive.</td>
</tr>
<tr>
<td>password</td>
<td>vpn router bgp neighbor password—Configure message digest5 (MD5) authentication and an MD5 password on the TCP connection with the BGP peer.</td>
</tr>
<tr>
<td>perfect-forward-secrecy</td>
<td>vpn interface ipsec ipsec perfect-forward-secrecy—Configure the PFS settings to use on an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>pim</code></td>
<td>vpn router pim—Configure PIM.</td>
</tr>
<tr>
<td><code>pimtu</code></td>
<td>vpn interface pimtu—Enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.</td>
</tr>
<tr>
<td><code>policer</code></td>
<td>policy policer—Configure or apply a policer to be used for data traffic.</td>
</tr>
<tr>
<td><code>policy</code></td>
<td>policy—Configure IPv4 policy.</td>
</tr>
<tr>
<td><code>policy ipv6</code></td>
<td>policy ipv6—Configure IPv6 policy.</td>
</tr>
<tr>
<td><code>port-forward</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>port-hop</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>port-offset</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>ppp</code></td>
<td>vpn 0 interface ppp—Configure the Point-to-Point Protocol properties associated with a PPPoE virtual interface.</td>
</tr>
<tr>
<td><code>pppoe-client</code></td>
<td>vpn interface pppoe-client—Enable a PPPoE client on an interface.</td>
</tr>
<tr>
<td><code>priority</code></td>
<td>vpn router ospf area interface priority—Set the priority of the router to be elected as the designated router.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>cellular profile—Add, modify, or delete a cellular profile. vpn 0 interface cellular profile—Configure the profile assigned to a cellular interface.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>vpn 0 interface cellular profile—Configure the profile assigned to a cellular interface.</td>
</tr>
<tr>
<td><code>propagate-aspath</code></td>
<td>vpn router bgp propagate-aspath—Carry the BGP AS path into OMP.</td>
</tr>
<tr>
<td><code>qos-map</code></td>
<td>qos-map—Configure a QoS map or apply one on an interface.</td>
</tr>
<tr>
<td><code>qos-scheduler</code></td>
<td>policy qos-scheduler—Configure a QoS scheduler for a forwarding class.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>radius-servers</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>range</code></td>
<td>vpn router ospf area range—Summarize OSPF areas at an area boundary so that only a single summary router is advertised to other areas by an ABR.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reauthentication</td>
<td>Configure the reauthentication of 802.1X clients.</td>
</tr>
<tr>
<td>redistribute</td>
<td>Redistribute routes learned from other protocols into OSPF.</td>
</tr>
<tr>
<td>refresh</td>
<td>Configure how NAT mappings are refreshed.</td>
</tr>
<tr>
<td>rekey</td>
<td>Modify the IPsec rekeying timer to use during IKE key exchanges or on the IPsec tunnel being used for IKE key exchange.</td>
</tr>
<tr>
<td>remote-as</td>
<td>Configure AS number of the remote peer.</td>
</tr>
<tr>
<td>replay-window</td>
<td>Modify the size of the IPsec replay window on an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>replicator-selection</td>
<td>Allow vEdge routers to use different replicators for the same multicast group.</td>
</tr>
<tr>
<td>respond-to-ping</td>
<td>Have a vEdge router that is acting as a NAT device respond to ping requests received from the public side of the connection.</td>
</tr>
<tr>
<td>retransmit-interval</td>
<td>Set the interval at which the router retransmits OSPF link-state advertisements to its adjacencies.</td>
</tr>
<tr>
<td>rewrite-rule</td>
<td>Configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header, or apply a rewrite rule on an interface.</td>
</tr>
<tr>
<td>route-consistency-check</td>
<td>Check whether the IPv4 routes in the device's route and forwarding table are consistent.</td>
</tr>
<tr>
<td>route-policy</td>
<td>Configure or apply a localized control policy.</td>
</tr>
<tr>
<td>router</td>
<td>Configure the BGP, OSPF, and PIM routing protocol to run in a VPN.</td>
</tr>
<tr>
<td>router-id</td>
<td>Configure the BGP router ID, which is the IP address associated with the router for BGP sessions.</td>
</tr>
<tr>
<td></td>
<td>Configure the OSPF router ID, which is the IP address associated with the router for OSPF adjacencies.</td>
</tr>
<tr>
<td>security</td>
<td>Configure security parameters.</td>
</tr>
<tr>
<td>Configuration Commands</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>send-backup-paths</td>
<td>om -p send-backup-paths—Have OMP send backup routes to vEdge routers (on vSmart controllers only). By default, OMP sends only the best route or routes.</td>
</tr>
<tr>
<td>send-community</td>
<td>vpn router bgp neighbor send-community—Send the local router's BGP community attribute to the BGP neighbor.</td>
</tr>
<tr>
<td>send-ext-community</td>
<td>vpn router bgp neighbor send-ext-community—Send the local router's BGP extended community attribute to the BGP neighbor.</td>
</tr>
<tr>
<td>send-path-limit</td>
<td>om -p send-path-limit—Configure the number of routes that can be advertised.</td>
</tr>
<tr>
<td>service</td>
<td>vpn service—Configure a service, such as a firewall or IDS, that is present on the local network in which the vEdge router is located.</td>
</tr>
<tr>
<td>shaping-rate</td>
<td>vpn interface 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.</td>
</tr>
<tr>
<td>shutdown</td>
<td>shutdown—Disable or enable a parameter or property.</td>
</tr>
<tr>
<td>site-id</td>
<td>system 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.</td>
</tr>
<tr>
<td>sla-class</td>
<td>policy sla-class—Create groupings of properties that identify an application for a policy to use with application-aware routing.</td>
</tr>
<tr>
<td>snmp</td>
<td>snmp—Configure the Simple Network Management Protocol.</td>
</tr>
<tr>
<td>sp-organization-name</td>
<td>system 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.</td>
</tr>
<tr>
<td>speed</td>
<td>vpn interface speed—Set the speed of the interface.</td>
</tr>
<tr>
<td>spt-threshold</td>
<td>vpn router pim spt-threshold—Configure when a PIM router should join the shortest-path source tree.</td>
</tr>
<tr>
<td>ssid</td>
<td>wlan interface ssid—Configure the service set identifier (SSID) for a WLAN.</td>
</tr>
<tr>
<td>static-ingress-qos</td>
<td>vpn interface static-ingress-qos—Allocate ingress traffic on an interface to a specific queue.</td>
</tr>
<tr>
<td>static-lease</td>
<td>vpn interface dhcp-server static-lease—Assign a static IP address to a host or other device on the service-side network.</td>
</tr>
<tr>
<td>static</td>
<td>vpn interface nat static—Configure 1:1 static NAT on a vEdge router that is acting as a NAT device.</td>
</tr>
<tr>
<td>stub</td>
<td>vpn router ospf area stub—Configure an OSPF stub area.</td>
</tr>
<tr>
<td>system</td>
<td>system—Configure system-wide parameters.</td>
</tr>
<tr>
<td>system-ip</td>
<td>system system-ip—Configure a system IP address for a Cisco vEdge device.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>system-tunnel-mtu</td>
<td>Configure the MTU to use on the DTLS tunnels that send control traffic between Cisco vEdge devices.</td>
</tr>
<tr>
<td>tacacs</td>
<td>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.</td>
</tr>
<tr>
<td>tcp-mss-adjust</td>
<td>Adjust the maximum segment size (MSS) of TCP SYN packets passing through a vEdge router.</td>
</tr>
<tr>
<td>tcp-optimization</td>
<td>Fine-tune TCP to decrease round-trip latency and improve throughput for TCP traffic.</td>
</tr>
<tr>
<td>tcp-optimization-enabled</td>
<td>Carve out a separate CPU core to use for performing TCP optimization.</td>
</tr>
<tr>
<td>tcp-syn-flood-limit</td>
<td>Configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall.</td>
</tr>
<tr>
<td>tcp-timeout</td>
<td>Configure when NAT translations over a TCP session time out.</td>
</tr>
<tr>
<td>technology</td>
<td>Assign a cellular technology to a cellular interface.</td>
</tr>
<tr>
<td>template-refresh</td>
<td>How often to send the cflowd template record fields to the collector.</td>
</tr>
<tr>
<td>timeout inactivity</td>
<td>Set how long to wait before revoking the authentication of a client that is using 802.1X to access a network.</td>
</tr>
<tr>
<td>timer</td>
<td>Configure the DNS cache timeout.</td>
</tr>
<tr>
<td>timers</td>
<td>Configure BGP timers, per-neighbor BGP timers, OMP timers, OSPF timers, and OSPF timers.</td>
</tr>
<tr>
<td>timers</td>
<td>Configure OMP timers on vEdge routers and vSmart controllers.</td>
</tr>
<tr>
<td>timers</td>
<td>Configure OSPF timers.</td>
</tr>
<tr>
<td>tloc-extension</td>
<td>Bind this interface, which connects to another vEdge router at the same site, to the local router's WAN transport interface.</td>
</tr>
<tr>
<td>tloc-extension-gre-from</td>
<td>Configure an interface as an extended interface channeling the TLOC traffic from the source branch router to the local WAN interface.</td>
</tr>
<tr>
<td>tloc-extension-gre-to</td>
<td>Configure a tunnel-interface with the tloc-extension-gre-to service.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>track-default-gateway</td>
<td>For a static route, determine whether the next hop is reachable before adding that route to the device's route table.</td>
</tr>
<tr>
<td>track-interface-tag</td>
<td>system track-interface-tag—Configure a tag to apply to routes associated with a network that is connected to a non-operational interface</td>
</tr>
<tr>
<td>track-transport</td>
<td>system track-transport—Regularly check whether the DTLS connection between the local device and a vBond orchestrator is up.</td>
</tr>
<tr>
<td>tracker</td>
<td>system tracker, vpn 0 interface tracker—Track the status of transport interfaces the connect to the internet.</td>
</tr>
<tr>
<td>trap group</td>
<td>snmp trap group—Configure SNMP trap groups.</td>
</tr>
<tr>
<td>trap target</td>
<td>snmp trap target—Configure the target SNMP server to receive the SNMP traps generated by this device.</td>
</tr>
<tr>
<td>tunnel-destination</td>
<td>vpn interface gre tunnel-destination—Configure the destination IP address of a GRE tunnel interface.vpn interface ipsec tunnel-destination—Configure the destination IP address of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>tunnel-destination</td>
<td>vpn interface ipsec tunnel-destination—Configure the destination IP address of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>tunnel-interface</td>
<td>vpn interface tunnel-interface—Configure the interface to be a secure DTLS WAN transport connection.</td>
</tr>
<tr>
<td>tunnel-source</td>
<td>vpn interface gre tunnel-source—Configure the source IP address of a GRE tunnel interface.vpn interface ipsec tunnel-source—Configure the source IP address of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>tunnel-source-interface</td>
<td>vpn interface gre tunnel-source-interface—Configure the physical interface that is the source of a GRE tunnel.vpn interface ipsec tunnel-source-interface—Configure the physical interface that is the source IP interface of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>tunnel-source-interface</td>
<td>vpn interface ipsec tunnel-source-interface—Configure the physical interface that is the source IP interface of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>tunnel-source</td>
<td>vpn interface ipsec tunnel-source—Configure the source IP address of an IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>udp-timeout</td>
<td>vpn interface nat udp-timeout—Configure when NAT translations over a UDP session time out.</td>
</tr>
<tr>
<td>update-source</td>
<td>vpn router bgp neighbor update-source—Allow BGP to use a specific IP address or interface for the TCP connection to the neighbor.</td>
</tr>
<tr>
<td>upgrade-confirm</td>
<td>system upgrade-confirm—Configure the time limit for confirming that a software upgrade is successful.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>system usb-controller</td>
<td>Enable or disable the USB controller, which drives the external USB ports.</td>
</tr>
<tr>
<td>system aaa user</td>
<td>Configure a login account for each user who can access the local Cisco vEdge device.</td>
</tr>
<tr>
<td>snmp group</td>
<td>Configure an SNMPv3 user.</td>
</tr>
<tr>
<td>system aaa usergroup</td>
<td>Configure groupings of users and assign authorization privileges to the group.</td>
</tr>
<tr>
<td>system vbond</td>
<td>Configure the IP address and other information related to the vBond orchestrator.</td>
</tr>
<tr>
<td>vpn 0 interface tunnel-interface vbond-as-stun-server</td>
<td>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.</td>
</tr>
<tr>
<td>snmp view</td>
<td>Define an SNMP MIB view.</td>
</tr>
<tr>
<td>bridge vlan</td>
<td>Set the tag to use as the VLAN ID for the bridging domain.</td>
</tr>
<tr>
<td>vmanage-connection-preference</td>
<td>Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.</td>
</tr>
<tr>
<td>vpn</td>
<td>Configure VPNs to use for segmentation of the Cisco SD-WAN overlay network.</td>
</tr>
<tr>
<td>vpn-membership</td>
<td>Configure or apply a centralized data policy based on VPN membership.</td>
</tr>
<tr>
<td>vrrp</td>
<td>Configure the Virtual Router Redundancy Protocol to allow multiple routers to share a common virtual IP address for default gateway redundancy.</td>
</tr>
<tr>
<td>vpn interface dot1x wake-on-lan</td>
<td>Allow a client to be powered up when the vEdge router receives an Ethernet magic packet frame.</td>
</tr>
<tr>
<td>wlan</td>
<td>Configure a WLAN.</td>
</tr>
<tr>
<td>wlan interface wpa-personal-key</td>
<td>Configure the password to access a wireless LAN that uses wpa-personal or wpa2-personal security.</td>
</tr>
<tr>
<td>policy zone</td>
<td>Create a group of one or more VPNs in the overlay network that form a zone.</td>
</tr>
<tr>
<td>policy zone-based-policy</td>
<td>Configure a firewall policy for stateful inspection of ICMP, TCP, and UDP flows.</td>
</tr>
<tr>
<td>policy zone-pair</td>
<td>Configure a zone pair to apply a zone-based firewall policy to traffic flows between a source zone and a destination zone.</td>
</tr>
<tr>
<td>zone-to-nozone-internet</td>
<td>policy 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 policy include VPN 0.</td>
</tr>
</tbody>
</table>
Overview of Configuration Commands

The articles on this page describe the CLI commands that you use to configure the functional network properties of vSmart controllers, vEdge routers, and vBond orchestrators. To configure a Viptela device, you enter configuration mode by issue 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 vEdge 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.

The articles in this section are arranged alphabetically, by configuration command name.
aaa

Configure role-based access to a Cisco vEdge device using authentication, authorization, and accounting.

vManage Feature Template

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

Command Hierarchy

system
  aaa
    admin-auth-order
    auth-fallback
    auth-order (local | radius | tacacs)
    logs
      [no] audit-disable
      [no] netconf-disable
    radius-servers tag
    user username
    group group-name
    password password
    usergroup group-name
    task (interface | policy | routing | security | system) (read | write)

Syntax Description

The command has no keywords or arguments.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

vEdge# config
Entering configuration mode terminal
vEdge(config)# system aaa
vEdge(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 $1$aLEJ6jve$aBpPQpk13h.SvA2dt4/6E/
    group operator
  !
  !
vEdge(config-aaa)# commit and quit
Commit complete.
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 $1$zvOh58p$QLX7/RS/F0c6ar94.xl2k.
    !
    user eve
      password $1$aLEj6jve$aBpPQpk13h.5vA2dt4/6E/
      group operator
    !
    !

**Operational Commands**

show aaa usergroup
show users

**Related Topics**

- dot1x, on page 225
- radius, on page 488
- tacacs, on page 557
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
    mirror mirror-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

<table>
<thead>
<tr>
<th>acl-name</th>
<th>Access List Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the access list to configure or to apply to the interface. acl-name can be up to 32 characters long.</td>
<td></td>
</tr>
<tr>
<td>Direction in which to Apply Access List:</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Direction in which to apply the access list. Applying it in the inbound direction (<strong>in</strong>) affects packets being received on the interface. Applying it in the outbound direction (<strong>out</strong>) affects packets being transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

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

```plaintext
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 33
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
```

**Apply an Access List**

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

**Syntax Description**

<table>
<thead>
<tr>
<th>access-list Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-name</td>
<td>Access List Name: Name of the access list to configure or to apply to the interface.</td>
</tr>
<tr>
<td>(in</td>
<td>out)</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 31
accounting-interval

How often an 802.1X interface 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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Accounting Update Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How often to send 802.1X interim accounting updates to the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>0 through 7200 seconds</td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>0 (no interim accounting updates are sent)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 37
  nas-identifier, on page 413
  nas-ip-address, on page 415
  radius, on page 488
  radius-servers, on page 492
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
da1x
    acct-req-attr attribute-number (integer integer | octet octet | string string)
```

Syntax Description

<table>
<thead>
<tr>
<th>attribute-number</th>
<th>Accounting Attribute Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RADIUS accounting attribute number.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 64</td>
</tr>
</tbody>
</table>

| (integerinteger | octetoctet | string) | Attribute Value: |
|-----------------|-----------|--------------|
|                  | Value of the attribute. Specify the value as an integer, octet, or string, depending on the accounting attribute itself. |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Set the Acct-Authentic attribute to RADIUS:

```
vpn 0
  interface ge0/0
da1x
    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 102
- [nas-identifier](#), on page 413
- [nas-ip-address](#), on page 415
- [radius](#), on page 488
- [radius-servers](#), on page 492
**action**

Configure the actions to take when the match portion of an IPv4 policy is 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
  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 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
```
Configuration Commands

For Cflowd Traffic Flow Monitoring

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 only.

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 only.

access-list acl-name
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default-action sla-class sla-class-name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>policy policy-name policy control-policy policy-name</strong></td>
<td>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 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.</td>
</tr>
<tr>
<td>**default-action (accept</td>
<td>reject) policy policy-name**</td>
</tr>
</tbody>
</table>

**For Zone-Based Firewall Policy**

Configure on vEdge routers only.

```
policy
zone-based-policy policy-name
  default-action action
  sequence number
  action
    drop
    count counter-name
    log
    accept
      class class-name
      count counter-name
      log
      mirror mirror-name
      policer policer-name
      set dscp value
      set next-hop ipv4-address
```

**For Zone-Based Firewall Policy**

Configure on vEdge routers only.

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

• 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.

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.
### (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)

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.
<table>
<thead>
<tr>
<th>set tloc-action</th>
<th>action</th>
</tr>
</thead>
</table>

Configuration Commands

45
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.

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 among them. Changing an OMP route's TLOC is one way to use policy to affect 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. |
| 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 throughput for TCP traffic. |
| policer policer-name | Policer: Policy the packets using the specified policer. |
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service service-name (tloc-ip-address</td>
<td>Direct matching packets to the named service. Traffic is directed to a TLOC if the service is available. If the TLOC is not available, traffic is dropped.</td>
</tr>
<tr>
<td>tloc-list</td>
<td></td>
</tr>
<tr>
<td>[list-name]</td>
<td></td>
</tr>
<tr>
<td>[vpn vpn-id]</td>
<td></td>
</tr>
<tr>
<td>Service via GRE Tunnel:</td>
<td>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 <code>restrict</code> option. In the service VPN, you must also advertise the service using the <code>service</code> command. Configure the GRE service.</td>
</tr>
<tr>
<td>redirect-dns (ip-address</td>
<td>Split DNS Server: For a policy that enables split DNS (that is, when the <code>match</code> condition specifies <code>dns-app-list</code> and <code>dns</code>), specify how to direct matching packets. For DNS queries (<code>dns request</code>), specify the IP address of the DNS server to use to resolve the DNS query. For DNS responses (<code>dns response</code>), specify <code>host</code> so that the response from the DNS server is properly forwarded to the requesting service VPN.</td>
</tr>
<tr>
<td>host)</td>
<td></td>
</tr>
<tr>
<td>set tloc-list list-name</td>
<td>TLOC from a List of TLOCs: Direct matching packets to one of the TLOCs in the list defined with a <code>policy lists tloc-list</code> 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.</td>
</tr>
<tr>
<td>set local-tloc color color [encap encapsulation]</td>
<td>TLOC Identified by Color: Direct matching packets to a TLOC identified by its color and, optionally, its encapsulation. <code>color</code> can be <code>3g</code>, <code>biz-internet</code>, <code>blue</code>, <code>bronze</code>, <code>custom1</code>, <code>custom2</code>, <code>custom3</code>, <code>default</code>, <code>gold</code>, <code>green lte</code>, <code>metro-ethernet</code>, <code>mpls</code>, <code>private1</code> through <code>private6</code>, <code>public-internet</code>, and <code>silver</code>. By default, <code>encapsulation</code> is <code>ipsec</code>. It can also be <code>gre</code>. 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 <code>restrict</code> option.</td>
</tr>
<tr>
<td>set tloc ip-address color color [encap encapsulation]</td>
<td>TLOC Identified IP Address and Color: Direct matching packets to a TLOC identified by its IP address and color, and optionally, by its encapsulation. <code>color</code> can be <code>3g</code>, <code>biz-internet</code>, <code>blue</code>, <code>bronze</code>, <code>custom1</code>, <code>custom2</code>, <code>custom3</code>, <code>default</code>, <code>gold</code>, <code>green lte</code>, <code>metro-ethernet</code>, <code>mpls</code>, <code>private1</code> through <code>private6</code>, <code>public-internet</code>, and <code>silver</code>. By default, <code>encapsulation</code> is <code>ipsec</code>. It can also be <code>gre</code>.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>set vpn vpn-id</td>
<td><strong>VPN:</strong> Set the VPN Identifier that is included in accepted packets.</td>
</tr>
</tbody>
</table>

**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.
**Syntax Description**

**For Localized Data Policy**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**(accept</td>
<td>drop)**</td>
</tr>
<tr>
<td><strong>count counter-name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>class class-name</strong></td>
<td>Class Assign the packets to the specified QoS class name.</td>
</tr>
<tr>
<td><strong>set dscp value</strong></td>
<td>DSCP; For QoS, set or overwrite the DSCP value in the packet. value can be a number from 0 through 63.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>Log Packet Headers:</td>
</tr>
<tr>
<td></td>
<td>Log the packet headers into the vsyslog and messages system logging (syslog) files.</td>
</tr>
<tr>
<td><strong>mirror</strong></td>
<td>Mirroring:</td>
</tr>
<tr>
<td><strong>mirror-name</strong></td>
<td>Mirror the packets to the specified mirror.</td>
</tr>
<tr>
<td><strong>set next-hop</strong></td>
<td>Next-Hop Address:</td>
</tr>
<tr>
<td><strong>ipv4-address</strong></td>
<td>Set the next-hop address. The address must be an IPv4 address.</td>
</tr>
<tr>
<td><strong>policer</strong></td>
<td>Policing:</td>
</tr>
<tr>
<td><strong>policer-name</strong></td>
<td>Police the packets using the specified policer.</td>
</tr>
</tbody>
</table>

**Syntax Description**

*For Zone-Based Firewall Policy*

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>drop</strong></td>
<td>Drop:</td>
</tr>
<tr>
<td></td>
<td>Discard the data traffic.</td>
</tr>
<tr>
<td><strong>inspect</strong></td>
<td>Inspect:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>Log Packet Headers:</td>
</tr>
<tr>
<td></td>
<td>Log the packet headers into the vsyslog and messages system logging (syslog) files.</td>
</tr>
<tr>
<td><strong>pass</strong></td>
<td>Pass Through:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Added application-aware routing policy.</td>
</tr>
<tr>
<td>14.3</td>
<td>Added Cflowd traffic monitoring.</td>
</tr>
<tr>
<td>15.2</td>
<td>Added setting GRE encapsulation and preferred color for an SLA class.</td>
</tr>
<tr>
<td>15.4</td>
<td>Added match condition for localized control policy.</td>
</tr>
<tr>
<td>16.1</td>
<td>Added log option to application-aware policy action.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added backup-sla-preferred-color option for application-aware routing.</td>
</tr>
<tr>
<td>17.1</td>
<td>Added load-balancing among multiple colors for application-aware routing.</td>
</tr>
<tr>
<td>17.2</td>
<td>Added redirect-dns option for centralized data policy.</td>
</tr>
<tr>
<td>18.2</td>
<td>Added zone-based firewall policy.</td>
</tr>
</tbody>
</table>

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
```

Operational Commands

- show app log flows
- show log
- show logging
- show running-config policy

Related Topics

- apply-policy, on page 81
- lists, on page 344
- match, on page 380
- policy, on page 457
- policy ipv6, on page 464
**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.

```plaintext
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
    mirror mirror-name
    policer policer-name
    set
    traffic-class value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`(accept</td>
<td>drop)`</td>
</tr>
<tr>
<td><code>count counter-name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>class class-name</code></td>
<td>Class: Assign the packets to the specified QoS class name.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Log Packet Headers: Log the packet headers into system logging (syslog) files.</td>
</tr>
<tr>
<td><code>mirror mirror-name</code></td>
<td>Mirroring: Mirror the packets to the specified mirror.</td>
</tr>
<tr>
<td><code>policer policer-name</code></td>
<td>Policing: Police the packets using the specified policer.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Command modified for IPv6.</td>
</tr>
</tbody>
</table>

---

**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 457
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv4_unicast</strong></td>
<td>Address Family: Currenty, the Viptela software supports only the BGP IPv4 unicast address family.</td>
</tr>
<tr>
<td><strong>aggregate-address prefix/length [as-set] [summary-only]</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>maximum-paths paths number</strong></td>
<td>IBGP and EBGIP 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</td>
</tr>
</tbody>
</table>
### Networks To Advertise:
Networks to be advertised by BGP. Identify the networks by their prefix and length.

<table>
<thead>
<tr>
<th>network</th>
<th>prefix / length</th>
</tr>
</thead>
</table>

### 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.
- **threshold** is the percentage of the maximum number of prefixes at which to either generate a warning message or restart the BGP peering session.
- **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.
- **warning-only** displays a warning message only when the maximum prefix limit is exceeded.

<table>
<thead>
<tr>
<th>maximum-prefixes</th>
<th>number [threshold] [restart minutes] [warning-only]</th>
</tr>
</thead>
</table>

### 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.

<table>
<thead>
<tr>
<th>route-policy</th>
<th>policy-name [in</th>
<th>out]</th>
</tr>
</thead>
</table>

---

| configuration commands | 56 | Configuration Commands | 56 |
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added redistribute natpool-outside option.</td>
</tr>
</tbody>
</table>

**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
```

Commit complete.
```
vEdge(config-address-family-ipv4-unicast)# commit and-quit
```

```
vEdge# show bgp routes
```

<table>
<thead>
<tr>
<th>VPN</th>
<th>PREFIX</th>
<th>NEXTHop</th>
<th>METRIC</th>
<th>LOCAL PREF</th>
<th>WEIGHT</th>
<th>ORIGIN</th>
<th>AS</th>
<th>PATH</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.20.25.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>-</td>
<td>32768</td>
<td>igp</td>
<td>Local valid,best</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>61.0.1.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>-</td>
<td>32768</td>
<td>igp</td>
<td>Local valid,best</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 Viptela devices:

Configuration ► Templates ► AAA

**Command Hierarchy**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.2</td>
<td>Modified for supporting authentication order process for console connections.</td>
</tr>
</tbody>
</table>

**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**

Related Topics

- auth-fallback, on page 94
- auth-order, on page 97
- radius, on page 488
- tacacs, on page 557
- usergroup, on page 624
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

<table>
<thead>
<tr>
<th>admin-state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>down</td>
<td>Disable DHCP Server Functionality:</td>
</tr>
<tr>
<td></td>
<td>By default, DHCP server functionality is disabled on a vEdge router interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable DHCP Server Functionality:</td>
</tr>
<tr>
<td></td>
<td>Allow the vEdge router to act as a DHCP server for the local site networks accessible through this interface.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Enable DHCP server functionality on an interface:

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

vManage Feature Template

For all Viptela devices:
Configuration ► Templates ► System

Command Hierarchy

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

This comand has no keywords or arguments.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 routes learned locally by the vEdge router to OMP (on vEdge routers only). OMP carries the routes learned to the vSmart controller. By default, a vEdge router advertises connected, static, OSPF inter-area, and OSPF intra-area routes to OMP.

Route advertisements that you configure with the `omp advertise` command apply to all VPNs configured on the router. With the `vpn omp advertise` command, you can configure how routes are advertised in any individual VPN except for VPN 0 and VPN 512, and this configuration applies only to the specific VPN. If you configure route advertisements with both commands, they are both applied. `advertise isis` command is added to support IS-IS route redistribution in OMP. OMP is update to advertise both Level 1 and Level 2 IS-IS routes for Software Defined Access (SDA). This is supported for both the IPv4 and IPv6 address families.

### vManage Feature Template

For vEdge routers only:
- Configuration ▶ Templates ▶ OMP
- Configuration ▶ Templates ▶ System

### Command Hierarchy

```
omp
  advertise (bgp | connected | ospf type | static)

vpn vpn-id
  omp
    advertise (aggregate prefix [aggregate-only] | bgp | connected | network prefix | ospf type | static)
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aggregate prefix [aggregate-only]</strong></td>
<td>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 <code>aggregate-only</code> option.</td>
</tr>
<tr>
<td><strong>bgp</strong></td>
<td>BGP Routes: Advertise all BGP routes learned by the vEdge router to OMP.</td>
</tr>
<tr>
<td><strong>connected</strong></td>
<td>Connected Routes: Advertise all connected routes on the vEdge router to OMP. Connected routes are advertised by default. To disable advertisement, use the <code>no advertise connected</code> command.</td>
</tr>
<tr>
<td><strong>network prefix</strong></td>
<td>Network Routes: Advertise a specific route learned by the vEdge router to OMP. This route must be in the vEdge router's route table for the VPN. Use this option to advertise a specific route instead of advertising all routes for a protocol.</td>
</tr>
</tbody>
</table>
ospf type
OSPF Routes:
Advertise all OSPF routes learned by the local vEdge router 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 vEdge router 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.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example
The following example shows the ISIS route distribution in OMP:

For a vEdge router in a branch network that is running BGP, advertise to the vSmart controller the routes that the vEdge router has learned from the local network:

```
omp
   advertise bgp
```

Operational Commands

- show ip routes
- show omp routes
**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**

<table>
<thead>
<tr>
<th>seconds</th>
<th>MAC Table Entry Aging Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How long an entry is in the MAC table before it ages out.</td>
</tr>
<tr>
<td></td>
<td>Default: 300 seconds (5 minutes)</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 4096 seconds</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
    !
```

Configuration Commands
**Operational Commands**

show bridge interface
show bridge mac
show bridge table
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**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

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

```plaintext
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 vEdge routers only). Note that no BFD sessions are established between the two collocated vEdge routers.

vManage Feature Template

For vEdge routers only:
Configuration ► Templates ► System

Command Hierarchy

system
  allow-same-site-tunnels

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 583
**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 explicit 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
```

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Type:</td>
<td></td>
</tr>
<tr>
<td>Name of a physical interface. The services that you configure in <code>allow-service</code> commands apply only to physical interfaces, such as <code>ge</code> and <code>eth</code> interfaces. They do not apply to non-physical interfaces, such as loopback interfaces.</td>
<td></td>
</tr>
</tbody>
</table>
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 of 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.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>BGP, OSPF services and support for netconf added on vEdge routers.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for DHCPv6.</td>
</tr>
<tr>
<td>18.1.1</td>
<td>Added support for https service on vEdge routers.</td>
</tr>
</tbody>
</table>

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
color lte
  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 171
icmp-redirect-disable, on page 279
implicit-acl-logging, on page 285
ntp, on page 431
service, on page 528
vbond-as-stun-server, on page 629
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

<table>
<thead>
<tr>
<th>policy-name</th>
<th>Application-Aware Routing Policy Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
Example

Configure and apply a simple data policy for application-aware routing

```bash
evSmart# 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 535
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Enable application-visibility on a vEdge router:

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

vEdge# show app dpi flows

<table>
<thead>
<tr>
<th>Source</th>
<th>Dest</th>
<th>Protocol</th>
<th>Application</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>SINCE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>23.4.153.244</td>
<td>1557</td>
<td>443</td>
</tr>
<tr>
<td>2015-05-04T13:47:29+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>74.125.20.95</td>
<td>20581</td>
<td>443</td>
</tr>
<tr>
<td>2015-05-04T13:47:07+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>74.125.25.188</td>
<td>55742</td>
<td>5228</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>19286</td>
<td>53</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>20605</td>
<td>53</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>34716</td>
<td>53</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>43894</td>
<td>53</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>50865</td>
<td>53</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>192.168.15.3</td>
<td>60079</td>
<td>443</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>216.115.20.77</td>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>2015-05-04T13:47:25+00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
vEdge# show app dpi applications

<table>
<thead>
<tr>
<th>VPN</th>
<th>SRC IP</th>
<th>APPLICATION</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.51.88.142</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.1</td>
<td>syslog</td>
<td>Application Service</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.1</td>
<td>tcp</td>
<td>Network Service</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.1</td>
<td>unknown</td>
<td>Standard</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>addthis</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>adobe</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>adobe_update</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>akamai</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>alexa</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>alibaba</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>aliexpress</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>amazon</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>amazon_adsystem</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>amazon_aws</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>amazon_cloud_drive</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>ask</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>att</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>bing</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>blackberry</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>blackberry_locate</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>blackberry_update</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>brightcove</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>chrome_update</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>10.192.42.2</td>
<td>cloudflare</td>
<td>Web</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>216.58.192.14</td>
<td>https</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>216.58.217.10</td>
<td>https</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>216.58.217.10</td>
<td>tcp</td>
<td>Network Service</td>
</tr>
<tr>
<td>1</td>
<td>216.58.217.46</td>
<td>https</td>
<td>Web</td>
</tr>
<tr>
<td>1</td>
<td>216.59.38.123</td>
<td>tcp</td>
<td>Network Service</td>
</tr>
<tr>
<td>1</td>
<td>216.115.100.103</td>
<td>tcp</td>
<td>Network Service</td>
</tr>
<tr>
<td>1</td>
<td>221.33.84.240</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>1</td>
<td>222.54.68.154</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>1</td>
<td>222.117.30.93</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
<tr>
<td>1</td>
<td>222.228.8.6</td>
<td>bittorrent</td>
<td>Peer to Peer</td>
</tr>
</tbody>
</table>

**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 Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>applications</code></td>
<td>Interface Node Type:</td>
</tr>
<tr>
<td></td>
<td>List of applications.</td>
</tr>
<tr>
<td></td>
<td>Values:</td>
</tr>
<tr>
<td></td>
<td>amazon_aws, box_net, concur, dropbox, google_apps, gotomeeting, intuit, office365, oracle, salesforce, sugarcrm, zendesk, zoho.crm</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th><strong>Cflowd Template</strong></th>
<th>Cflowd Template:</th>
</tr>
</thead>
<tbody>
<tr>
<td>template-name</td>
<td>For a centralized data policy that applies to cflowd flow collection, associate a flow collection template with the data policy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Policy Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>**app-route-policy policy-name control-policy policy-name (in</td>
</tr>
<tr>
<td>**data-policy policy-name (all</td>
</tr>
</tbody>
</table>
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 site 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Added app-route-policy.</td>
</tr>
<tr>
<td>14.3</td>
<td>Added cflowd-template.</td>
</tr>
<tr>
<td>15.2</td>
<td>Added all, from-service, and from-tunnel options</td>
</tr>
<tr>
<td>15.4</td>
<td>Added restrictions so that you cannot apply the same type of policy.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for overlapping sites in different site lists.</td>
</tr>
</tbody>
</table>

### 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
```
command introduced in Viptela 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 53
Cflowd-template, on page 143
Control-policy, on page 183
Data-policy, on page 194
Lists, on page 344
Match, on page 377
Policy, on page 457
**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 Viptel devices:

Configuration ► Templates ► Archive

**Command Hierarchy**

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

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>interval minutes</strong></th>
<th>Archival Time Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How often to archive the full running configuration. In addition, the running configuration is archived each time you issue the <strong>commit</strong> command on a Cisco vEdge device.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong></td>
</tr>
<tr>
<td></td>
<td>5 minutes through 525600 minutes (about one year)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong></td>
</tr>
<tr>
<td></td>
<td>10080 minutes (7 days)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>path file-path/ filename</strong></th>
<th>Location of Archival File:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ftp</strong>: file-path—Path to a file on an FTP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>scp</strong>: user @ host : file-path</td>
</tr>
<tr>
<td></td>
<td>• / file-path / filename—Path to a file on the local Cisco vEdge device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ssh-id-file filename</strong></th>
<th>SSH Key File</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 Viptela device. If you do not include the <strong>ssh-id-file</strong> option in the configuration, the software uses the automatically generated private key. You can also manually generate and upload an SSH private key file.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

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

```plaintext
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**

<table>
<thead>
<tr>
<th><strong>number</strong></th>
<th><strong>Area Number:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of the OSPF area.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong></td>
</tr>
<tr>
<td></td>
<td>The area is a 32-bit number.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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  ENCAP PORT
      VPN INTERFACE IP ADDRESS STATUS STATUS TYPE TYPE MTU HWADDR MBPS
      VPN   INTERFACE IP ADDRESS STATUS STATUS TYPE TYPE MTU HWADDR MBPS

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
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ip-address mac mac-address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>no arp ip ip-address</strong></td>
<td>Disable ARP: Remove a static ARP mapping address.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>seconds</th>
<th>Timeout Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time before a dynamically learned ARP entry times out.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>0 through 2678400 seconds (744 hours)</td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>1200 seconds (20 minutes)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

```
auth-fail-vlan vlan-id
```

<table>
<thead>
<tr>
<th>VLAN Identifier:</th>
<th>Identifier of the VLAN to be the restricted VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range:</td>
<td>1 through 4094</td>
</tr>
</tbody>
</table>

Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
```

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 100
  - bridge, on page 136
  - default-vlan, on page 208
  - guest-vlan, on page 262
  - radius, on page 488
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, either because the user has entered invalid credentials or because the authentication server is unreachable (or all authentication servers are unreachable). 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.

**vManage Feature Template**

For all Cisco vEdge devices:

Configuration ► Templates ► AAA

**Command Hierarchy**

```
system
   aaa
      auth-fallback
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2.8</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.2</td>
<td>Added support for authentication order process for console connections.</td>
</tr>
</tbody>
</table>

**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.

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 60
  auth-order, on page 97
  radius, on page 488
  tacacs, on page 557
  usergroup, on page 624
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)
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mab</th>
<th>MAC Authentication Bypass:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Use MAC authentication bypass for authentication, which provides authentication for non-802.1X-compliant devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>radius</th>
<th>RADIUS Authentication:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Use RADIUS servers for authentication.</td>
</tr>
</tbody>
</table>

### 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 375
- **radius**, on page 488
- **radius-servers**, on page 492
auth-order

Configure the order in 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 server` command. 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 Viptela 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

<table>
<thead>
<tr>
<th>Default Authentication Order:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default authentication order is <strong>local</strong>, then <strong>radius</strong>, and then <strong>tacacs</strong>.</td>
</tr>
</tbody>
</table>

| **loc**a| Loco| e 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**. |

| **radio**s | 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.2</td>
<td>Added authentication order process for console connections.</td>
</tr>
</tbody>
</table>

### Example

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

```sh
Viptela# config
Entering configuration mode terminal
Viptela(config)# system aaa radius local
Viptela(config-aaa)# commit and-quit
Commit complete.
Viptela# 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 60
- `auth-fallback`, on page 94
radius, on page 488

tacacs, on page 557

usergroup, on page 624
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

<table>
<thead>
<tr>
<th><code>vlan-id</code></th>
<th>VLAN Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifier of VLAN into which to place 802.1x-enabled clients if authentication for the clients is rejected by the RADIUS servers.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 4094</td>
</tr>
</tbody>
</table>

Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
```

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 92
  bridge, on page 136
  default-vlan, on page 208
  guest-vlan, on page 262
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

<table>
<thead>
<tr>
<th>attribute-number</th>
<th>Authentication Attribute Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RADIUS authentication attribute number.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 64</td>
</tr>
</tbody>
</table>

| (integer integer | 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
do1x
  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 37
- nas-identifier, on page 413
- nas-ip-address, on page 415
- radius, on page 488
- radius-servers, on page 492
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>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.</td>
</tr>
<tr>
<td>authentication type md5 encrypted-key</td>
<td>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 (&quot; &quot;).</td>
</tr>
<tr>
<td>authentication type simple</td>
<td>Simple Authentication: Use simple, or plain text, authentication for all OSPF protocol exchanges on an interface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 "$40P3T3z2sCirxa5+CLEFXXw==<"

**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**

<table>
<thead>
<tr>
<th>local-id id</th>
<th>remote-id id</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE Session Identifier:</strong> 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. <em>id</em> 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)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pre-shared-secret password</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preshared Password:</strong> Password to use with the preshared key. <em>password</em> can be an ASCII or a hexadecimal string from 1 through 127 characters long.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 405
authentication-type

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

**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-Viptela 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 Viptela AH software ignore the ID field in the IP header so that the Viptela 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
**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

**Operational Commands**

show security-info
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**

<table>
<thead>
<tr>
<th>mbps</th>
<th>Reference Bandwidth:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface speed.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 4294967</td>
</tr>
<tr>
<td></td>
<td>Mbps</td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>100 Mbps</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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-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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.1</td>
<td>Disable this command for IRB interfaces.</td>
</tr>
</tbody>
</table>

**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 230
- **speed**, on page 539
**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.

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 rates 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 osf
      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 118
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.

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**

<table>
<thead>
<tr>
<th>kbps</th>
<th>Interface Transmission Bandwidth:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 2147483647 ((2^{32} / 2) – 1) kbps</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
going no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
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
rx-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 116
banner login

**banner login**—Configure banner text to be displayed before the login prompt on a Viptela device.

**vManage Feature Template**

For all Cisco SD-WAN devices:

Configuration ► Templates ► Banner

**Command Hierarchy**

```
banner
  login "text"
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Banner Text:</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1.1</td>
<td>Changed maximum banner length to 2048 characters</td>
</tr>
</tbody>
</table>

**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 121
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.
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1.1</td>
<td>Changed maximum banner length to 2048 characters.</td>
</tr>
</tbody>
</table>

**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 120
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Select Routes with BGP Multipath:</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-path multipath-relax</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Use the MED to Select the Active BGP Path:</th>
</tr>
</thead>
<tbody>
<tr>
<td>med (always-compare</td>
<td>Use the MED to Select the Active BGP Path:</td>
</tr>
<tr>
<td>deterministic</td>
<td>Use the MED to Select the Active BGP Path:</td>
</tr>
<tr>
<td>missing-as-worst)</td>
<td>Compare the specified multi-exit discriminator (MED) parameter to determine the active path. The MED parameter can be one of:</td>
</tr>
<tr>
<td></td>
<td>always-compare: Always compare MEDs regardless of whether the peer ASs of the compared routes are the same.</td>
</tr>
<tr>
<td></td>
<td>deterministic: Compare MEDs from all routes received from the same AS regardless of when the route was received.</td>
</tr>
<tr>
<td></td>
<td>missing-as-worst: If a path is missing a MED attribute, consider it to be the worst path.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Use the Router ID to Select the Active BGP Path:</th>
</tr>
</thead>
<tbody>
<tr>
<td>compare-router-id</td>
<td>Use the Router ID to Select the Active BGP Path:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 6</td>
</tr>
<tr>
<td></td>
<td>Default: 6</td>
</tr>
</tbody>
</table>

| **poll-interval milliseconds** | Polling Interval:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 4,294,967,296 (2^{32} - 1) milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 600,000 milliseconds (10 minutes)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 126
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hello-interval</code></td>
<td>Identifier for the Transport Tunnel: 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)</td>
</tr>
<tr>
<td>milliseconds</td>
<td>Identifier for the Transport Tunnel: 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)</td>
</tr>
<tr>
<td><code>color</code></td>
<td>Identifier for the Transport Tunnel: 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)</td>
</tr>
<tr>
<td>color</td>
<td>Identifier for the Transport Tunnel: 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)</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Identifier for the Transport Tunnel: 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)</td>
</tr>
</tbody>
</table>

**Values:**
**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.

Default:
Enabled

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>Added pmtu-discovery option, renamed interval option to hello-interval, and changed Hello interval units from seconds to milliseconds.</td>
</tr>
<tr>
<td>15.1.1</td>
<td>Changed default multiplier from 3 to 7.</td>
</tr>
<tr>
<td>15.2</td>
<td>Added colors private3, private4, private5, and private6.</td>
</tr>
<tr>
<td>15.3.2</td>
<td>Enabled path MTU discovery by default.</td>
</tr>
<tr>
<td>16.1</td>
<td>Added default multiplier for vEdge Cloud routers.</td>
</tr>
<tr>
<td>16.2</td>
<td>Changed maximum hello interval from 60 seconds to 5 minutes.</td>
</tr>
</tbody>
</table>
**Example**

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

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

**Operational Commands**

- `show bfd sessions`
- `show control connections`

**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 124
- `encapsulation`, on page 239
- `last-resort-circuit`, on page 340
- `mtu`, on page 406
- `pmtu`, on page 452
- `hello-interval`, on page 264
- `hello-tolerance`, on page 270
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local-as-number</code></td>
</tr>
<tr>
<td><strong>Local AS Number:</strong></td>
</tr>
<tr>
<td>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).</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Configure BGP in VPN 1:

```
vpn 1
  router
    bgp 123
      address-family ipv4 unicast
      redistribute ospf
      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 ospf 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
<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Physical WAN interface to bind to a loopback interface. <code>interface-name</code> has the format <code>ge slot/port</code>. Both the loopback and physical WAN interfaces must be in VPN 0.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Cisco SD-WAN Release 19.2</td>
<td>Added support for Cisco XE SD-WAN routers.</td>
</tr>
<tr>
<td>Cisco IOS XE SD-WAN Release 16.12.1</td>
<td></td>
</tr>
</tbody>
</table>

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
```
Example 2

(for Cisco XE 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 interface'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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>name</th>
<th>Bridging Domain Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Text description of the bridging domain. If <em>text</em> contains spaces, enclose it in quotation marks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bridge-id</th>
<th>Bridging Domain Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number that identifies the bridging domain.</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 63</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>INTERFACE</th>
<th>VLAN</th>
<th>STATUS</th>
<th>STATUS</th>
<th>TYPE</th>
<th>IFINDEX</th>
<th>MTU</th>
<th>PKTS</th>
<th>OCTETS</th>
<th>PKTS</th>
<th>OCTETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ge0/2</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>34</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>ge0/5</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>36</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>ge0/6</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>38</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>ge0/2</td>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>40</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ge0/5</td>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>42</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ge0/6</td>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td>vlan</td>
<td>44</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>50</td>
<td>ge0/2</td>
<td>-</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>16</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>50</td>
<td>ge0/5</td>
<td>-</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>19</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>50</td>
<td>ge0/6</td>
<td>-</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>20</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

**Operational Commands**

- show bridge interface
- show bridge mac
- show bridge table

**Related Topics**

- interface irb, on page 307
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

\textbf{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**

\begin{verbatim}
vpn 0
   interface interface-name
   tunnel-interface
   carrier carrier-name
\end{verbatim}

**Table 1: Syntax Description**

<table>
<thead>
<tr>
<th>\textbf{carrier-name}</th>
<th>Private Network Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Carrier name to associate with a tunnel interface.</td>
</tr>
<tr>
<td></td>
<td>Values:</td>
</tr>
<tr>
<td>carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default</td>
<td></td>
</tr>
<tr>
<td>Default:</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

Associate a carrier name with a tunnel connection:

\begin{verbatim}
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
\end{verbatim}
carrier

!
no shutdown
!

**Operational Commands**

show control connections
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**

<table>
<thead>
<tr>
<th>cellular number</th>
<th>Cellular Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Name of the cellular interface. It must be cellular0.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 481
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. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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:** |
|-----------------|---------------------------------|
| Auto            | 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. |
| Auto-No-DFS     | Default: auto                   |

<table>
<thead>
<tr>
<th>Channel</th>
<th><strong>2.4-GHz WLANs:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>A 2.4-GHz radio band. This band supports IEEE 802.11b, 802.11g, and 802.11n clients.</td>
</tr>
<tr>
<td>Range</td>
<td>1 through 13, depending on the country configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Channel</th>
<th><strong>5.0-GHz WLANs:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>16.3</td>
</tr>
</tbody>
</table>
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+IEZB2vcQpeEoSR4ia9JqqDsPNoHukAb8fvxAg5I=
    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 147
**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**

<table>
<thead>
<tr>
<th><code>megahertz</code></th>
<th>Channel Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bandwidth available on the WLAN channel.</td>
</tr>
<tr>
<td></td>
<td>Values:</td>
</tr>
<tr>
<td></td>
<td>20, 40, 80 MHz</td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>20 MHz (for 2.4 GHz); 80 MHz (for 5 GHz)</td>
</tr>
</tbody>
</table>

**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 145
**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**

<table>
<thead>
<tr>
<th>suite</th>
<th>Authentication and Encryption Type for IKE Key Exchange:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type of authentication and integrity checking to use during IKE key exchange. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes128-cbc-sha1</strong>—Use the AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes128-cbc-sha2</strong>—Use the AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes256-cbc-sha1</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes256-cbc-sha2</strong>—Use the AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>suite</th>
<th>Encryption Type for IPsec Tunnel:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type of encryption to use on an IPsec tunnel that is being used for IKE key exchange. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes256-cbc-sha1</strong>—Calculate message encryption using the AES-256 cipher in CBC (cipher block chaining) mode using HMAC-SHA1-96 keyed-hash message authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>aes256-gcm</strong>—Calculate message encryption using the AES-256 algorithm in GCM (Galois/counter mode). This is the default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>null-sha1</strong>—Do not encrypt the IPsec tunnel that is being used for IKE key exchange traffic.</td>
</tr>
</tbody>
</table>
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>18.2</td>
<td>Added support for SHA2-based ciphers for IKE.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>class</th>
<th>class-name</th>
<th>queue number</th>
<th>Class Mapping to Output Queue:</th>
</tr>
</thead>
</table>
|       |            |              | 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.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Changed the LLQ queue from queue 1 to queue 0. The software supports only one queue for LLQ, and it must be queue 0.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for multicast traffic and for vEdge Cloud routers.</td>
</tr>
<tr>
<td>17.2.2</td>
<td>vEdge Cloud routers support eight queues, with queue 0 reserved for LLQ</td>
</tr>
</tbody>
</table>

**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
!

Operational Commands

show policy qos-map-info

Related Topics

- access-list, on page 33
- cloud-qos, on page 155
- qos-map, on page 484
- qos-scheduler, on page 486
- rewrite-rule, on page 515
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

This command is not applicable for Cisco XE SD-WAN Routers.

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

**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**

```
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 406
- pmtu, on page 452
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

<table>
<thead>
<tr>
<th>timezone</th>
<th>timezone</th>
</tr>
</thead>
<tbody>
<tr>
<td>timezone</td>
<td>Set the timezone on the device. <code>timezone</code> is one of the timezones in the tz database (also called tzdata, the zoneinfo database, or the IANA timezone database). <code>timezone</code> has the format <code>area/location</code>. <code>area</code> 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). <code>location</code> 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</td>
</tr>
</tbody>
</table>

Examples

**California time zone**

California time:

```
v6# show running-config system
system
clock timezone America/Los_Angeles
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2</td>
<td>Support for the IANA timezone database added.</td>
</tr>
</tbody>
</table>

Related Commands

clock set date
clock set time
show system status
**cloud-qos**

**policy cloud-qos**—Enable QoS scheduling and shaping for traffic that the router receives from transport-side interfaces (on vEdge Cloud and vEdge 5000 routers only).

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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:

```bash
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 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
qos-scheduler qos-sched0
class class0
  bandwidth-percent 1
  buffer-percent 1
qos-scheduler qos-sched1
class class1
  bandwidth-percent 1
  buffer-percent 1
qos-map qos-map1
gos-scheduler qos-sched0
gos-scheduler qos-sched1

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
qos-map qos-map1
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
    qos-map qos-map1
    rewrite-rule rewrite-to-0

**Operational Commands**

show policy qos-map-info
show policy qos-scheduler-info

**Related Topics**

- **access-list**, on page 33
- **class-map**, on page 151
- **cloud-qos-service-side**, on page 158
- **qos-map**, on page 484
- **qos-scheduler**, on page 486
- **rewrite-rule**, on page 515
cloud-qos-service-side

**policy cloud-qos-service-side**—Enable QoS scheduling and shaping for traffic that the router receives from service-side interfaces (on vEdge Cloud routers only).

**vManage Feature Template**

For vEdge routers:

Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Cloud QoS Service Side

**Command Hierarchy**

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

**Syntax Description**

None

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
cloud-qos-service-side
```

```plaintext
class-map
class class0 queue 0
class class1 queue 1
class class16 queue 0
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 class17 low dscp 61
class class2 low dscp 41
class class22 low dscp 60
class class3 low dscp 32
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
qos-scheduler qos-sched0
class class0
  bandwidth-percent 1
  buffer-percent 1
qos-scheduler qos-sched1
class class1
  bandwidth-percent 1
  buffer-percent 1
qos-map qos-map1
qos-scheduler qos-sched0
qos-scheduler qos-sched1

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
qos-map qos-map1
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
  qos-map qos-map1
  rewrite-rule rewrite-to-0

**Operational Commands**

show policy qos-map-info
show policy qos-scheduler-info

**Related Topics**

  access-list, on page 33
  class-map, on page 151
  cloud-qos, on page 155
  qos-map, on page 484
  qos-scheduler, on page 486
  rewrite-rule, on page 515
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address ip-address</strong></td>
<td>IP address of the collector and port number to use. The default collector</td>
</tr>
<tr>
<td><strong>port port number</strong></td>
<td>port is 4739.</td>
</tr>
<tr>
<td><strong>source-interface</strong></td>
<td>Interface to reach collector:</td>
</tr>
<tr>
<td><strong>interface-name</strong></td>
<td>Interface to use to send flows to the collector. <em>interface-name</em> can be a</td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet or 10-Gigabit Ethernet interface (ge) or a loopback</td>
</tr>
<tr>
<td></td>
<td>interface (loopback number).</td>
</tr>
<tr>
<td><strong>transport transport-type</strong></td>
<td>Transport Protocol. transport-type can be transport_tcp or transport_udp.</td>
</tr>
<tr>
<td><strong>vpn vpn-id</strong></td>
<td>VPN:</td>
</tr>
<tr>
<td></td>
<td>Number of the VPN in which the collector is located.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2.2</td>
<td>Added source-interface option.</td>
</tr>
</tbody>
</table>

**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

color

 vpn 0 interface tunnel-interface color—Identify an individual WAN transport tunnel (on vEdge routers only). In the Viptela 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 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>Added restrict option.</td>
</tr>
<tr>
<td>15.2</td>
<td>Added colors private3, private4, private5, and private6.</td>
</tr>
<tr>
<td>15.2</td>
<td>Supported application of restrict option to any color.</td>
</tr>
</tbody>
</table>

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.

```plaintext
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 239
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 | Community String:
|-------------------------|---------------------------------------------------------------
|                         | 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Allowed angle brackets in the community string.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
```
compatible rfc1583

Configuration Commands

**VM1**

```
vml(config)# vpn 1 router ospf
vml(config-ospf)# no compatible rfc1583
vml(config-ospf)# show config
vpn 1
  router
    ospf
      no compatible rfc1583
  
  
vml# show ospf process | include rfc1583
rfc1583-compatible false
vml#
```

**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**

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

**Syntax Descriptions**

<table>
<thead>
<tr>
<th>number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of HTTPS Connections:</td>
<td></td>
</tr>
<tr>
<td>Set the maximum number of HTTPS connections to a vManage application server.</td>
<td></td>
</tr>
<tr>
<td>Range:</td>
<td></td>
</tr>
<tr>
<td>1 through 512</td>
<td></td>
</tr>
<tr>
<td>Default:</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

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

```plaintext
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 72
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**

<table>
<thead>
<tr>
<th>rate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>rate</td>
<td>Baud Rate:</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

Change the console baud rate to 57600:

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

**Operational Commands**

```
show running-config system
```
**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**

<table>
<thead>
<tr>
<th>string</th>
<th>Name of Contact:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 (&quot; &quot;).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 — Configure a vSmart controller as a container within a vContainer host (on vContainer hosts only).

### Command Hierarchy

```
container
    instance instance-name
        allow-address prefix/length 0 [port] protocol
description "text"
image filename
interface interface-name
    host-ip-address prefix/length
memory megabytes
[no] shutdown
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **allow-address** | Address from which to access the container instance: Prefixes from which to access the container instance and the port and protocol to use to access the container instance. **prefix/length** is an IPv4 prefix. You can configure up to 64 prefixes, specifying one per **allow-address** command. To specify the port and protocol to use to access the instance, type a **0**, followed by the port and protocol:  
  - **0 all** — Open all ports and allow all protocols.  
  - **0 icmp** — Open access for ICMP traffic  
  - **0 port-number tcp** — Open the specified port for TCP traffic.  
  - **0 port-number udp** — Open the specified port for UDP traffic. Typically, the prefixes are those of other controller devices, including vBond orchestrators, vSmart controllers, and vManage NMSs. If you configure multiple **allow-address** commands, the IP addresses are cumulative. That is, a second **allow-address** command does not overwrite the addresses that you configured with the first **allow-address** command. To delete a single IP addresses from the list of allowed addresses, use the **no allow-address ip-address** command. |
<p>| <strong>[no] shutdown</strong> | Enable or disable the instance: To enable a container instance, use the <strong>no shutdown</strong> command. To disable a container instance, use the <strong>shutdown</strong> command. |
| <strong>image filename</strong> | Image to use on the vSmart controller: Name of the software image to use on the vSmart controller. This image must already be installed on the vContainer host. |
| <strong>description &quot;text&quot;</strong> | Instance description: Text description of the container instance. The text can be a maximum of 32 characters. If it includes spaces, enclose the entire string in quotation marks (&quot; &quot;). |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance instance-name</td>
<td>Instance Name</td>
</tr>
<tr>
<td></td>
<td>Name of the instance. It can be a string up to 32 characters long.</td>
</tr>
<tr>
<td>interface interface-name</td>
<td>Interface Associated with the Instance:</td>
</tr>
<tr>
<td>host-ip-address ip-address</td>
<td>Name of the interface associated with the container instance and the interface's IP address. Specify interface-name in the format <code>eth number</code>, where number is an integer starting with 0. <code>eth0</code> is the management interface, and <code>eth1</code> is the transport interface.</td>
</tr>
<tr>
<td>memory megabytes</td>
<td>Memory To Allocate to the Instance:</td>
</tr>
<tr>
<td></td>
<td>Amount of memory to allocate to the container instance.</td>
</tr>
<tr>
<td></td>
<td>Range: 256 through 16384 MB</td>
</tr>
<tr>
<td></td>
<td>Default: 512 MB</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3.2</td>
<td>Added allow-address command.</td>
</tr>
</tbody>
</table>

**Example**

Configure IP address lists, and configure containers for three vSmart controllers on a container host:

```bash
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

  ip address-list, on page 313
security control—Configure the protocol to use on control plane connections to a vSmart controller (on vEdge routers, vManage NMSs, and vSmart controllers only).

vManage Feature Template
For vEdge routers, vManage NMSs, and vSmart controllers only:
Configuration ► Templates ► Security

Command Hierarchy

Synax Description

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>tls-port</td>
<td>port-number</td>
<td>TLS Port Number: For TLS tunnels only, port number to use for TLS control plane connections. Range: 1025 through 65535 Default: 23456</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Change the control-plane protocol to TLS:

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 vManage NMS. 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.

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 vSmart controllers. This routing information is shared across all the TLOCs on the router. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3.3</td>
<td>Supported a vEdge router establishes only one control connection to the vManage NMS</td>
</tr>
<tr>
<td>15.4</td>
<td>This command is deprecated. Use the max-control-connections command instead</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
control-direction

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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-name</strong></td>
</tr>
<tr>
<td>Name of the control policy to configure or to apply to a site list. <em>policy-name</em> can be up to 32 characters long.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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.

**vManage Feature Template**

For all Cisco vEdge devices:

Configuration ► Templates ► System

**Command Hierarchy**

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

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>Rate</strong></th>
<th>Flow Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the maximum rate of DTLS control session traffic, in packets per second (pps).</td>
</tr>
<tr>
<td></td>
<td>Range:</td>
</tr>
<tr>
<td></td>
<td>1 through 65535 pps</td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>300 pps</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

Change the maximum control session traffic rate to 250 pps:

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

**Operational Commands**

show running-config system

**Related Topics**

- `host-policer-pps`, on page 277
- `icmp-error-pps`, on page 278
- `policer`, on page 453
**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**

<table>
<thead>
<tr>
<th>number</th>
<th>Controller Group Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Numeric identifier of the controller group to which the vSmart controller belongs.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 100</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 186
- [exclude-controller-group-list](#), on page 244
- [max-control-connections](#), on page 392
- [max-omp-sessions](#), on page 399
controller-group-list

List of controller groups to which the vEdge router belongs (on vEdge routers only). A vEdge router can form control connections only with the vSmart controllers that are in the same controller group.

**Command Hierarchy**

```
system
    controller-group-list number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>number</th>
<th>List of Controller Groups:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifier of one or more vSmart controller groups to which the vEdge router belongs. You configure this identifier on the vSmart controller, using the <code>system controller-group-id</code> command.</td>
</tr>
<tr>
<td></td>
<td>The number of controller groups cannot exceed the maximum number of control connections configured on the router.</td>
</tr>
</tbody>
</table>

**Example**

Allow a vEdge router to establish control connections to the vSmart controllers in groups 1 and 2:

```
vEdge(config)# system controller-group-list 1 2
vEdge(config)# commit and-quit
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Operational Commands**

- show control affinity config
- show control affinity status
- show control connections
- show control local-properties

**Related Topics**

- `controller-group-id`, on page 185
- `exclude-controller-group-list`, on page 244
max-control-connections, on page 392
max-omp-sessions, on page 399
**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**

```
<table>
<thead>
<tr>
<th>number</th>
<th>Cost of the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 1 through 65535</td>
<td></td>
</tr>
</tbody>
</table>
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>country</code></td>
<td>Country in which the WLAN vEdge router is installed.</td>
</tr>
<tr>
<td>Values:</td>
<td>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</td>
</tr>
<tr>
<td>Default:</td>
<td>United States</td>
</tr>
</tbody>
</table>

**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+IEZB2voQpeEoSR4ia9JqgDsPNoHukAb8fvxAg5I=
    no shutdown
```
interface vap3
  ssid  tb31_pm6_5ghz_vap3
  data-security  wpa2-enterprise
  mgmt-security  optional
  radius-servers  tag1
  no shutdown

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Operational Commands

clear wlan radius-stats
show wlan clients
show wlan interfaces
show wlan radios
show wlan radius

Related Topics

channel, on page 145
channel-bandwidth, on page 147
radius, on page 488
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>secret-key password</code></td>
<td>Password: Password that the RADIUS or other authentication server uses to access the vEdge router 802.1X interface.</td>
</tr>
<tr>
<td><code>port port-number</code></td>
<td>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 802.1X interfaces on a vEdge router, you must configure each interface to use a different UDP port. Range: 1 through 65535 Default: 3799</td>
</tr>
<tr>
<td><code>client ip-address</code></td>
<td>RADIUS Server IP Address: IP address of the RADIUS authentication server or other authentication server from which to accept CoA requests.</td>
</tr>
</tbody>
</table>
require-timestamp

Timesteps:

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 $4$L3rwZms1ic8zj4Bg1EFXKw==
  !
  !
  !
**Operational Commands**

clear dot1x client
show dot1x clients
show dot1x interfaces
show dot1x radius
show system statistics

**Related Topics**

radius, on page 488
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

<table>
<thead>
<tr>
<th>policy-name</th>
<th>Data Policy Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the localized data policy to configure or to apply to a list of sites in the overlay network.</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 32</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Configure and apply a simple data policy

vSmart# show running-config 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 640
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

<table>
<thead>
<tr>
<th>security</th>
<th>Data Security Method:</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>No security is applied to the WLAN data. This is the default.</td>
</tr>
<tr>
<td>wpa-enterprise</td>
<td>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.</td>
</tr>
<tr>
<td>wpa-personal</td>
<td>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.</td>
</tr>
<tr>
<td>wpa/wpa2-enterprise</td>
<td>Enable both WPA and WPA2 security in conjunction with a RADIUS authentication server. Configure the RADIUS server to use with the radius-servers command.</td>
</tr>
<tr>
<td>wpa/wpa2-personal</td>
<td>Enable both WPA and WPA2 security using only a username and password for authentication. Configure the password with the wpa-personal-key command.</td>
</tr>
<tr>
<td>wpa2-enterprise</td>
<td>Enable WPA2 security in conjunction with a RADIUS authentication server. Configure the RADIUS server to use with the radius-servers command.</td>
</tr>
<tr>
<td>wpa2-personal</td>
<td>Enable WPA2 security using only a username and password for authentication. Configure the password with the wpa-personal-key command.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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+IEZB2vcQpeEoSR4ia9JqgD8PN0hukAb8fvxAq5I=
     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 401
- radius, on page 488
- radius-servers, on page 492
- wpa-personal-key, on page 648
**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
```

<table>
<thead>
<tr>
<th>seconds</th>
<th>Dead Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The default dead interval of 40 seconds is four times the default hello interval of 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 40 seconds</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 268
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

<table>
<thead>
<tr>
<th>interval seconds</th>
<th>Liveness Detection Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>retries number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number of Retries:</td>
</tr>
<tr>
<td>How many unacknowledged IKE Hello packets to send before declaring the IKE peer to be dead.</td>
</tr>
<tr>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td>Default: 3</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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)**

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.

**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 (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Add application-aware routing.</td>
</tr>
<tr>
<td>18.2</td>
<td>Add zone-based firewall policy.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>originate metric-type type 1</td>
<td>Advertise Type 1 External Routes:</td>
</tr>
<tr>
<td></td>
<td>Advertise the default route as an OSPF Type 1 external route.</td>
</tr>
<tr>
<td>originate metric-type type 2</td>
<td>Advertise Type 2 External Routes:</td>
</tr>
<tr>
<td></td>
<td>Advertise the default route as an OSPF Type 2 external route.</td>
</tr>
<tr>
<td>originate always</td>
<td>Always Advertise the Default Route:</td>
</tr>
<tr>
<td></td>
<td>Always advertise the default route in an OSPF routing domain.</td>
</tr>
<tr>
<td>originate metric metric</td>
<td>Assign a Metric to the Default Route:</td>
</tr>
<tr>
<td></td>
<td>Set the metric to use to generate the default route.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 16777214</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.1</td>
<td>Remove default value for originate metric</td>
</tr>
</tbody>
</table>

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
!
!

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**

<table>
<thead>
<tr>
<th>Syntx</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>VLAN Identifier: Identifier of the VLAN for 802.1X–compliant clients that are successfully authenticated by the RADIUS server.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 92
- [auth-reject-vlan](#), on page 100
- [bridge](#), on page 136
- [guest-vlan](#), on page 262
- [radius](#), on page 488
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>text</code></td>
<td>Text Description</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 411
**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 ]
```

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>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 (&quot;&quot;).</td>
</tr>
<tr>
<td>group-names</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.3</td>
<td>Add support for four IP addresses on a single DHCP helper interface.</td>
</tr>
<tr>
<td>17.2.2</td>
<td>Add support for eight IP addresses on a single DHCP helper interface.</td>
</tr>
</tbody>
</table>

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)# dhcp-helper 10.22.11.1
vEdge(config)# 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
  no shutdown
!
!

Operational Commands

show running-config vpn interface

Related Topics

dhcp-server, on page 214
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 72
  dhcp-helper, on page 212
**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**

<table>
<thead>
<tr>
<th>inside</th>
<th>outside</th>
<th>Direction To Perform Network Address Translation: Direction in which to perform network address translation. It can be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 239
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
distance

Define the BGP route administrative distance based on route type (on vEdge routers only).

vManage Feature Template

For vEdge routers only:
Configuration ► Templates ► BGP

Command Hierarchy

```
vpn vpn-id
  router
    bgp
distance
      external number
      internal number
      local number
```

Syntax Description

<table>
<thead>
<tr>
<th>external number</th>
<th>Distance for External Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the administrative distance for routes learned from a neighbor that is external to the autonomous system.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>internal number</th>
<th>Distance for Internal Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the administrative distance for routes learned from another BGP router within the same autonomous system.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>local number</th>
<th>Distance for Local Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the administrative distance for local routes. Local routes are networks configured with the bgp address-family network command. By default, a route received locally from BGP is preferred over a route received from OMP.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
Example

Have BGP prefer routes learned from OMP:

vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 router bgp 1
vEdge(config-bgp-1)# distance external 10
vEdge(config-bgp-1)# distance local 50
vEdge(config-bgp-1)# show configuration
vpn 1
  router
    bgp 1
      distance external 10
      distance local 50
    !
  !
  !

Operational Commands

show bgp routes
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>external number</code></td>
<td>Distance for External Routes:</td>
</tr>
<tr>
<td></td>
<td>Set the OSPF distance for routes learned from other domains.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110</td>
</tr>
<tr>
<td><code>inter-area number</code></td>
<td>Distance for Interarea Routes</td>
</tr>
<tr>
<td></td>
<td>Set the distance for routes coming from one area into another.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110</td>
</tr>
<tr>
<td><code>inter-area number</code></td>
<td>Distance for Intra-Area Routes</td>
</tr>
<tr>
<td></td>
<td>Set the distance for routes within an area.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Add support for IPv6 DNS server addresses.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Domain ID default changed to 1.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
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
```
Configuration Commands

!  
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 488
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(full</td>
<td>Duplex Mode:</td>
</tr>
<tr>
<td>half)</td>
<td>Set the interface to run in full-duplex or half-duplex mode.</td>
</tr>
<tr>
<td></td>
<td>Default: full</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Support for autonegotiation added.</td>
</tr>
</tbody>
</table>

**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 114
  - speed, on page 539
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

<table>
<thead>
<tr>
<th>Time to Live for BGP Connections to External Peers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time to live (TTL) for BGP connections to external peers.</td>
</tr>
<tr>
<td>Range: 0 to 255</td>
</tr>
<tr>
<td>Default: 1</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

### Example

Enable EBG 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
    !
    !
```

---

**Configuration Commands**

---

232
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**

The **layer4** flag uses 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

Use the Layer 4 source and destination ports in the ECMP 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

<table>
<thead>
<tr>
<th>number</th>
<th>Number of OMP Paths:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum number of OMP paths that can be installed in a vEdge router's route table.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 16</td>
</tr>
<tr>
<td></td>
<td>Default: 4</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3.3</td>
<td>Installing ECMP routes only if the next hop can be resolved added.</td>
</tr>
</tbody>
</table>

Operational Commands

show omp routes
eco-friendly-mode

Configure a vEdge Cloud router not 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Enable eco-friendly mode:

```
vEdge-Cloud# config
vEdge-Cloud(config)# system eco-friendly-mode
```

Operational Commands

```
show running-config system
```
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
distribute-list {acl-num | acl-name | gateway address | prefix prefix-name | route-map route-map-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 ospf 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
**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encapsulation:</strong></td>
<td>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. You must explicitly configure an encapsulation.</td>
</tr>
<tr>
<td><strong>Preference:</strong></td>
<td>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. Range: 0 through 4294967295 (2^32 – 1) Default: 0</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>preference and weight commands moved from under tunnel-interface to under encapsulation.</td>
</tr>
<tr>
<td>15.2</td>
<td>Add GRE encapsulation.</td>
</tr>
</tbody>
</table>

---

**Example**

Create a GRE tunnel and direct voice traffic to it:

```plaintext
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
!```

---

**Configuration Commands**

240
! 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 126
- color, on page 164
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

<table>
<thead>
<tr>
<th>ip-address</th>
<th>Address To Exclude:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address to exclude from the DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td>To specify multiple individual addresses, list them in a single <strong>exclude</strong> command, separated by a space (for example, <code>exclude 1.1.1.1 2.2.2.2 3.3.3.3</code>). To specify a range of addresses, separate them with a hyphen (for example, <code>exclude 1.1.1.1-1.1.1.10</code>).</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>Support for command ranges added.</td>
</tr>
</tbody>
</table>

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.

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 185
controller-group-list, on page 186
max-control-connections, on page 392
max-omp-sessions, on page 399
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

```plaintext
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Default timeout value changed to 10 minutes.</td>
</tr>
</tbody>
</table>

Example

Configure a cflowd template:

```plaintext
vSmart# show running-config policy
cflowd-template test-cflowd-template
collector vpn 1 address 172.16.255.14 port 11233
default-time 60
flow-active-timeout 90
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 249
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 gslot/port
    flow-control control
```

Syntax Description

<table>
<thead>
<tr>
<th>control</th>
<th>Flow Control Direction:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure flow control on an interface. control an be autoneg, both, egress, ingress, or none.</td>
<td></td>
</tr>
<tr>
<td>Default: autoneg</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Timeout Due to Inactivity:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 <strong>clear app cflowd flows</strong> command.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 60 seconds (1 minute)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Default timeout value changed to 1 minute.</td>
</tr>
</tbody>
</table>

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
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 246
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

<table>
<thead>
<tr>
<th>number</th>
<th>Sampling Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65536</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 Description
None

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>latitude</strong></td>
<td>decimal-degrees</td>
</tr>
<tr>
<td><strong>longitude</strong></td>
<td>decimal-degrees</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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](http://link), on page 356
- [location](http://link), on page 354
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

```plaintext
omp
graceful-restart
```

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no omp graceful-restart</code></td>
<td>Disable Graceful Restart</td>
</tr>
<tr>
<td><code>omp timers graceful-restart-timer 0</code></td>
<td>By default, OMP graceful restart is enabled on vEdge routers and vSmart controllers. Use one of these two commands to disable it.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Operational Commands

show omp peers detail

Related Topics

timers, on page 580
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication</strong></td>
<td>Group Authentication: Authentication to use for members of the group. <em>authentication</em> can be one of the following:</td>
</tr>
<tr>
<td>• auth-no-priv—Provide authentication using the HMAC-MD5 or HMAC-SHA algorithm.</td>
<td></td>
</tr>
<tr>
<td>• auth-priv—Provide authentication using the HMAC-MD5 or HMAC-SHA algorithm, and provide CBC DES 56-bit encryption.</td>
<td></td>
</tr>
<tr>
<td>• no-auth-no-priv—Provide authentication based on a username.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group</strong></td>
<td>Group Name:</td>
</tr>
<tr>
<td><strong>group-name</strong></td>
<td>Name of the SNMPv3 group. <em>group-name</em> can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (&quot; &quot;).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>view</strong></td>
<td>SNMP View:</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>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 (&quot; &quot;).</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Operational Commands

```
show running-config snmp
```

Related Topics

- [user](user) on page 619
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**

<table>
<thead>
<tr>
<th>number</th>
<th>Group Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td>2</td>
<td>Use the 1024-bit more modular exponential (MODP) Diffie-Hellman group.</td>
</tr>
<tr>
<td>14</td>
<td>Use the 2048-bit MODP Diffie-Hellman group.</td>
</tr>
<tr>
<td>15</td>
<td>Use the 3072-bit MODP Diffie-Hellman group.</td>
</tr>
<tr>
<td>16</td>
<td>Use the 4096-bit MODP Diffie-Hellman group.</td>
</tr>
</tbody>
</table>

Default: 16

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 405
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

<table>
<thead>
<tr>
<th>nanoseconds</th>
<th>Guard Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the guard interval. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 800—Normal guard interval, which is 800 nanoseconds. This is the default value for 2.4-GHz radio frequencies.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VLAN Identifier:</th>
<th>Identifier of the VLAN into which to place non-802.1X–enabled clients.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>1 through 4094</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 vlan-id 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 92
  auth-reject-vlan, on page 100
  bridge, on page 136
  default-vlan, on page 208
  mac-authentication-bypass, on page 375
  radius, on page 488
**hello-interval**

Configure the keepalive interval between Hello packets sent on a DTLS or TLS WAN transport connection.

**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

**Command Hierarchy**

```
vpn 0
    interface interface-name
    tunnel-interface
    hello-interval milliseconds
```

**Syntax Description**

<table>
<thead>
<tr>
<th>milliseconds</th>
<th>Hello Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.)</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

Range: 100 through 600000 milliseconds (10 minutes)

Default: 1000 milliseconds (1 second)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2</td>
<td>Maximum interval changed from 60 seconds to 10 minutes.</td>
</tr>
<tr>
<td>16.2.1</td>
<td>Add requirement that hello tolerance must be at least 2 times the hello interval.</td>
</tr>
</tbody>
</table>

Example

Decrease the amount of keepalive traffic sent between a vEdge router and Viptela controller devices:

```plaintext
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

To display the negotiated hello interval and hello tolerance values:

- show control connections detail
- show orchestrator connections detail

Related Topics

- `bfd color`, on page 126
- `hello-tolerance`, on page 270
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**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Hello Interval Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td>How often to send PIM hello messages. Hello messages advertise that PIM is enabled on the router.</td>
<td></td>
</tr>
<tr>
<td>Range: 1 through 3600 seconds</td>
<td></td>
</tr>
<tr>
<td>Default: 30 seconds</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Hello Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time interval at which the vEdge router sends OSPF hello packets to its neighbors.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 199
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 all 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**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Hello Tolerance Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.)</td>
</tr>
</tbody>
</table>

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 of 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2</td>
<td>Maximum tolerance increased from 1 minute to 10 minutes.</td>
</tr>
<tr>
<td>16.2.1</td>
<td>Add requirement that hello tolerance must be at least 2 times the hello interval.</td>
</tr>
</tbody>
</table>

## Example

Decrease the amount of keepalive traffic sent between a vEdge router and Viptela controller devices:

```bash
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 126
- hello-interval, on page 264
**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**

<table>
<thead>
<tr>
<th><strong>string</strong></th>
<th>Hostname:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the vEdge router within the VPN. The name can be a maximum of 128 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ip-address</strong></th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPv4 or IPv6 address to associate with the router. You can associate up to 8 total IP addresses with a hostname.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Add support for IPv6 addresses.</td>
</tr>
</tbody>
</table>

**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
    ...```

**Configuration Commands**
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**

<table>
<thead>
<tr>
<th>multi-auth</th>
<th>Multiple Authenticated Clients:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A single 802.1X interface grants access to multiple authenticated clients on data VLANs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>multi-host</th>
<th>Multiple Clients:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>single-host</th>
<th>Single Client:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The 802.1X interface grants access only to the first authenticated client. All other clients attempting access are denied and dropped.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 488
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

<table>
<thead>
<tr>
<th>string</th>
<th>Hostname:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 (&quot; &quot;).</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Increase range from 20000 pps to 25000 pps, and change default from 5000 pps to 20000 pps.</td>
</tr>
</tbody>
</table>

**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 184
- icmp-error-pps, on page 278
- policer, on page 453
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-error-pps</td>
<td>Disable ICMP Error Message Generation:</td>
</tr>
<tr>
<td>0</td>
<td>Configure a value of 0 to have a policer generate no ICMP error messages.</td>
</tr>
<tr>
<td>rate</td>
<td>ICMP Error Message Generation Rate:</td>
</tr>
<tr>
<td></td>
<td>How many ICMP error messages a policer can generate or receive, in packets per second (pps).</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 200 pps</td>
</tr>
<tr>
<td></td>
<td>Default: 100 pps</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 184
- host-policer-pps, on page 277
- policer, on page 453
icmnp-rediect-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 PPP
Configuration ► 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 72
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**

<table>
<thead>
<tr>
<th>minutes</th>
<th>Timeout Value:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 300 minutes (5 hours)</td>
</tr>
<tr>
<td></td>
<td>Default: CLI session does not time out</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Example**

Configure CLI sessions to timeout 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
  !
```

**Operational Commands**

- clear igmp interface
- clear igmp protocol
- clear igmp statistics
- show igmp groups
show igmp interface
show igmp statistics
show igmp summary
ike

Configure the Internet Key (IKE) protocol parameters for an IPsec tunnel (on vEdge routers only). Cisco SD-WAN supports IKE version 1, as defined in RFC 2409, The Internet Key Exchange (IKE) and IKE version 2, as defined in RFC 7296, Internet Key Exchange Protocol, Version 2 (IKE v2).

vManage Feature Template

For vEdge routers only:

Configuration ► Templates ► VPN Interface IPsec

Command Hierarchy

```
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
```

Syntax Description

<table>
<thead>
<tr>
<th>(version number)</th>
<th>IKE Version:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the version of the IKE protocol to use. Cisco SD-WAN supports IKE version 1 and IKE version 2.</td>
</tr>
<tr>
<td></td>
<td>Values: 1, 2</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

View the default IKE configuration:

```
vEdge# show running-config vpn 1 interface ipsec1 ike
vpn 1
   interface ipsec1
     ike
        version 1
        mode main
        rekey 14400
```
ciphersuite aes256-shal
    group 16
    authentication-type
    pre-shared-key
    pre-shared-secret viptela
    
    
    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 implicit 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 72
- log-frequency, on page 357
### 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 kbps (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
dot1x
  accounting-interval seconds
  acct-req-attr attribute-number (integer integer | octet octet | string string)
  auth-fail-vlan vlan-id
domain-name domain-name
  interface mtu mtu
tftp-servers ip-address
static-lease mac-address ip ip-address host-name hostname
  accounting-interval seconds
  acct-req-attr attribute-number (integer integer | octet octet | string string)
auth-reject-vlan vlan-id
auth-order (mab | radius)
auth-req-attr attribute-number (integer integer | octet octet | string string)
control-direction direction
```
Configuration Commands

```
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
```
<table>
<thead>
<tr>
<th>Configuration Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
</tr>
</tbody>
</table>

authentication {chap | pap} hostname name password password
pppoe-client (on vEdge routers only)
  ppp-interface name
profile profile-id (on vEdge routers only)
gos-map name (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)
upgrade-confirm minutes
vrrp group-name (on vEdge routers only)
priority number
timer seconds
track-omp
Syntax Description

```
interface-name
```

<table>
<thead>
<tr>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the interface.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Add support for natpool interface type.</td>
</tr>
<tr>
<td>15.3.3</td>
<td>Add support for ppp interfaces.</td>
</tr>
<tr>
<td>15.4.1</td>
<td>Add support for GRE interfaces.</td>
</tr>
<tr>
<td>17.1</td>
<td>Add support for IPsec interfaces.</td>
</tr>
</tbody>
</table>

Example

Configure a tunnel interface in VPN 0 on a vEdge router:

```
vEdge# show running-config vpn 0
```
interface ge0/0
ip address 10.1.15.15/24
tunnel-interface
color lte
allow-service dhcp
allow-service dns
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] shutdown</code></td>
<td>Enable or Disable the Interface:</td>
</tr>
<tr>
<td></td>
<td>By default, an interface in a bridge domain is disabled. To enable it, include</td>
</tr>
<tr>
<td></td>
<td>the <code>no shutdown</code> command.</td>
</tr>
<tr>
<td><code>description text</code></td>
<td>Interface Description:</td>
</tr>
<tr>
<td></td>
<td>Text description of the interface. If <code>text</code> contains spaces, enclose it in</td>
</tr>
<tr>
<td></td>
<td>quotation marks.</td>
</tr>
<tr>
<td><code>interface-name</code></td>
<td>Interface Name:</td>
</tr>
<tr>
<td></td>
<td>Name of the interface to associate with the bridging domain. Specify <code>interface-name</code> in the format <code>ge slot/port</code>.</td>
</tr>
<tr>
<td><code>native-vlan</code></td>
<td>Native VLAN:</td>
</tr>
<tr>
<td></td>
<td>Treat untagged traffic as belonging to the VLAN in that particular bridge. Only</td>
</tr>
<tr>
<td></td>
<td>one VLAN associated with an interface can be configured to run as native</td>
</tr>
<tr>
<td></td>
<td>VLAN. Native VLAN is disabled by default.</td>
</tr>
<tr>
<td><code>static-mac-address mac-address</code></td>
<td>Static MAC Address</td>
</tr>
<tr>
<td></td>
<td>Manually add static MAC address entries for an interface in a bridge domain.</td>
</tr>
</tbody>
</table>

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>BRIDGE</th>
<th>INTERFACE</th>
<th>VLAN</th>
<th>STATUS</th>
<th>STATUS</th>
<th>TYPE</th>
<th>IINDEX</th>
<th>MTU</th>
<th>PKTS</th>
<th>OCTETS</th>
<th>PKTS</th>
<th>OCTETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ge0/2</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan 34</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ge0/5</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan 36</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ge0/6</td>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>vlan 38</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ge0/2</td>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td>vlan 40</td>
<td>1500</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>242</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Status</td>
<td>Speed</td>
<td>Duplex</td>
<td>MAC Address</td>
<td>VLAN</td>
<td>MTU</td>
<td>Index</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
<td>------</td>
<td>-----</td>
<td>-------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge0/5</td>
<td>Up</td>
<td>1000M</td>
<td>Full</td>
<td>00:00:00:00:00:00</td>
<td>42</td>
<td>1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge0/6</td>
<td>Up</td>
<td>1000M</td>
<td>Full</td>
<td>00:00:00:00:00:00</td>
<td>44</td>
<td>1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge0/2</td>
<td>Up</td>
<td>1000M</td>
<td>Full</td>
<td>00:00:00:00:00:00</td>
<td>null</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge0/5</td>
<td>Up</td>
<td>1000M</td>
<td>Full</td>
<td>00:00:00:00:00:00</td>
<td>null</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge0/6</td>
<td>Up</td>
<td>1000M</td>
<td>Full</td>
<td>00:00:00:00:00:00</td>
<td>null</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the interface to participate in the IGMP domain.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 vEdge 100wm 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:

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] shutdown</code></td>
<td>Disable or Enable the VAP Interface:</td>
</tr>
<tr>
<td></td>
<td>Disable or enable the VAP interface.</td>
</tr>
<tr>
<td><code>vap number</code></td>
<td>VAP Interface:</td>
</tr>
<tr>
<td></td>
<td>VAP instance.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 3</td>
</tr>
<tr>
<td><code>description</code></td>
<td>VAP Interface Description:</td>
</tr>
<tr>
<td><code>text</code></td>
<td>Text description of the VAP interface. The text can be from 4 through 64 characters long.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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  wpa2-personal
    mgmt-security  optional
    wpa-personal-key  $4$BES+IEZB2vcQpeEoSR4ia9JqgDsPNo8ukAb8fvxAg5I=
    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**

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the interface, in the format ge slot/port or loopback number.</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the interface, in the format <code>ge slot/port</code>..</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 gre number
  access-list acl-name
  block-non-source-ip
  clear-dont-fragment
  description text
  ip address prefix/length
  keepalive seconds retries
  mtu bytes
  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**

<table>
<thead>
<tr>
<th><strong>gre number</strong></th>
<th>Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the GRE interface. <code>number</code> can be a value from 1 through 255.</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4.1</td>
<td>Support for GRE interfaces added.</td>
</tr>
</tbody>
</table>

**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
    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
    tcp-mss-adjust bytes
    tunnel-destination (dns-name | ipv4-address)
    (tunnel-source ip-address | tunnel-source-interface interface-name)
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>description text</strong></th>
<th>Interface Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 (&quot; &quot;).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ipsec number</strong></th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of the ipsec interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>18.2</td>
<td>Add support for IPsec tunnels in VPN 0.</td>
</tr>
</tbody>
</table>

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
            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**

<table>
<thead>
<tr>
<th><strong>irb</strong> &lt;br&gt; <strong>number</strong></th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the interface. number can from 1 through 63, and it must be the same number as the identifier of the bridging domain that the IRB is connected to, as configured with the bridge command.</td>
<td></td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Configure two IRB interfaces:

```bash
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

vEdge# show running-config vpn 3
vpn 3
interface irb3
  ip address 3.3.3.15/24
  no shutdown
```

Operational Commands

show interface

Related Topics

bridge, on page 136
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
    qos-map name
    rewrite-rule name
    shaping-rate name
    shutdown
    speed speed
    static-ingress-qos number
    tcp-mss-adjust bytes
    tloc-extension interface-name
```

Syntax Description

<table>
<thead>
<tr>
<th>ppp number</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of the PPP interface. number can be from 1 through 31.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Add support for IPv6.</td>
</tr>
</tbody>
</table>
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 $4$OHHjdmsC6Mb8j4BgLEFKKw==
    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
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

<table>
<thead>
<tr>
<th>ipv4-prefix/length</th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
```
Configuration Commands

Operational Commands

show interface

show ipv6 interface

Related Topics

ip dhcp-client, on page 315
ipv6 address, on page 328
ipv6 dhcp-client, on page 330
system-ip, on page 554
ip secondary-address, on page 323
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface eth number</td>
<td>Interface Name: Name of the interface on the container. The first interface is <strong>eth1</strong>.</td>
</tr>
<tr>
<td>ip address-list prefix/length</td>
<td>IP Address List: Network address available on the interface.</td>
</tr>
<tr>
<td>vpn vpn-id</td>
<td>VPN Identifier: VPN for the interfaces. <strong>vpn-id</strong> can be either 0 (for the WAN transport VPN) or 512 (for the management VPN).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
!
nvpn 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
!
nvpn 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 175
**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**

<table>
<thead>
<tr>
<th>dhcp-distance number</th>
<th>Administrative Distance:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the administrative distance of routes learned from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 311
- ipv6 address, on page 328
- ipv6 dhcp-client, on page 330
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

<table>
<thead>
<tr>
<th><strong>gre number [gre number2]</strong></th>
<th>GRE Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>prefix/length</strong></th>
<th>Prefix of GRE Static Route:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 321
- keepalive, on page 338
- nat, on page 417
**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**

| **ipsecnumber [ipsecnumber2]** | 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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-shal
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 317
  ip route, on page 321
  keepalive, on page 338
  nat, on page 417
ip route

Configure an IPv4 static route in a VPN.

**vManage Feature Template**

For all vEdge devices:

Configuration ► Templates ► VPN

**Command Hierarchy**

```plaintext
vpn vpn-id
  ip route prefix/length next-hop [administrative-distance]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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. |

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
Example

Configure a static route to the prefix 10.0.0.1/24 via the next hop at 10.10.0.1:

```
vpn 0
 ip route 10.0.0.1/24 10.10.0.1
```

Operational Commands

- `show ip routes` (for IPv4 routes)
- `show ipv6 routes`

Related Topics

- `ip gre-route`, on page 317
- `ipv6 route`, on page 332
- `nat`, on page 417
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>IP Address: IPv4 address of the interface, in decimal four-part dotted notation. You can configure secondary IPv4 addresses for <code>ge</code> and <code>irb</code> 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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 311
- [ip dhcp-client](#), on page 315
- [ipv6 address](#), on page 328
- [ipv6 dhcp-client](#), on page 330
- [system-ip](#), on page 554
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 Description**

None

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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-shal
```

**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 283
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.1</td>
<td><strong>iptables-enable</strong> is enabled by default.</td>
</tr>
</tbody>
</table>

Example

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.

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 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 311
- ipv6 address, on page 328
- ipv6 dhcp-client, on page 330
- system-ip, on page 554
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 Viptela 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

<table>
<thead>
<tr>
<th><code>dhcp-distance number</code></th>
<th>Administrative Distance:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the administrative distance of routes learned from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><code>dhcp-rapid-commit</code></th>
<th>Rapid Commit:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable the DHCPv6 rapid commit option to speed up the assignment of IP addresses.</td>
</tr>
<tr>
<td></td>
<td>Rapid commit uses a two-message exchange to expedite address assignment.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
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 311
- `ipv6 address`, on page 328
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

<table>
<thead>
<tr>
<th>Prefix/Length</th>
<th>Address of Static Route:</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix/length</td>
<td>IPv6 address of the static route, written as the prefix and prefix length.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administrative-Distance</th>
<th>Administrative Distance of Route:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Next-Hop</th>
<th>Next Hop towards the Destination:</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop</td>
<td>IPv6 address of the next hop to reach the static route. The next hop can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• ipv6-address—IP address of the next-hop router.</td>
</tr>
<tr>
<td></td>
<td>• null0—Next hop is the null interface. All packets sent to this interface are dropped without sending any ICMPv6 messages.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 321
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

!  !

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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Join/Prune Interval Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PIM join/prune message interval. vEdge routers send join/prune messages to their upstream RPF neighbor.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 60 seconds</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Keepalive Time: How often the GRE interface sends keepalive packets on the GRE tunnel. Range: 0 through 65535 seconds Default: 10 seconds</td>
</tr>
<tr>
<td>retries</td>
<td>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</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
## 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 601
- `tunnel-source`, on page 608
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 126
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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Lease Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How long DHCP-assigned addresses are valid.</td>
</tr>
<tr>
<td></td>
<td>Range: 60 through 4294967295 seconds</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Example

Set the DHCP lease time to 2 hours:

vEdge# config
Entering configuration mode terminal
vEdge(config)# vpn 1 interface ge0/4
vEdge(config)# 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

show dhcp interfaces

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
```
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

A 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.

**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.

**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.

**data-prefix-list** list-name

A 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.

**site-list** list-name

A 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

A 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 application-aware routing policy, you group policy sequences within VPN lists, with the policy **vpn-list sequence** command.

**color-list** list-name

A list 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*  

**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.

**ip-prefix**  *prefix/length*  

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.
### TLOC List

**tloc-list** `list-name`

**tloc** `address` `color` `encap` `encapsulation` 

* [preference value]

TLOC List:

List of one or more addresses 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

**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.

### Application List

**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.

`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.

`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`.

### Data Prefix List

**data-prefix-list** `list-name`

**ip-prefix** `prefix/length`

Data 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.
### site-list

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>site-list list-name</code></td>
<td>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 <code>site-id</code> 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 <code>apply-policy</code> command) by site list.</td>
</tr>
</tbody>
</table>

### site-id

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>site-id site-id</code></td>
<td></td>
</tr>
</tbody>
</table>

### tloc-list

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tloc-list list-name</code></td>
<td>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. <code>address</code> is the system IP address. <code>color</code> can be one of <code>3g</code>, <code>biz-internet</code>, <code>blue</code>, <code>bronze</code>, <code>custom1</code>, <code>custom2</code>, <code>custom3</code>, <code>default</code>, <code>gold</code>, <code>green</code>, <code>lte</code>, <code>metro-ethernet</code>, <code>mpls</code>, <code>private1</code> through <code>private6</code>, <code>public-internet</code>, <code>red</code>, and <code>silver</code>. <code>encapsulation</code> can be <code>gre</code> or <code>ipsec</code>. 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 <code>action accept</code> 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 <code>tloc</code> options, specifying one TLOC number in each option. In centralized data policy, you can refer to a TLOC list in <code>match route tloc-list</code> and match <code>tloc tloc-list</code> match conditions, and in <code>action accept</code> conditions.</td>
</tr>
</tbody>
</table>

### tloc

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tloc address color color</code></td>
<td></td>
</tr>
<tr>
<td>`encap (gre</td>
<td>ipsec)`</td>
</tr>
<tr>
<td><code>[preference value weight value]</code></td>
<td></td>
</tr>
</tbody>
</table>

### vpn-list

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpn-list list-name</code></td>
<td>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 <code>vpn</code> options, specifying one VPN number in each option. 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 <code>match vpn-list</code> 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.</td>
</tr>
</tbody>
</table>

### vpn

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpn vpn-id</code></td>
<td></td>
</tr>
</tbody>
</table>

### For Localized Control Policy:

### as-path

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-path path-list</code></td>
<td>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 (&quot; &quot;). To configure multiple AS paths in a single list, include multiple <code>as-path</code> options, specifying one AS path in each option.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-path path-list</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Commands

- `lists`
### BGP Communities:

List of one or 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.

### 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 0.0.0.0/0 ge 25` matches all IP prefixes with lengths from /25 through /32.
- **0.0.0.0/0 ge length1 le length2**, or **0.0.0.0/0 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.

### For Localized Data Policy (ACLs):

<table>
<thead>
<tr>
<th>data-prefix-list</th>
<th>IP Prefix:</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>List of one or more IP prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple <code>ip-prefix</code> options, specifying one prefix in each option.</td>
</tr>
</tbody>
</table>

### Configuration Commands

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Add support for overlapping sites in different site lists, and add support for IP multicast addresses.</td>
</tr>
</tbody>
</table>

### Example

**Configure a list of VPNs:**

```properties
policy
lists
vpn-list west-coast
vpn 20-30
```
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 39
- apply-policy, on page 81
- match, on page 380
- policy, on page 457
- sla-class, on page 535
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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	house-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 254
location, on page 356
**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**

<table>
<thead>
<tr>
<th>string</th>
<th>Device Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Text string that describes the location of the device. If the name contains spaces, enclose it in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 255</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 254
- location, on page 354
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

<table>
<thead>
<tr>
<th>number</th>
<th>Logging Frequency:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How often packet flows are logged.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Default: 1000. With this default, the logging frequency is rounded down to 512. So, by default, every 512th packet is logged.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>string</th>
<th>Location description:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Text string that describes the location of the device. If the name contains spaces, enclose it in quotation marks.</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 128</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 285
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 natpool number
  nat
  log-translations
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 239
- static, on page 544
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
      number
      size megabytes
      priority priority
### Syntax Description

<table>
<thead>
<tr>
<th>enable</th>
</tr>
</thead>
</table>
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.

<table>
<thead>
<tr>
<th>priority</th>
<th>Message priority:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. The default priority value is &quot;informational&quot;, so, by default, all syslog messages are recorded.</td>
</tr>
<tr>
<td></td>
<td>The priority level can be one of the following (in order of decreasing severity):</td>
</tr>
<tr>
<td></td>
<td>• Emergency—System is unusable (corresponds to syslog severity 0).</td>
</tr>
<tr>
<td></td>
<td>• Alert—Action must be taken immediately (corresponds to syslog severity 1).</td>
</tr>
<tr>
<td></td>
<td>• Critical—A serious condition (corresponds to syslog severity 2).</td>
</tr>
<tr>
<td></td>
<td>• Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3).</td>
</tr>
<tr>
<td></td>
<td>• Warning—A minor error condition (corresponds to syslog severity 4).</td>
</tr>
<tr>
<td></td>
<td>• Notice—A normal, but significant condition (corresponds to syslog severity 5).</td>
</tr>
<tr>
<td></td>
<td>• Informational—Routine condition (the default) (corresponds to syslog severity 6).</td>
</tr>
</tbody>
</table>
LogFileRotation:

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 is notified. 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 (10 MB), nor can you configure the number of rotations (10).

**rotate number size megabytes**

<table>
<thead>
<tr>
<th>Command</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>Files used to store syslog files changed.</td>
</tr>
<tr>
<td>16.3</td>
<td>Debug output is placed in the /var/log/tmplog/vdebug file, not the /var/log/vdebug file.</td>
</tr>
</tbody>
</table>

**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 367
  show crash
  show logging
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

<table>
<thead>
<tr>
<th>source-interface</th>
<th>interface-name</th>
<th>Interface for System Log Messages to Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
**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).

**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 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2.7</td>
<td>Support for multiple syslog servers added.</td>
</tr>
<tr>
<td>15.4</td>
<td><code>source-interface</code> command added.</td>
</tr>
</tbody>
</table>

### 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:

```bash
%Viptela - module - level - MessageID: text-of-syslog-message
```

In Releases 15.4 and later, each syslog message has the following format:
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:

```plaintext
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 361
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 Viptela devices:

Configuration ► Templates ► AAA

**Command Hierarchy**

```
  system
   aaa
    logs
      [no] audit-disable
      [no] netconf-disable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit-disable</td>
<td>Disable the logging of AAA events.</td>
</tr>
<tr>
<td></td>
<td>Default: These events are logged.</td>
</tr>
<tr>
<td>netconf-disable</td>
<td>Disable the logging of Netconf events.</td>
</tr>
<tr>
<td></td>
<td>Default: These events are logged.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 (on vEdge routers only). This configuration command is relevant only for a spoke vEdge router in a hub-and-spoke deployment scenario, where the spoke has a low-bandwidth link, such as an LTE link. You include this configuration command only on the spoke router, to minimize traffic sent between the hub and the spoke.

Setting a tunnel as a low-bandwidth link minimizes how often control traffic is sent over the link while ensuring that critical information, such as routing updates, are propagated in a timely fashion among vEdge routers. Also, on such links, application-aware routing data is collected only when user data is transmitted from the LAN to the WAN, to reduce BFD traffic on the link.

For vEdge routers with LTE modems, low-bandwidth-link is enabled by default. For other routers, this option is disabled by default.

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
      [no] low-bandwidth-link

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 genumber/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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 Viptela 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**

<table>
<thead>
<tr>
<th><strong>mac-address</strong></th>
<th>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.</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-authentication-bypass</td>
<td>Enable Authentication for Non-802.1X–Compliant Hosts: Turn on authentication for non-802.1X–compliant clients.</td>
</tr>
<tr>
<td>allow mac-address</td>
<td>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.</td>
</tr>
<tr>
<td>server</td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 488
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

<table>
<thead>
<tr>
<th>class class-name</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Match the specified class name. The name can be from 1 through 32 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>destination-port number</th>
<th>Destination Port:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 [-]).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>next-header protocol</th>
<th>Next Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>packet-length number</th>
<th>Packet Length:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 [-]).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>plp (high</th>
<th>low)</th>
<th>Packet Loss Priority:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
| source-port number | Source Port:  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 [-]).</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for IPv6 ACLs.</td>
</tr>
</tbody>
</table>

**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:

```bash
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 380
**match**

Define the properties that must be matched so that an IPv4 policy action can take effect (on vEdge routers and vSmart controllers only).

```plaintext
match
```

- `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.

```plaintext
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
    plp (high | low)
    protocol number
    source-data-prefix-list list-name
    source-ip prefix/length
    source-port number
```

**For Centralized Control Policy**

Configure on vSmart controllers only.

```plaintext
policy
  control-policy policy-name
  sequence number
  match
    route
      color color
      color-list list-name
      omp-tag number
      origin protocol
```
For Centralized Data Policy
Configure on vSmart controllers only.

```plaintext
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
        packet-length number
        plp (high | low)
        protocol number
        source-data-prefix-list list-name
        source-ip prefix/length
        source-port number
        tcp flag
  vpn-membership policy-name
    sequence number
      match
        vpn vpn-id
        vpn-list list-name
```

For Localized Control Policy
Configure on vEdge routers only.

```plaintext
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
```
For Localized Data Policy

Configure on vEdge routers only.

```text
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
        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.

```text
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>app-id app-id-name</strong></td>
<td>Application Identifier: Match the name of an application defined with a policy <strong>app-id</strong> command.</td>
</tr>
<tr>
<td><strong>destination-data-prefix-list list-name</strong></td>
<td>Destination Prefix or Port: Match a destination prefix or port. For prefixes, you can specify a single prefix or a list of prefixes. list-name is the name of a list defined with a policy lists <strong>prefix-list</strong> command. For the 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 [-]).</td>
</tr>
<tr>
<td><strong>dscp number</strong></td>
<td>DSCP: Match the specified DSCP value.</td>
</tr>
</tbody>
</table>
### Packet Loss Priority
- **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
- **protocol number**
  - **Protocol:**
  - Match the TCP or IP protocol number.

### Source Prefix or Port
- **source-data-prefix-list list-name**
  - **Source Prefix or Port:**
  - Match a source prefix or port. For prefixes, 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. For the 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 [-]).

### Split DNS
- **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.

### For Centralized Control Policy
- **color color**
  - **Color:**
  - Match an individual color or a group of colors defined with a policy lists color-list list.

### Domain
- **domain-id number**
  - **Domain:**
  - Match the domain identifier. Currently, the domain identifier can only be 1.

### OMP Tag
- **omp-tag number**
  - **OMP Tag:**
  - Match an OMP tag value in the route. number can be a value from 0 through 4294967295.

### Originating Address
- **originator ip-address**
  - **Originating Address:**
  - Match the IP address of the device from which the route was learned.

### Originating Protocol
- **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
| Preference | Preference:  
| number | Match the preference value in the route. |
| Prefix-list | Prefix:  
| list-name | Match one or more IP prefixes in a list defined with a policy lists prefix-list list. |
| Site-id | Site:  
| site-id | 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. |
| Site-list | TLOC from a List of TLOCs:  
| list-name | Match one of the TLOCs in the list defined with a policy lists tloc-list list. |
| TLOC address color color [encap encapsulation] | TLOC Identified by IP Address and Color:  
| tloc-list list-name | Match an individual TLOC identified by its IP address and color, and optionally, by its encapsulation.  
| color | 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:  
| vpn vpn-id | Match an individual VPN identifier or the VPN identifiers in a list defined with a policy lists vpn-list command. |
| vpn-list list-name |  |

For Centralized Data Policy

| Destination-data-prefix-list | Destination Prefix or Port:  
| list-name | Match a destination prefix or port. For prefixes, 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. For the 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 [-]). |
| destination-ip |  
| prefix/length destination-port number | DSCP:  
| number | Match the specified DSCP value. |
| Packet Length  
| packet-length number | Match packets of the specified length. number can be 0 through 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 [-]) |
| Packet Loss Priority:  
| plp (high | low) | 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:**

Match the TCP or IP protocol number.

**Source Prefix or Port:**

Match a source prefix or port. For prefixes, 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. For the 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 [-]).

**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:**

Match TCP flags. Flag can be syn.

**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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop list-name</td>
<td>Next Hop:</td>
</tr>
<tr>
<td></td>
<td>Next hop in the route. list-name is the name of an IP prefix list defined</td>
</tr>
<tr>
<td></td>
<td>with a policy lists prefix-list command.</td>
</tr>
<tr>
<td>omp-tag number</td>
<td>OMP Tag:</td>
</tr>
<tr>
<td></td>
<td>OMP tag number for use by BGP or OSPF.</td>
</tr>
<tr>
<td></td>
<td>number can be a value from 0 through 4294967295.</td>
</tr>
<tr>
<td>ospf-tag number</td>
<td>OSPF Tag:</td>
</tr>
<tr>
<td></td>
<td>OSPF tag value.</td>
</tr>
<tr>
<td></td>
<td>number can be a value from 0 through 4294967295.</td>
</tr>
<tr>
<td>peer ip-address</td>
<td>Peer Address:</td>
</tr>
<tr>
<td></td>
<td>IP address of the peer.</td>
</tr>
<tr>
<td>address list-name</td>
<td>Prefix from which Route Was Learned:</td>
</tr>
<tr>
<td></td>
<td>IP prefix or prefixes from which the route was learned. list-name is the</td>
</tr>
<tr>
<td></td>
<td>name of an IP prefix list defined with a policy lists prefix-list command.</td>
</tr>
<tr>
<td>metric number</td>
<td>Route Metric:</td>
</tr>
<tr>
<td></td>
<td>Metric in the route.</td>
</tr>
<tr>
<td></td>
<td>number can be a value from 0 through 4294967295.</td>
</tr>
</tbody>
</table>

For Localized Data Policy

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class class-name</td>
<td>Classification:</td>
</tr>
<tr>
<td></td>
<td>Match the specified class name.</td>
</tr>
<tr>
<td>destination-data-prefix-list list-name</td>
<td>Destination Prefix or Port:</td>
</tr>
<tr>
<td></td>
<td>Match a destination prefix or port. For prefixes, you can specify a single</td>
</tr>
<tr>
<td></td>
<td>prefix or a list of prefixes. list-name is the name of a list defined with</td>
</tr>
<tr>
<td></td>
<td>a policy lists prefix-list command. For the port, you can specify a single</td>
</tr>
<tr>
<td></td>
<td>port number, a list of port numbers (with numbers separated by a space), or</td>
</tr>
<tr>
<td></td>
<td>a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>destination-ip prefix/length destination-port number</td>
<td>Packet Length</td>
</tr>
<tr>
<td></td>
<td>Match packets of the specified length. The packet length is a combination</td>
</tr>
<tr>
<td></td>
<td>of the lengths of the IPv4 header and the packet payload.</td>
</tr>
<tr>
<td></td>
<td>number can be 0 though 65535. Specify a single length, a list of lengths</td>
</tr>
<tr>
<td></td>
<td>(with numbers separated by a space), or a range of lengths (with the two</td>
</tr>
<tr>
<td></td>
<td>numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>dscp number</td>
<td>DSCP:</td>
</tr>
<tr>
<td></td>
<td>Match the specified DSCP value.</td>
</tr>
<tr>
<td>packet-length number</td>
<td>Packet Length</td>
</tr>
<tr>
<td></td>
<td>Match packets of the specified length. The packet length is a combination</td>
</tr>
<tr>
<td></td>
<td>of the lengths of the IPv4 header and the packet payload.</td>
</tr>
<tr>
<td></td>
<td>number can be 0 though 65535. Specify a single length, a list of lengths</td>
</tr>
<tr>
<td></td>
<td>(with numbers separated by a space), or a range of lengths (with the two</td>
</tr>
<tr>
<td></td>
<td>numbers separated with a hyphen [-]).</td>
</tr>
</tbody>
</table>
### Packet Loss Priority

**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.

**source-data-prefix-list list-name**

Source Prefix or Port:
Match a source prefix or port. For prefixes, 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. For the 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 [-]).

**source-ip prefix/length**

**source-port number**

**tcp flag**

TCP Flag:
Match TCP flags. flag can be syn.

### For Zone-Based Firewall Policy

**destination-data-prefix-list list-name**

Destination Prefix or Port:
Match a destination prefix or port. For prefixes, 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. For the 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 [-]).

**destination-ip prefix/length**

**destination-port number**

**protocol number**

Protocol:
Match the TCP or IP protocol number.

**source-data-prefix-list list-name**

Source Prefix or Port:
Match a source prefix or port. For prefixes, 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. For the 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>Added omp-tag match condition for localized control policy, and rename tag to omp-tag.</td>
</tr>
<tr>
<td>16.1</td>
<td>Added packet-length match condition for centralization and localized data policy.</td>
</tr>
</tbody>
</table>
### Release | Modification
--- | ---
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.
17.2 | Added dns and dns-app-list match conditions for application-aware routing policy and centralized data policy.
18.2 | Added zone-based firewall policy.

### 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
  !
  !

Create 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
```
Create a route policy match condition that matches the prefix from which a route was learned:

```
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
```

**Operational Commands**

- show running-config policy

**Related Topics**

- `action`, on page 39
- `apply-policy`, on page 81
- `lists`, on page 344
- `match`, on page 377
- `policy`, on page 457
max-clients

Configure the maximum number of clients allowed to connect to the WLAN (on vEdge routers only).

**Command Hierarchy**

```
wlan radio-band
    interface vap number
    max-clients number
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>number</strong></th>
<th>Maximum Number of WLAN Clients:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 50</td>
</tr>
<tr>
<td></td>
<td>Default: 25</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 vSmart 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 vSmarts controllers having higher System-IP.

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

<table>
<thead>
<tr>
<th>number</th>
<th>Maximum Number of Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the maximum number of vSmart controllers that the vEdge router can connect to. These connections are DTLS or TLS control plane tunnels.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 100</td>
</tr>
<tr>
<td></td>
<td>Default: Maximum number of OMP sessions configured with the system max-omp-sessions command.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced. This command replaces the max-controliers command.</td>
</tr>
<tr>
<td>16.1</td>
<td>Maximum number of controllers changed from 8 to 100, and default value changed from 2 to maximum number of configured OMP sessions.</td>
</tr>
</tbody>
</table>

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 185
corrector-group-list, on page 186
exclude-controller-group-list, on page 244
max-omp-sessions, on page 399
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>This command is deprecated. Use the <code>max-control-connections</code> command instead.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th><code>number</code></th>
<th>Number of Leases:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of IP addresses that can be assigned on this interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
vEdge(config)# dhcp-server max-leases 500
vEdge(config)# 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**

<table>
<thead>
<tr>
<th>number</th>
<th>MAC Addresses:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum number of MAC addresses that the bridging domain can learn.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4096</td>
</tr>
<tr>
<td></td>
<td>Default: 1024</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router-lsa administrative</code></td>
<td>Advertise Administratively: Force the maximum metric to take effect immediately, through operator intervention.</td>
</tr>
<tr>
<td><code>router-lsa on-startup seconds</code></td>
<td>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)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 overlay 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

<table>
<thead>
<tr>
<th>number</th>
<th>Maximum Number of OMP Sessions:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 100</td>
</tr>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Change the maximum number of vSmart controller connections to 4:

```bash
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 185
controller-group-list, on page 186
exclude-controller-group-list, on page 244
max-control-connections, on page 392
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>security</code></td>
<td>Encryption of Management Frames</td>
</tr>
<tr>
<td></td>
<td>Whether encryption of management frames is performed on wireless WANs.</td>
</tr>
<tr>
<td></td>
<td>Values: none, optional, required</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Configure management frame encryption for VAP 3:

```bash
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 197
mirror

Configure or apply a mirror to copy data packets to a specified destination for analysis (on vEdge routers only).

You can mirror only unicast traffic. You cannot mirror multicast traffic.

vManage Feature Template

For vEdge routers:
Configuration ► Policies ► Localized Policy

Command Hierarchy

Create a Localized Control Policy

policy
  mirror mirror-name
  remote-dest ip-address source ip-address

Apply a Localized Control Policy

policy
  access-list acl-name
  default-action action
  sequence number
  action accept
  mirror mirror-name

Syntax Description

<table>
<thead>
<tr>
<th>mirror-name</th>
<th>Mirror Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the mirror to configure or to apply in an access list.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Remote Destination:</td>
</tr>
<tr>
<td></td>
<td>Destination to which to mirror the packets.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Source:</td>
</tr>
<tr>
<td></td>
<td>Source of the packets to mirror.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure and apply a mirror:

vEdge# show running-config policy
policy
mirror m1
remote-dest 10.2.2.11 source 10.20.23.16
!
access-list acl2
  sequence 1
  match
    source-ip 10.20.24.17/32
    destination-ip 10.20.25.18/32
!
action accept
  mirror m1
!
!
default-action drop
!
!
Operational Commands

show running-config
mode

Configure the mode to use in IKEv1 Diffie-Hellman key exchanges (on vEdge routers only).

**Command Hierarchy**

```
vpn vpn-id
    interface ipsec number
    ike
        mode mode
```

**Syntax Description**

<table>
<thead>
<tr>
<th>mode</th>
<th>Exchange Mode:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mode to use for IKEv1 Diffie-Hellman key exchanges. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 259
Set the maximum MTU size of packets on the interface.

**vManage Feature Template**

For all Viptela 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**

<table>
<thead>
<tr>
<th>bytes</th>
<th>MTU Size:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 576 through 2000 bytes</td>
</tr>
<tr>
<td></td>
<td>Default: 1500</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Maximum MTU changed from 1804 bytes to 2000 bytes.</td>
</tr>
</tbody>
</table>

**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 126
- pmtu, on page 452
- tcp-mss-adjust, on page 560
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>percentage</td>
<td>Interface Bandwidth:</td>
</tr>
<tr>
<td></td>
<td>Set the percentage of interface bandwidth that multicast traffic can use.</td>
</tr>
<tr>
<td></td>
<td>Range: 5 through 100 percent</td>
</tr>
<tr>
<td></td>
<td>Default: 20 percent</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>vpn</th>
<th>vpn-id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>router</td>
</tr>
<tr>
<td></td>
<td>multicast-replicator local [threshold number]</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>string</th>
<th>VPN Name:</th>
</tr>
</thead>
</table>
| Text name or description of the VPN. If it includes spaces, enclose the entire string in quotation marks (" ").
| Maximum characters: 32 |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure a description for VPN 1:

```
vpn 1
  name "Customer A VPN"
```

Operational Commands

```
show running-config vpn
```
**name**

Provine a text name for the Viptela device.

**vManage Feature Template**

For all Viptela devices:

Configuration ► Templates ► SNMP

**Command Hierarchy**

```
snmp
  name string
```

**Syntax Description**

<table>
<thead>
<tr>
<th>string</th>
<th>Device Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the Cisco vEdge device. If it contains spaces, enclose the string in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 255</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Configure the SNMP name of this Viptela 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 37
- auth-req-attr, on page 102
- nas-ip-address, on page 415
- radius, on page 488
- radius-servers, on page 492
**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**

<table>
<thead>
<tr>
<th><strong>ip-address</strong></th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NAS IP address to send to the RADIUS server.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Operational Commands**

- clear dot1x client
- show dot1x clients
- show dot1x interfaces
- show dot1x radius
- show system statistics
Related Topics

acct-req-attr, on page 37
auth-req-attr, on page 102
nas-identifier, on page 413
radius, on page 488
radius-servers, on page 492
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>Multiple NAT interfaces can be configured.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for 1:1 static NAT and dynamic NAT.</td>
</tr>
</tbody>
</table>

Operational Commands

- show ip nat filter
- show ip nat interface
- show ip nat interface-statistics

Related Topics

- encapsulation, on page 239
- action, on page 53
- ip gre-route, on page 317
- ip route, on page 321
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 Viptela 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

<table>
<thead>
<tr>
<th>range-start ip-address1</th>
<th>range-end ip-address2</th>
<th>NAT Pool Address Range:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Define the range of IP addresses to use for the NAT address pool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ip-address1</em> must be less than or equal to <em>ip-address2</em>. The pool can contain a maximum of 32 IP addresses. The addresses must be in the same subnet as the interface's IP address.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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-multipath 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**

<table>
<thead>
<tr>
<th><code>ip-address</code></th>
<th>Neighbor Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address of the BGP neighbor.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

\[ \text{vpn} \ \text{vpn-id} \]
\[ \text{router} \]
\[ \text{ospf} \]
\[ \text{area} \ number \]
\[ \text{interface} \ \text{interface-name} \]
\[ \text{network} \ (\text{broadcast} \mid \text{point-to-point}) \]

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure an interface as a point-to-point interface:

\[
\text{vml} \# \text{show running-config vpn 1 router ospf area 0}
\]
\[
\text{vpn 1}
\text{router}
\text{ospf}
\text{area 0}
\text{interface ge0/1}
\text{point-to-point}
\text{exit}
\text{exit}
! ! !
\]

Configuration Commands

424
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:

```
vml# 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>me</th>
<th>Interface Node Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Node type for Cloud OnRamp for SaaS on this interface.</td>
</tr>
<tr>
<td></td>
<td>Values: client, gateway</td>
</tr>
<tr>
<td></td>
<td>Default: client</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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. |

<table>
<thead>
<tr>
<th>no-summary</th>
<th>Summary Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do not inject OSPF summary routes into the NSSA.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure area 1 to be an NSSA:

```
vml# show running-config vpn 1 router ospf
vpn 1
router
ospf
  redistribute static
  redistribute ospf
  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 Viptela device allows that device to contact NTP servers to synchronize time. Other devices are allowed to ask a Viptela device for the time, but no devices are allowed to use the Viptela device as an NTP server.

**vManage Feature Template**

For all Viptela devices:

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**

<table>
<thead>
<tr>
<th>source-interface</th>
<th>Interface for NTP To Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>server</th>
<th>Location of NTP Server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(dns-server-address</td>
<td>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.</td>
</tr>
<tr>
<td>ipv4-address)</td>
<td></td>
</tr>
</tbody>
</table>
### MD5Authentication

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.

To designate an MD5 authentication key as trustworthy, specify the key in the `trusted` command.

To associate an MD5 authentication key with a server, specify the key in the `key` command. For the key to work, you must mark it as trusted.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>Added support for up to four NTP servers, MD5 authentication, and configuring the source interface.</td>
</tr>
</tbody>
</table>

### 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 $4$KXLzYTk6M8zj4BglEFXKw==
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
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 72
**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 ge slot/port
        dhcp-server
            offer-time seconds
```

**Syntax Description**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Duration of IP Address Offer:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 600 seconds</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>shutdown</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added vpn omp command.</td>
</tr>
</tbody>
</table>
**Operational Commands**

- show omp peers
- show omp routes
- show omp services
- show omp summary
- show omp tlocs
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-gateway ip-address</td>
<td>Default Gateway: IP address of a default gateway in the service-side network.</td>
</tr>
<tr>
<td>dns-servers ip-address</td>
<td>DNS Servers: One or more of IP addresses for a DNS server in the service-side network. You can specify up to eight addresses.</td>
</tr>
<tr>
<td>domain-name domain-name</td>
<td>Domain Name: Domain name that the DHCP client uses to resolve hostnames.</td>
</tr>
<tr>
<td>interface-mtu mtu</td>
<td>Interface MTU: MTU size on the interface to the DHCP client. Range: 68 to 65535 bytes</td>
</tr>
<tr>
<td>tftp-servers ip-address</td>
<td>TFTP Servers: IP address of a TFTP server in the service-side network. You can specify one or two addresses.</td>
</tr>
<tr>
<td>option-code 43 ascii</td>
<td>Vendor specific information.</td>
</tr>
<tr>
<td>option-code 191 ascii</td>
<td>Vendor specific information.</td>
</tr>
</tbody>
</table>
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Configure options to send when requested by a DHCP client:

```plaintext
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**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
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**

```plaintext
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
        ! end area
        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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 ospf
    area 0
      interface ge0/0
    exit
  exit

vEdge# show interface vpn 1

Monitoring Commands

show ospf database
show ospf database-summary
show ospf interface
show ospf neighbor
show ospf process
show ospf routes
**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**

<table>
<thead>
<tr>
<th><code>as-number</code></th>
<th>AS Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Operational Commands**

- `show bgp routes`
- `show omp routes`

**Related Topics**

- `propagate-aspath`, on page 483
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**

```plaintext
vpn vpn-id
  interface natpoolnumber
    nat
    [no] overload
```

**Syntax Description**

None

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

**Dynamic NAT**

Configure a vEdge router to perform dynamic NAT:

```plaintext
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 239
  static, on page 544
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 digest (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

<table>
<thead>
<tr>
<th>md5-digest-string</th>
<th>Password:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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+gFX1RXXw==
```
Operational Commands

show bgp neighbor
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

<table>
<thead>
<tr>
<th>pfs-setting</th>
<th>PFS Setting for IPsec Tunnel:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type of PFS to use on an IPsec tunnel that is being used for IKE key exchange. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• group-2—Use the 1024-bit Diffie-Hellman prime modulus group.</td>
</tr>
<tr>
<td></td>
<td>• group-14—Use the 2048-bit Diffie-Hellman prime modulus group.</td>
</tr>
<tr>
<td></td>
<td>• group-15—Use the 3072-bit Diffie-Hellman prime modulus group.</td>
</tr>
<tr>
<td></td>
<td>• group-16—Use the 4096-bit Diffie-Hellman prime modulus group.</td>
</tr>
<tr>
<td></td>
<td>• none—Disable PFS.</td>
</tr>
</tbody>
</table>

Default: group-16

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
**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 Viptela 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 126
- `clear-dont-fragment`, on page 153
- `mtu`, on page 406
policer

**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**

```plaintext
policy
policer policer-name
  burst bytes
  exceed action
  rate bps
```

**Apply a Policer in Centralized Data Policy**

On vSmart controllers only.

```plaintext
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.

```plaintext
policy
  access-list list-name
    sequence number
    action accept
    policer policer-name
```

**Apply a Policer Directly to an Interface**

On vEdge routers only.

```plaintext
vpn vpn-id
  interface interface-name
    policer policer-name (in | out)
```
### Syntax Description

**policer-name**

<table>
<thead>
<tr>
<th>Policer Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 <code>policy policer</code> configuration command.</td>
</tr>
</tbody>
</table>

**burst** *bytes*

**exceed** *action*

**rate** *bps*

<table>
<thead>
<tr>
<th>Policer Parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the policing parameters:</td>
</tr>
<tr>
<td>• <strong>burst</strong> is the maximum traffic burst size.</td>
</tr>
<tr>
<td>• <strong>exceed</strong> is the action to take when the burst size or traffic rate is exceeded.</td>
</tr>
<tr>
<td>• <strong>rate</strong> is the maximum traffic rate, in bits per second.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>burst <strong>bytes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bytes</code> can be a value from 15000 to 10000000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>exceed <strong>action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>action</code> 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>rate <strong>bps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bps</code> can be value from 0 through 264 – 1.</td>
</tr>
</tbody>
</table>

**policy access-list**

<table>
<thead>
<tr>
<th>Apply a Policer Conditionally to an Interface, via an Access List:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**vpn interface access-list**

<table>
<thead>
<tr>
<th>Apply a Policer Unconditionally to an Interface:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for multicast traffic.</td>
</tr>
</tbody>
</table>
Examples

Example 1
Create a policer, and apply it conditionally to outbound traffic on an interface in VPN 1:

```plaintext
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:

```plaintext
policy
policer p1
rate 1000000
burst 15000
exceed drop
!
vpn 1
interface ge0/4
ip address 10.20.24.15/24
no shutdown
!
!
```

Operational Commands

clear policer statistics
show interface detail
show policer
show running-config

**Related Topics**
- control-session-pps, on page 184
- host-policer-pps, on page 277
- icmp-error-pps, on page 278
- match, on page 380
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
  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
    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
For Centralized Data Policy

Configure on vSmart controllers only.

```plaintext
color-list list-name
color color
prefix-list list-name
ip-prefix 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
sequence number
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
```

Configuration Commands
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

classification
  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
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
content 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

policing
  policy
  data-policy policy-name
  default-action action
  sequence number
  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
  sequence number
  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 [as:nn | internet | local-as | no-advertise | no-export]
    ext-community-list list-name
    community [rt (as:nn | ip-address) | soo (as:nn | ip-address)]
    prefix-list list-name
    ip-prefix prefix/length

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
    ospf-tag number
    origin (egp | igp | incomplete)
    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)
orignator 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
  mirror mirror-name
  remote-dest ip-address source ip-address
  policer policer-name
  burst types
  exceed action
  rate bps
qos-map map-name
  qos-scheduler scheduler-name
qos-scheduler scheduler-name
  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
  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
    count counter-name
    drop
    log
  accept
    class class-name
    mirror mirror-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
  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

Syntax Description
None

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Added application-aware routing policy.</td>
</tr>
<tr>
<td>18.2</td>
<td>Added zone-based firewall policy.</td>
</tr>
</tbody>
</table>

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 33
  apply-policy, on page 81
  policy ipv6, on page 464
redistribute, on page 499
policy ipv6

policy ipv6—Configure IPv6 policy (on vEdge routers only).

Command Hierarchy

Localized Data Policy for IPv6
Confgure on vEdge routers only.

policy
  mirror mirror-name
  remote-dest ip-address source ip-address
  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
    mirror mirror-name
    policer policer-name
    set
    traffic-class value

Syntax Description
None

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
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 457
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-start port-number1</td>
<td>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</td>
</tr>
<tr>
<td>port-end port-number2</td>
<td></td>
</tr>
<tr>
<td>private-ip-address</td>
<td>Private Server: IP address of the internal device to which to direct traffic that matches the port-forwarding rule.</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
</tr>
<tr>
<td>private-vpn vpn-id</td>
<td>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</td>
</tr>
<tr>
<td>(tcp</td>
<td>udp)</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no port-hop</code></td>
<td>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 <code>no port-hop</code> at the <code>system</code> 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.</td>
</tr>
</tbody>
</table>

**Examples**

Enable port hopping:
system
  port-hop

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.1</td>
<td>Port hopping enabled by default.</td>
</tr>
<tr>
<td>15.3.8</td>
<td>Added support for BFD port hopping.</td>
</tr>
<tr>
<td>16.2</td>
<td>Port hopping is disabled by default on vManage NMSs and vSmart controllers.</td>
</tr>
</tbody>
</table>

Operation Commands

request port-hop

show control local-properties

Related Topics

  graceful-restart, on page 255
  port-offset, on page 470
  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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Configure a port offset value:

```bash
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
system-ipv6/unique-id 2e06d6d1-4d1a-b7f4-014650e0d0e0
derial-num NOT-A-HARDWARE
keypair-interval 1:00:00:00
retry-interval 0:0:0:0:14
no-activity-exp-interval 0:0:0:0:12
dns-cache-ttl 0:0:0:0:10
port-hopped TRUE
time-since-last-port-hop 0:0:0:0:38
number-vbond-peers 1

INDEX IP PORT
-------------------------------
0 10.1.14.14 12346

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
```
show control local-properties

show orchestrator local-properties

port-hop, on page 468

request port-hop
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac-name name</td>
<td>Access Concentrator Name: Name of the access concentrator used by PPPoE to route connections to the internet.</td>
</tr>
<tr>
<td>chap hostname</td>
<td>Authentication Credentials for CHAP: Hostname and password provided by your Internet Service Provider (ISP). <code>hostname</code> 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.</td>
</tr>
<tr>
<td>password</td>
<td></td>
</tr>
<tr>
<td>pap sent-username</td>
<td>Authentication Credentials for PAP: Username and password provided by your Internet Service Provider (ISP). <code>sent-username</code> 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.</td>
</tr>
<tr>
<td>password</td>
<td></td>
</tr>
</tbody>
</table>

**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 $490HJidmsC7M8z5BgLEFXKw==
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.1</td>
<td>Added ability to configure both CHAP and PAP authentication on a PPP interface.</td>
</tr>
</tbody>
</table>

Operational Commands

clear pppoe statistics
show pppoe session
show pppoe statistics
show ppp interface

Related Topics

pppoe-client, on page 474
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

<table>
<thead>
<tr>
<th>pppnumber</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the PPP interface.</td>
</tr>
<tr>
<td></td>
<td>Possible values: from ppp1 through ppp31</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
dshow interface detail
dshow ppp interface
dshow pppoe session
dshow pppoe statistics
Related Topics

ppp, on page 472
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**

<table>
<thead>
<tr>
<th>number</th>
<th>Designated Router Priority:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 255</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
    exit
  !
!```
Operational Commands

show ospf interface

Related Topics

router-id, on page 522
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>apn name</strong></td>
<td>Access Point Name: Name of the gateway between the service provider network and the public Internet. It can be up to 32 characters long.</td>
</tr>
<tr>
<td><strong>auth auth-method</strong></td>
<td>Authentication Method: Authentication method used for the connection to the cellular network. Possible values are CHAP, None, PAP, or PAP/CHAP.</td>
</tr>
<tr>
<td><strong>primary-dns ip-address</strong></td>
<td>DNS Servers: IP addresses of the primary and secondary DNS servers in the service provider network, in decimal four-part dotted notation.</td>
</tr>
<tr>
<td><strong>secondary-dns ip-address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>name profile-name</strong></td>
<td>Name: Name used to identify the cellular profile. It can be up to 14 characters long.</td>
</tr>
</tbody>
</table>
| **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for profile 0; changed profile 16 to reserved, so you cannot modify it.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
vEdge# show running-config cellular
  cellular cellular0
    profile 1
      apn req 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 cellular0
    profile profile-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>profile</strong></td>
<td>Profile:</td>
</tr>
<tr>
<td><strong>profile-id</strong></td>
<td>Number that identifies the profile to use for the cellular interface. This profile is one you configure with the <code>cellular profile</code> command.</td>
</tr>
</tbody>
</table>

`profile-id` can be a value from 1 through 15.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

```
vEdge# show running-config vpn 0 interface cellular0
vpn 0
  interface cellular0
    ip dhcp-client
tunnel-interface
color lte
  encapsulation ipsec
  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
  mtu 1428
!```
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 478
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-as-path
```

**Syntax Description**
None

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Carry local BGP AS path information into OMP, and receive AS path information from OMP:

```
vpn 1
 router
  bgp 1
    propagate-as-path
```

**Operational Commands**

- show bgp summary
- show omp routes detail

**Related Topics**

- overlay-as, on page 443
qos-map

**qos-map**—Configure a QoS map, or apply a QoS map on an interface (on vEdge routers only). QoS is applied to unicast or multicast packets being transmitted out the interface.

**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 Ethernet

**Command Hierarchy**

**Create a QoS Map**

```
policy
  qos-map map-name
  qos-scheduler class-name
```

**Apply a QoS Map on an Interface**

```
vpn vpn-id
  interface interface-name
  qos-map map-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>map-name</strong></th>
<th>QoS Map Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the QoS map. It can be a text string from 1 through 32 characters long. When you are configuring a QoS map, it can contain 64 QoS schedulers. The interface cannot be a VLAN interface (subinterface). When you apply a QoS map to an interface, the map name must match that which you specified when you created the QoS with the <code>policy qos-map</code> configuration command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>qos-scheduler class-name</strong></th>
<th>QoS Scheduler:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of a QoS scheduler configured with a <code>policy qos-scheduler</code> configuration command.</td>
</tr>
</tbody>
</table>

**Examples**

Create a QoS scheduler and QoS map, and apply it to an interface in VPN 1:

```
vEdge(config)# show config
policy
qos-scheduler af1
  class af1
  bandwidth-percent 20
```
buffer-percent 20
drops red-drop

! qos-map test-qos-map
  qos-scheduler af1
  
  !
  vpn 1
  interface ge0/0
    qos-map test-qos-map


Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for multicast traffic.</td>
</tr>
<tr>
<td>17.1</td>
<td>Can no longer configure qos-map on a VLAN interface.</td>
</tr>
</tbody>
</table>

Operational Commands

show policy qos-map-info

show policy qos-scheduler-info

Related Topics

class-map, on page 151
qos-map, on page 484
qos-scheduler, on page 486
rewrite-rule, on page 515
**qos-scheduler**

**policy qos-scheduler**—Configure a QoS scheduler for a forwarding class (on vEdge routers only).

A scheduler can apply to unicast and multicast traffic.

**vManage Feature Template**

For vEdge routers:

Configuration ► Policies ► Localized Policy

**Command Hierarchy**

```
policy
  qos-scheduler scheduler-name
    bandwidth-percent percentage
    buffer-percent percentage
    class class-name
    drops (red-drop | tail-drop)
    scheduling (llq | wrr)
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler-name</td>
<td>Scheduler Name: Name of the QoS scheduler for a forwarding class. It can be a text string from 1 through 32 characters long.</td>
</tr>
<tr>
<td>bandwidth-percent</td>
<td>Bandwidth Percentage: Percentage of the interface's bandwidth to allocate to the forwarding class. The sum of the bandwidth on all forwarding classes on an interface should not exceed 100 percent.</td>
</tr>
<tr>
<td>buffer-percent</td>
<td>Buffer Percentage: Percentage of the interface's buffering capacity to allocate to the forwarding class. The sum of the buffering capacity of all forwarding classes on an interface should not exceed 100 percent.</td>
</tr>
<tr>
<td>class class-name</td>
<td>Class: Name of the forwarding class. <em>class-name</em> can be a text string from 1 through 32 characters long. The common class names correspond to the per-hop behaviors AF (assured forwarding), BE (best effort), and EF (expedited forwarding).</td>
</tr>
<tr>
<td>drops (red-drop</td>
<td>tail-drop)</td>
</tr>
</tbody>
</table>
**scheduling (llq | wrr)**

Queue Scheduling:
Algorithm to use to schedule interface queues. It can be either low-latency queuing (llq) or weighted round-robin (wrr). If you use LLQ, you cannot configure RED packet drops.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2.3</td>
<td>Beginning with this release, if you attempt to configure LLQ and red drops, an error message is displayed when you try to validate the configuration, and the commit operation does not continue.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for multicast traffic.</td>
</tr>
</tbody>
</table>

**Examples**

Create a QoS scheduler and QoS map, and apply it to an interface in VPN 1:

```bash
vEdge(config)# show config policy
policy
  qos-scheduler af1
    class af1
    bandwidth-percent 20
    buffer-percent 20
    drops red-drop
  qos-map test-qos-map
    qos-scheduler af1

vEdge(config)# show config vpn 1
vpn 1
  interface ge0/0
    qos-map test-qos-map
```

**Operational Commands**

- `show policy qos-map-info`
- `show policy qos-scheduler-info`

**Related Topics**

- `access-list`, on page 33
- `class-map`, on page 151
- `cloud-qos`, on page 155
- `qos-map`, on page 484
- `rewrite-rule`, on page 515
**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 Viptela 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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 Viptela 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. |
<table>
<thead>
<tr>
<th>Configuration Commands</th>
</tr>
</thead>
</table>

### 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 Viptela 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.3</td>
<td>Added <code>source-interface</code> command.</td>
</tr>
<tr>
<td>15.3.8</td>
<td>Added <code>secret-key</code> command and deprecated <code>key</code> command.</td>
</tr>
<tr>
<td>16.1</td>
<td>Changed authentication key from 32 to 128 characters.</td>
</tr>
<tr>
<td>16.2.2</td>
<td>Added <code>priority</code> command.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added <code>acct-port</code> and <code>tag</code> commands, and added support for IEEE 802.1X LAN and IEEE 802.11i WLAN authentication.</td>
</tr>
</tbody>
</table>

Examples

Configure two RADIUS servers:

```bash
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 29
admin-auth-order, on page 60
auth-fallback, on page 94
auth-order, on page 97
dot1x, on page 225
tacacs, on page 557
wlan, on page 646
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
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$6fmVCA6JHrEg/AKSy3jIXKyhtvXJNNTlv3My2l19/6hS6ICNMV13Ydxl9gQOGVJGW391dlaqjPPDZUkuxyIyI3/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+IEZB2vcQpeEoSR4ia9JqgD5NcP0hukAb8fvxAg5I-
        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 488
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.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>Cost for the Summary Routes:</td>
</tr>
<tr>
<td>number</td>
<td>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</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Do Not Advertise Type 3 Summary LSAs:</td>
</tr>
<tr>
<td></td>
<td>Do not advertise the Type 3 Summary LSAs.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>minutes</th>
<th>Time between Reauthentication Attempts:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the time between reauthentication attempts.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 1440 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: 0 (no reauthentication attempts are made after the initial LAN access request)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Require a client to reauthenticate once an hour:

```
vpn 0
  interface ge0/8
    dot1x
      reauthentication 3600
```

**Operational Commands**

- clear dot1x client
- show dot1x clients
- show dot1x interfaces
- show dot1x radius
- show system statistics
Related Topics

radius, on page 488
redistribute

**vpn router ospf redistribute**—Redistributes routes learned from other protocols into OSPF (on vEdge routers only). By default, no routes from other protocols are redistributed into OSPF.

**vManage Feature Template**

For vEdge routers only:

Configuration ► Templates ► OSPF

**Command Hierarchy**

```
vpn vpn-id
   router
      ospf
         redistribute (bgp | connected | nat | natpool-outside | omp | static) route-policy policy-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`bgp</td>
<td>connected</td>
</tr>
<tr>
<td>`(bgp</td>
<td>connected</td>
</tr>
<tr>
<td><code>route-policy policy-name</code></td>
<td>Route Policy to apply to redistributed routes:</td>
</tr>
<tr>
<td></td>
<td>Name of policy to apply to routes before they are redistributed into OSPF.</td>
</tr>
</tbody>
</table>

**Release Information**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Added nat option.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added natpool-outside option.</td>
</tr>
</tbody>
</table>

**Examples**

Redistribute OMP and static routes into OSPF:

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

Operational Commands

show ospf routes

Related Topics

route-policy, on page 518
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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bi-directional</strong></td>
<td>Refresh NAT Mappings for Inbound and Outbound Packets: On the interface, keep the NAT mappings for both outbound and inbound traffic active.</td>
</tr>
<tr>
<td><strong>outbound</strong></td>
<td>Refresh NAT Mappings for Outbound Packets Only: On the interface, keep the NAT mappings for outbound traffic active. This is the default behavior.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
vm5(config-nat-nat)#
  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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Rekeying Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 1209600 seconds (14 days)</td>
</tr>
<tr>
<td></td>
<td>Default: 86400 seconds (24 hours)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3.5</td>
<td>Rekeying time default changed from 7200 seconds (2 hours) and maximum time increased from 2 days to 7 days.</td>
</tr>
</tbody>
</table>

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 255
request security ipsec-rekey
show bfd sessions
timers, on page 580
**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**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Rekeying Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How often IKE changes the AES key that is being used during IKE key exchanges.</td>
</tr>
<tr>
<td></td>
<td>Range: 30 through 1209600 seconds (up to 14 days)</td>
</tr>
<tr>
<td></td>
<td>Default: 3600 seconds (1 hour) (for ipsec rekey); 14400 seconds (4 hours) (for ike rekey)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>remote-as</th>
<th>as-number</th>
<th>Remote AS Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AS number of the remote BGP peer.</td>
</tr>
</tbody>
</table>

Release Information

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 ipsec
        ipsec
        replay-window number

Syntax Description

<table>
<thead>
<tr>
<th>number</th>
<th>Replay Window Size:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Size of the sliding replay window.</td>
</tr>
<tr>
<td></td>
<td>Values: 64, 128, 256, 512, 1024, 2048, 4096 packets</td>
</tr>
<tr>
<td></td>
<td>Default: 512 packets</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

clear ipsec ike sessions
show ipsec ike inbound-connections
show ipsec ike outbound-connections
show ipsec ike sessions

Related Topics

ike, on page 283
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

<table>
<thead>
<tr>
<th>number</th>
<th>Replay Window Size:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Size of the sliding replay window.</td>
</tr>
<tr>
<td></td>
<td>Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets</td>
</tr>
<tr>
<td></td>
<td>Default: 512 packets</td>
</tr>
</tbody>
</table>

Release Information

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 replicator at random. |
|          | • sticky—Always use the same replicator. This is the default. |

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Retransmit Interval:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time interval at which the OSPF retransmits LSAs to its neighbors.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5 seconds</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>layer-2-cos</code>&lt;br&gt;<code>number</code></td>
<td>Class-of-Service Value:&lt;br&gt;Number of an 802.1p CoS value to use to mark transit traffic.&lt;br&gt;Range: 0 through 7</td>
</tr>
<tr>
<td><code>dscp dscp-value</code></td>
<td>DSCP Value:&lt;br&gt;Assign a DSCP value to transit traffic.&lt;br&gt;Range: 0 through 63</td>
</tr>
<tr>
<td><code>class class-name</code></td>
<td>Forwarding Class Name:&lt;br&gt;Name of the forwarding class.</td>
</tr>
</tbody>
</table>
**LossPriority:**
Packet loss priority (PLP) for the forwarding class.
Values: high, low

<table>
<thead>
<tr>
<th><strong>rule-name</strong></th>
<th>Rewrite Rule Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note**
Cisco IOS XE SD-WAN supports maximum of 64 entries only per rewrite rule.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.3</td>
<td>Added support for multicast traffic.</td>
</tr>
<tr>
<td>18.3</td>
<td>Added support for Layer 2 class of service (CoS).</td>
</tr>
</tbody>
</table>

### Examples

Create a rewrite rule, and apply it to an interface:

```
veEdge(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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 321
ipv6 route, on page 332
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

<table>
<thead>
<tr>
<th>policy-name</th>
<th>Control Policy Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the localized control policy to configure or apply to a BGP neighbor or to OSPF.</td>
</tr>
<tr>
<td></td>
<td>policy-name can be up to 32 characters long.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>in, out</th>
<th>Direction To Apply Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>Added support for configuring route policy on all OSPF inbound routes (route-policy in).</td>
</tr>
</tbody>
</table>

Operational Commands

show ip routes detail
show running-config

Related Topics

policy, on page 457
redistribute, on page 499
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>PIM and multicast added.</td>
</tr>
<tr>
<td>14.3</td>
<td>IGMP added.</td>
</tr>
</tbody>
</table>

**Examples**

**Enable OSPF in VPN 1**

```
vm5# 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
    !
    !
```

**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 ompl multicast-auto-discover
show ompl 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**

| `ipv4-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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 476
- `system-ip`, on page 554
**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**

<table>
<thead>
<tr>
<th>router-id ip-address</th>
<th>BGP Router ID:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 554
security

Configure security parameters (on vEdge routers, vManage NMSs, and vSmart controllers only).

vManage Feature Template

For vEdge routers, vManage NMSs, and vSmart controllers only:
Configuration ▶ Templates ▶ Security

Command Hierarchy

```
security
  control
    protocol (dtls | tls)
    tls-port number
  ipsec (on vEdge routers only)
    authentication-type type
    rekey-seconds
    replay-window number
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.3</td>
<td>control command added.</td>
</tr>
</tbody>
</table>

Operational Commands

- `show tunnel local-sa`
- `show control summary`
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure the local vEdge router to send the BGP extended community attribute to its BGP neighbor

```
vml# 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
```

<table>
<thead>
<tr>
<th>Number of Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of equal-cost routes that a vEdge router advertises to a vSmart controller or that a vSmart controller redistributes to vEdge routers. More exactly, a route is a route–TLOC tuple. (Each TLOC consists of a IP address and color.) Each vEdge router can have up to four WAN interfaces and hence can advertise up four route–TLOC tuples for each route.</td>
</tr>
</tbody>
</table>

**Range:** 1 through 16  
**Default:** 4  

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2</td>
<td>Maximum number of routes increased to 16.</td>
</tr>
</tbody>
</table>

**Operational Commands**

```
show omp routes
```
service

Configure a service, such as a firewall or IDS, that is present on the local network in which the vEdge router is located (on vEdge routers only). 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

For vEdge routers only:
Configuration ► Templates ► VPN

Command Hierarchy

```
vpn vpn-id
  service service-name address ip-address
vpn vpn-id
  service service-name interface gre number1 [gre number2]
```

Syntax Description

<table>
<thead>
<tr>
<th>service-name</th>
<th>Type of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type of service available at the local site and in the VPN. Standard services are firewall, IDS, and IDP. Four custom services are available.</td>
</tr>
<tr>
<td></td>
<td>Values: FW, IDP, IDS, netsvc1, netsvc2, netsvc3, netsvc4, TE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>address ip-address</th>
<th>Location of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface gre number1 [gre number2]</td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Configured IP address of the service resolved locally.</td>
</tr>
<tr>
<td>15.4.1</td>
<td>Support for GRE interfaces added.</td>
</tr>
<tr>
<td>17.2.0</td>
<td>Support for traffic engineering (TE) service added.</td>
</tr>
</tbody>
</table>
Examples

Configure a firewall service that is available in VPN 1

```
vpn 1
  service FW address 10.0.2.11
```

Related Commands

- show omp services
- show tunnel gre-keepalives

Related Topics

- allow-service, on page 72
- tunnel-destination, on page 601
- tunnel-source, on page 608
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).

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

<table>
<thead>
<tr>
<th>kbps</th>
<th>Traffic Shaping Rate:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rate at which to transmit traffic, in kilobits per second (kbps).</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 0 through the maximum interface speed</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.1</td>
<td>Starting with this release, you can no longer configure <code>shaping-rate</code> on a VLAN interface</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
  !
  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

<table>
<thead>
<tr>
<th>IF</th>
<th>VPN INTERFACE</th>
<th>IP ADDRESS</th>
<th>SPEED</th>
<th>RX</th>
<th>TX</th>
<th>STATUS</th>
<th>STATUS</th>
<th>TYPE</th>
<th>PORT TYPE</th>
<th>MTU</th>
<th>HWADDR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ge0/0</td>
<td>10.1.16.16/24</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>transport</td>
<td>1500</td>
<td>00:0c:29:d7:63:18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge0/1</td>
<td>10.1.18.16/24</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>service</td>
<td>1500</td>
<td>00:0c:29:d7:63:22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge0/2</td>
<td>-</td>
<td>-</td>
<td>Down</td>
<td>Down</td>
<td>null</td>
<td>1500</td>
<td>00:0c:29:d7:63:2c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge0/3</td>
<td>10.0.21.16/24</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>service</td>
<td>1500</td>
<td>00:0c:29:d7:63:36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ge0/7</td>
<td>10.0.100.16/24</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>service</td>
<td>1500</td>
<td>00:0c:29:d7:63:5e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>system</td>
<td>172.16.255.16/32</td>
<td>Up</td>
<td>Up</td>
<td>null</td>
<td>loopback</td>
<td>1500</td>
<td>00:00:00:00:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>site-id</th>
<th>Site Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Range:** 1 through 4294967295 ($2^{32} - 1$)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

Create groupings of properties that identify an application for a policy to use with application-aware routing (on vSmart controllers only). You can configure a maximum of four SLA classes.

vManage Feature Template

For vSmart controllers:

Configuration ► Policies ► Centralized Policy

Command Hierarchy

```
policy
  sla-class sla-class-name
    jitter milliseconds
    latency milliseconds
    loss percentage
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>jitter milliseconds</strong></td>
<td>Packet jitter: Jitter on the connection. Packets matching the policy for application-aware routing are directed out connections that have the specified jitter or a lower jitter value. &lt;br&gt;&lt;br&gt; <em>Range:</em> 1 through 1000 milliseconds</td>
</tr>
<tr>
<td><strong>latency milliseconds</strong></td>
<td>Packet latency: Latency on the connection. Packets matching the policy for application-aware routing are directed out connections that have the specified latency or a lower latency value. &lt;br&gt;&lt;br&gt; <em>Range:</em> 0 through 1000 milliseconds</td>
</tr>
<tr>
<td><strong>loss percentage</strong></td>
<td>Packet loss: Packet loss on the connection. Packets matching the policy for application-aware routing are directed out connections that have the specified packet loss or a lower packet loss value. &lt;br&gt;&lt;br&gt; <em>Range:</em> 0 through 100 percent</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2</td>
<td>jitter option added.</td>
</tr>
</tbody>
</table>
Examples

Configure an SLA for a latency of 50 milliseconds

```plaintext
policy
  sla-class 50ms-sla
  latency 50
```

Operational Commands

```plaintext
show running-config policy sla-class
```
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2</td>
<td>Support for SNMP traps added.</td>
</tr>
<tr>
<td>16.2</td>
<td>Support for SNMPv3 traps added.</td>
</tr>
</tbody>
</table>

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**

**NEED** 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>speed</th>
<th>Interface Speed:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface speed, in Mbps.</td>
</tr>
<tr>
<td></td>
<td>Values: 10, 100</td>
</tr>
<tr>
<td></td>
<td>Default: Autonegotiate (10/100/1000 Mbps) on vEdge 1000 routers</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Support for autonegotiation added</td>
</tr>
</tbody>
</table>

**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 114
- **duplex**, on page 230
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**

<table>
<thead>
<tr>
<th>kbps</th>
<th>Traffic Rate:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 100 kbps</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
- 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 interface 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

**Configure four SSIDs**

```bash
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 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 3: 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 4: 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. 

*Configuration Commands*

*static*
translate-port number

Translated Port Number:
Number to translate the port number to.

Range: 1 through 65535

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>18.3</td>
<td>Support for static NAT address mappings in VPN 0 added.</td>
</tr>
</tbody>
</table>

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 239
  - direction, on page 216
  - natpool, on page 421
  - overload, on page 444
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**

<table>
<thead>
<tr>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Number:</td>
</tr>
<tr>
<td>Queue number to use for incoming traffic.</td>
</tr>
<tr>
<td>Range: 0 through 7</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>host-name hostname</code></td>
<td>Hostname of Client:</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>Network Client:</td>
</tr>
<tr>
<td><code>ip ip-address</code></td>
<td>Static IP Address:</td>
</tr>
<tr>
<td><code>host-name hostname</code></td>
<td>Hostname of client device.</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>MAC address of client to which static IP address is being assigned.</td>
</tr>
<tr>
<td><code>ip ip-address</code></td>
<td>Static IP address to assign to the client.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>no-summary</th>
<th>Summary Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do not inject OSPF summary routes into the stub area.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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

```
configuration 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
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
### 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 "Viptela 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 $1$ZDmsK2bcSoVs.oZxEZFDAVLrBLJCR9.
    !
  !
  logging
    disk
    enable
    !
  !
```

#### 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 Viptela 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>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.</td>
</tr>
</tbody>
</table>
```

Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
```

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 |
```
<table>
<thead>
<tr>
<th>VPN</th>
<th>INTERFACE</th>
<th>IP ADDRESS</th>
<th>RX MBPS</th>
<th>TX Duplex</th>
<th>UPTIME</th>
<th>TX UPTIME</th>
<th>PACKETS</th>
<th>RX PACKETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ge0/1</td>
<td>10.0.26.11/24</td>
<td>Up</td>
<td>Up</td>
<td>null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:62</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>full</td>
<td>00:00:46:41</td>
<td>82</td>
<td>28</td>
<td>0:00:46:41</td>
<td>82</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/2</td>
<td>10.0.5.11/24</td>
<td>Up</td>
<td>Up</td>
<td>null transport</td>
<td>1500</td>
<td>00:0c:29:ab:b7:6c</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>full</td>
<td>00:00:46:41</td>
<td>19399</td>
<td>19368</td>
<td>0:00:46:41</td>
<td>19399</td>
<td>19368</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Down Down null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:76</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>2</td>
<td>0:00:46:41</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Down Down null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:80</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>2</td>
<td>0:00:46:41</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Down Down null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:8a</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>2</td>
<td>0:00:46:41</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Down Down null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:94</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>2</td>
<td>0:00:46:41</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>ge0/7</td>
<td>10.0.110.11/24</td>
<td>Up</td>
<td>Up</td>
<td>null service</td>
<td>1500</td>
<td>00:0c:29:ab:b7:9e</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>full</td>
<td>00:00:46:41</td>
<td>1198</td>
<td>71</td>
<td>0:00:54:34</td>
<td>1198</td>
<td>71</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>system</td>
<td>172.16.255.11/32</td>
<td>Up</td>
<td>Up</td>
<td>null loopback</td>
<td>1500</td>
<td>00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>full</td>
<td>00:00:46:17</td>
<td>0</td>
<td>0</td>
<td>0:00:46:17</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Operational Commands**

- show control local-properties
- show interface vpn 0

**Related Topics**

- [ip address](#), on page 311
- [router-id](#), on page 523
- [router-id](#), on page 522
**system-tunnel-mtu**

Configure the MTU to use on the tunnels that send OMP control traffic between Viptela 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
```

<table>
<thead>
<tr>
<th>MTU:</th>
<th>MTU size to use on tunnels that carry OMP control traffic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range:</td>
<td>500 through 2000 bytes</td>
</tr>
<tr>
<td>Default:</td>
<td>1024 bytes</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 560
**tacacs**

Configure the properties of a TACACS+ server that is used in conjunction with AAA to authorize and authenticate users who attempt to access Viptela 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>server ip-address</strong></td>
<td>Address of TACACS+ Server: IP address of a TACACS+ server host in the local network. You can configure up to 8 TACACS+ servers.</td>
</tr>
<tr>
<td><strong>secret-key password</strong></td>
<td>Authentication Key: secret-key password Key to use for authentication and encryption between the Viptela 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.</td>
</tr>
<tr>
<td><strong>auth-port port-number</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>source-interface interface-name</strong></td>
<td>Interface To Use To Reach Server: Interface on the local device to use to reach the TACACS+ server.</td>
</tr>
<tr>
<td><strong>authentication authentication-type</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**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 Viptela 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.3</td>
<td>source-interface command added.</td>
</tr>
<tr>
<td>15.3.8</td>
<td>secret-key and deprecate key commands added.</td>
</tr>
<tr>
<td>16.2.2</td>
<td>authentication and priority commands added.</td>
</tr>
</tbody>
</table>

**Examples**

**Configure TACACS+**

```
vEdge(config)# system tacacs
vEdge(config-tacacs)# server 1.2.3.4 secret-key $4$aCGzJg5k6M8zj4BgLEFKKw==
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 29
- admin-auth-order, on page 60
- auth-fallback, on page 94
- auth-order, on page 97
- radius, on page 488
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 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.

**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**

<table>
<thead>
<tr>
<th>bytes</th>
<th>Change the Packet Size:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSS</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 552 to 1960 bytes; for PPP interface, 552 to 1452 bytes</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>TCP SYN MSS dynamically adjusted based on the interface or tunnel MTU.</td>
</tr>
<tr>
<td>16.3</td>
<td>Maximum TCP MSS changed from 1460 bytes to 1960 bytes.</td>
</tr>
</tbody>
</table>
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

Operational Commands

show interface

Related Topics

system-tunnel-mtu, on page 556
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 563
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 562
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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
definition-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 640
  zone, on page 650
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**

<table>
<thead>
<tr>
<th>minutes</th>
<th>Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time after which NAT translations over TCP sessions time out.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65536 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: 60 minutes (1 hour)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2.10 and 16.3.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 478
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

<table>
<thead>
<tr>
<th>seconds</th>
<th>Refresh Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 60 through 86400 seconds (1 minute through 1 day)</td>
</tr>
<tr>
<td></td>
<td>Default: 90 seconds</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 inactive 802.1X 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Revoke a client's authentication after 2 hours

```
vpn 0
  interface ge0/7
    dot1x
      timeout
        inactivity 7200
```

Operational Commands

- clear dot1x client
- show dot1x clients
- show dot1x interfaces
- show dot1x radius
show system statistics

**Related Topics**

radius, on page 488
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4.4</td>
<td>Default timeout changed from 30 minutes to 2 minutes.</td>
</tr>
</tbody>
</table>

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 Viptela 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 0:00:00:00
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 626
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spf delay initial-hold-time maximum-hold-time</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

**Set the OSPF SPF timers**

```bash
vEdge# show running-config vpn 1 router ospf
vpn 1
  router
    ospf
timers spf 300 1200 15000
  redistribute static
  redistribute ospf
  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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>advertisement-interval</strong> seconds</td>
<td>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</td>
</tr>
<tr>
<td><strong>connect-retry</strong> seconds</td>
<td>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</td>
</tr>
</tbody>
</table>
### Hold Time

<table>
<thead>
<tr>
<th><strong>holdtime seconds</strong></th>
<th>Hold Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Provisioning the hold time for a specific neighbor overrides the global default or the hold time configured at the global level.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 180 seconds (three times the keepalive timer)</td>
</tr>
</tbody>
</table>

### Keepalive Time

<table>
<thead>
<tr>
<th><strong>keepalive seconds</strong></th>
<th>Keepalive Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Provisioning the keepalive time for a specific neighbor overrides the global default or the keepalive configured at the global level.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 65535 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 60 seconds (one-third the hold-time value)</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.  
  Range: 1 through 604800 seconds (168 hours, or 7 days)  
  Default: 43200 seconds (12 hours) |
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
Default: 60 seconds

Update Advertisement Interval: Configure the amount of time between OMP Update packets.

Range: 0 through 65535 seconds
Default: 1 second

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>14.2</td>
<td>Removed keepalive option; changed default hold-time interval from 15 to 60 seconds; added graceful-restart-timer command.</td>
</tr>
<tr>
<td>15.3</td>
<td>Changed maximum graceful restart timer value to 12 hours.</td>
</tr>
<tr>
<td>15.3.5</td>
<td>Change default graceful restart timer value to 12 hours, and changed maximum graceful restart timer value to 7 days.</td>
</tr>
<tr>
<td>16.2</td>
<td>Added eor-timer command</td>
</tr>
</tbody>
</table>

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 255
- rekey, on page 503
**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**

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Local Router's WAN Transport Interface:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 lte
   !
no shutdown
!
interface ge0/2.102
```

---

Configuration Commands

583
ip address 102.1.19.15/24
mtu 1496
tunnel-interface
color mpls
no shutdown
!

vEdge2# show running-config vpn 0
interface ge0/0
ip address 172.16.255.2
tunnel-interface
color lte
no shutdown
!
in interface ge0/3
ip address 172.16.255.16
tunnel-interface
color mpls
no shutdown
!
in interface ge0/2.101
ip address 101.1.19.16/24
mtu 1496
tloc-extension ge0/0
no shutdown
!
in 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 tllocs

Related Topics
allow-same-site-tunnels, on page 70
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

<table>
<thead>
<tr>
<th>wan-interface-name</th>
<th>Interface Name: Name of WAN interface that you are using for sending traffic over the extended TLOC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>extended-wan-interface-ip-address</td>
<td>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.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.9.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 ge0/2.101
    encapsulation dot1q 101
    ip address 30.1.19.16/24
    mtu 1496
  !
  interface ge0/2.102
    encapsulation dot1q 102
    ip address 40.1.19.16/24
    mtu 1496

585
sdwan
interface ge0/0
  ip address 172.16.255.2
  tunnel-interface
    color lte

interface ge0/2.101
tloc-extension-gre-from 10.1.19.15 xconnect GigabitEthernet0/0

interface ge0/2.102
tloc-extension-gre-from 20.1.19.15 xconnect GigabitEthernet0/3

interface ge0/3
  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 587
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

<table>
<thead>
<tr>
<th>extended-interface-ip-address</th>
<th>IP Address of GRE Tunnel Destination:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GRE tunnel destination IP address of the interface that you are extended to another router in the branch.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.9.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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.

ISRK1# show sdwan running-config
sdwan
  interface ge0/2.101
    no shutdown
    encapsulation dot1 101
    ip address 10.1.19.15/24
    mtu 1496
  !
  interface ge0/2.102
    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 ge0/2.101
  tunnel-interface
color lte
tloc-extension-gre-to 30.1.19.16

! interface ge0/2.102
  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 585
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 responses, the static route is added back to the route table.

vManage Feature Template

For all vEdge devices:

```
Configuration ► Templates ► System
```

Command Hierarchy

```
system
  track-default-gateway
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3.5</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.4</td>
<td>Number of retries changed from 3 to 10.</td>
</tr>
</tbody>
</table>

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 321
```
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

<table>
<thead>
<tr>
<th>number</th>
<th>Tag:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the tag string to include in routes associated with a network that is connected to a non-operational interface.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 4294967295</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3.8 and 15.4.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 590
track-transport

Regularly check whether the DTLS connection between the local device and a vBond orchestrator is up. By default, transport checking is enabled.

vManage Feature Template

For all vEdge devices:

Configuration ► Templates ► System

Command Hierarchy

system
   [no] track-transport

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>TRACK</th>
<th>TYPE</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>HOST</th>
<th>INDEX</th>
<th>TIME</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>-</td>
<td>2001:cdba::1:2</td>
<td>system12.vbond</td>
<td>0</td>
<td>Wed May 10 10:27:29 2017</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>system</td>
<td>-</td>
<td>2001:cdba::1:3</td>
<td>system12.vbond</td>
<td>0</td>
<td>Wed May 10 10:29:01 2017</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>Wed May 10 10:27:30 2017</td>
<td>down</td>
<td></td>
</tr>
</tbody>
</table>

Operational Commands

show transport connection
tracker

Track the status of transport interfaces that connect to the internet (on vEdge routers only).

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.

vManage Feature Template

For vEdge routers only:
Configuration ► Templates ► System
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

system
  tracker tracker-name
    endpoint-dns-name dns-name
    endpoint-ip ip-address
    interval seconds
    multiplier number
    threshold milliseconds

vpn 0
  interface interface-name
  tracker tracker-name

Syntax Description

<table>
<thead>
<tr>
<th>endpoint-dns-name</th>
<th>DNS Name of Interface End Point:</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-name</td>
<td>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.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>endpoint-ip ip-address</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>interval seconds</strong></td>
<td>Interval between Status Probes</td>
</tr>
<tr>
<td><strong>multiplier number</strong></td>
<td>Number of Retries</td>
</tr>
<tr>
<td><strong>threshold milliseconds</strong></td>
<td>Time To Wait for Response</td>
</tr>
<tr>
<td><strong>tracker-name</strong></td>
<td>Tracker Name</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

Enable transport tracking on a NAT interface.

```
system
 tracker nat-tracker
   endpoint-ip 1.2.3.4
   vpn 0
 interface ge0/1
    nat
 tracker nat-tracker
```

**Operational Commands**

```
show running-config system
```
Related Topics

nat, on page 417
**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 viptela command to display these messages.

For SNMPv3, the PDU type for notifications is 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group group-name</td>
<td>Group Name: Name of the trap group. It can be from 1 to 32 characters.</td>
</tr>
<tr>
<td>level severity</td>
<td>Severity Level: Severity level of the trap. Severity can be <strong>critical</strong>, <strong>major</strong>, or <strong>minor</strong>. You can specify one, two, or three severity levels for each trap type.</td>
</tr>
</tbody>
</table>
**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 Viptela 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

### 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 599
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>community-name</code></td>
<td>Community Name: Name of an SNMP community configured with the <code>community</code> command.</td>
</tr>
<tr>
<td><code>group group-name</code></td>
<td>Group Name: Name of a trap group configured with the <code>trap group</code> command.</td>
</tr>
<tr>
<td><code>source-interface</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>vpn vpn-id ipv4-address udp-port</code></td>
<td>Trap Target: Location of the SNMP server to receive the trap information. You must specify the following: <code>vpn vpn-id</code>—Number of the VPN to use to reach to the SNMP server. It can be a value from 0 through 65530. <code>ipv4-address</code>—IPv4 address of the SNMP server. <code>udp-port</code>—UDP port number to connect to on the SNMP server. The number can be a value from 1 through 65535.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
### 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 eth0
!
  trap group test
  all
  level critical major minor
!
```

### Operational Commands

- `show running-config snmp`

### Related Topics

- `show notification stream`
- `trap group`, on page 596
**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**

<table>
<thead>
<tr>
<th><code>ip-address</code></th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address of the destination of a GRE tunnel interface.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 gre 1
    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 338
- tunnel-source, on page 608
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dns-name</code></td>
<td>DNS Name: DNS name that points to the destination of the IPsec tunnel.</td>
</tr>
<tr>
<td><code>ipv4-address</code></td>
<td>IPv4 Address: IPv4 address of the tunnel's destination.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 283
tunnel-source, on page 607
tunnel-source-interface, on page 610
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>19.1</td>
<td>Added group option.</td>
</tr>
</tbody>
</table>

**Examples**

*Create a tunnel for LTE traffic*

```bash
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**

<table>
<thead>
<tr>
<th><code>ipv4-address</code></th>
<th>Source Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source IPv4 address of the IPsec tunnel. This is an address in VPN 0 on the local vEdge router.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 283
- `tunnel-destination`, on page 603
- `tunnel-source-interface`, on page 610
**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**

<table>
<thead>
<tr>
<th><code>ip-address</code></th>
<th>Source Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source IP address of a GRE tunnel. This is an address on the local vEdge router.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 338
- tunnel-destination, on page 601
- tunnel-source-interface, on page 611
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**

<table>
<thead>
<tr>
<th><code>interface name</code></th>
<th>Source Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 283
- `tunnel-destination`, on page 603
- `tunnel-source`, on page 607
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**

<table>
<thead>
<tr>
<th><strong>interface-name</strong></th>
<th><strong>Source Address:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 338
- [tunnel-destination](#), on page 601
- [tunnel-source](#), on page 608
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

<table>
<thead>
<tr>
<th>minutes</th>
<th>Time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Time after which NAT translations over UDP sessions time out.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 65536 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: 1 minute</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ip-address</th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address to use for the TCP connection to the neighbor, in decimal four-part dotted notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interface-name</th>
<th>Interface Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface name to use for the TCP connection to the neighbor.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Configure the IP address to use for the TCP connection to the BGP neighbor

```
v6# 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 $4$L3rwZmsI1ZB6wtBgLEFXKw==
    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.

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

<table>
<thead>
<tr>
<th>minutes</th>
<th>Time To Wait for Confirmation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 5 through 60 minutes</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2</td>
<td>Support for vBond orchestrator, vManage NMS, and vSmart controller added.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auth</strong></td>
<td>Authentication Type and Password:</td>
</tr>
<tr>
<td><strong>authentication</strong></td>
<td>Authentication mechanism to use for the user. <strong>authentication</strong> can be either message digest5 (md5) or SHA-2 message digest (sha). Enter the password either in cleartext or as an AES-encrypted key.</td>
</tr>
<tr>
<td><strong>auth-password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>group</strong></td>
<td>Group Name:</td>
</tr>
<tr>
<td><strong>group-name</strong></td>
<td>Name of an SNMPv3 group configured with the <strong>snmp group</strong> command. <strong>group-name</strong> can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td><strong>priv</strong></td>
<td>Privacy Type and Password:</td>
</tr>
<tr>
<td><strong>privacy</strong></td>
<td>Privacy mechanism to use for the user. <strong>privacy</strong> 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, <strong>privacy</strong> can also be the data encryption standard algorithm (des).</td>
</tr>
<tr>
<td><strong>priv-password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>Enter the password either in cleartext or as an AES-encrypted key.</td>
</tr>
<tr>
<td><strong>user</strong></td>
<td>Username:</td>
</tr>
<tr>
<td><strong>username</strong></td>
<td>Name of an SNMP user. It can be 1 to 32 alphanumeric characters. If the name includes spaces, enclose it in quotation marks (&quot; &quot;).</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.2</td>
<td>Support for DES privacy removed.</td>
</tr>
</tbody>
</table>
Operational Commands

show running-config snmp

Related Topics

  group, on page 258
system aaa user: Configure a login account for each user who can access the local Viptela 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

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Authorization Group: Name of an authorization group configured with the usergroup command. You must assign the user to one or more groups.</td>
</tr>
<tr>
<td>group-name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User-name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-name</td>
<td>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 lower case letters, the digits 0 through 9, hyphens (-), underscores (<em>), 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 (</em>) 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.</td>
</tr>
</tbody>
</table>

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 directory of /home/username (so, /home/eve).
**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 into 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.

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>14.1</td>
</tr>
<tr>
<td>17.1</td>
</tr>
</tbody>
</table>

**Examples**

**Configure a user whose role is to be a system operator**

Viptela# config
Entering configuration mode terminal
Viptela(config)# system aaa
vedge-1(config-aaa)# user eve
Viptela(config-user-eve)# password 123456
Viptela(config-user-eve)# group operator
Viptela(config-user-eve)# exit
Viptela(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 94
auth-order, on page 97
radius, on page 488
tacacs, on page 557
usergroup, on page 624
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

<table>
<thead>
<tr>
<th>group-name</th>
<th>Group Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 (<em>), 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 (</em>) characters. The name cannot contain any uppercase letters.</td>
</tr>
</tbody>
</table>

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, nongroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, ump, 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).
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.

<table>
<thead>
<tr>
<th>Task (interface</th>
<th>policy</th>
<th>routing</th>
<th>security</th>
<th>system) (read</th>
<th>write)</th>
<th>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.</th>
</tr>
</thead>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.3</td>
<td>Force a user to log out when their permissions are changed.</td>
</tr>
<tr>
<td>17.1</td>
<td>Increase maximum group name to 128 characters and support periods (.) in group name.</td>
</tr>
</tbody>
</table>

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 488
  tacacs, on page 557
  user, on page 621
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

<table>
<thead>
<tr>
<th>vbond-only</th>
<th>Configure Device To Be only a vBond Orchestrator:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Deprecated starting with Release 16.1)</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>dns-name</th>
<th>DNS Name of the vBond Orchestrator:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DNS name that points to one vBond orchestrator or to a number of vBond orchestrators. The addresses can resolve to vBond orchestrators configured with IPv4 addresses, with IPv6 addresses, or with both IPv4 and IPv6 adresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip-address</th>
<th>IP Address of the vBond Orchestrator:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>local</th>
<th>Local vBond System:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(On vBond orchestrator only. Designate the local vEdge router to be a vBond orchestrator in the vEdge overlay network domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Starting in Release 16.3, if you configure the <code>local</code> 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.</td>
</tr>
</tbody>
</table>
### 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.

### Multiple vBond Orchestrators:
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 to Connect to vBond Orchestrator:
Port number to use to connect to the vBond orchestrator.

<table>
<thead>
<tr>
<th>Port number</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>If you do not want to rotate through these three port numbers, configure the port number to use to connect to the vBond orchestrator.</td>
<td></td>
</tr>
<tr>
<td>Default: 12346</td>
<td></td>
</tr>
<tr>
<td>Range: 1 through 65535</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>14.3</td>
<td><strong>ztp-server</strong> option added.</td>
</tr>
<tr>
<td>16.1</td>
<td><strong>vbond-only</strong> option deprecated.</td>
</tr>
</tbody>
</table>

**Examples**

Configure the DNS name of a vBond orchestrator on a vEdge router:

```plaintext
system
  vbond vbond.east.acme.com
!`
```

Designate the local vEdge router to be a vBond orchestrator in its vEdge overlay network domain:

```plaintext
system
  vbond 10.0.4.12 local
!`
```

Designate the local vEdge router to be an enterprise ZTP server:

```plaintext
system
  vbond 75.1.16.4 local ztp-server
!`
```

**Operational Commands**

- nslookup
- show control connections

**Related Topics**

- port-hop, on page 468
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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
cshow running-config

Related Topics
allow-service, on page 72
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

<table>
<thead>
<tr>
<th>exclude</th>
<th>Include or Exclude a Subtree of MIB Objects:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you omit the <code>exclude</code> option in the <code>oid</code> command, the subtree of MIB objects is included, or viewable, in the MIB view.</td>
</tr>
<tr>
<td></td>
<td>If you specify the <code>exclude</code> 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).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>oid</th>
<th>Object Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>view string</th>
<th>View Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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 (&quot; &quot;).</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>16.2</td>
<td>Wildcard for configuring OID subtree added.</td>
</tr>
</tbody>
</table>

Examples

Create a view of the Internet portion of the SNMP MIB:

```
Viptela# 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 Viptela MIB:
viptela(config-snmp)# view viptela-private oid 1.3.6.1.4.1.41916

Configure a MIB view for system status:
Viptela(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

<table>
<thead>
<tr>
<th>vlan-id</th>
<th>VLAN Tag:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VLAN identifier to associate with the bridging domain.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4095</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>number</th>
<th>Preference Value:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 8</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 372
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 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)
```
Configuration Commands

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)
gos-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
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
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-destination (tunnel-source ip-address | tunnel-source-interface interface-name) (GRE interfaces; on vEdge routers only)
tunnel-destination (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

<table>
<thead>
<tr>
<th>vpn-id</th>
<th>VPN Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Values: On vEdge routers: 0 through 65530</td>
</tr>
<tr>
<td></td>
<td>On Viptela controller devices: 0, 512</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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

```plaintext
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

<table>
<thead>
<tr>
<th><code>policy-name</code></th>
<th>VPN Membership Policy Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the VPN membership policy to configure or to apply to a list of sites in the overlay network. <code>policy-name</code> can be up to 32 characters long.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

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 194
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 master, thus assuming the role of the default gateway, and the other routers take the role of slave. When the master router fails, one of the slaves is elected as the new master 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn vpn-id</td>
<td></td>
</tr>
<tr>
<td>interface gslot/port[.subinterface]</td>
<td></td>
</tr>
<tr>
<td>vrrp group-number</td>
<td></td>
</tr>
<tr>
<td>ipv4 ip-address</td>
<td></td>
</tr>
<tr>
<td>priority number</td>
<td></td>
</tr>
<tr>
<td>timer seconds</td>
<td>(track-omp</td>
</tr>
</tbody>
</table>

Syntax Description

<table>
<thead>
<tr>
<th>timer seconds</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Advertisement Time:</td>
</tr>
<tr>
<td></td>
<td>How often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master.</td>
</tr>
<tr>
<td></td>
<td>For Cisco vEdge Devices</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 1 second</td>
</tr>
<tr>
<td></td>
<td>For Cisco XE SD-WAN Routers</td>
</tr>
<tr>
<td></td>
<td>Range: 100 through 3600 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 100 milliseconds</td>
</tr>
</tbody>
</table>
| **priority number** | Priority To Be Elected Master:  
Priority level of the router. The router with the highest priority is elected as master. If two vEdge routers have the same priority, the one with the higher IP address is elected as master.  
Range: 1 through 254  
Default: 100 |
|---|---|
| *(track-omp | track-prefix-list)*  
*list-name | list-name) | Track Interface State:  
By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which vEdge router is the master virtual router. When the interface for the master goes down, a new VRRP master 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 master virtual router. If all OMP sessions are lost on the master 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 master. 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 60 seconds.) Until the hold timer expires and a new VRRP master is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as master 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 24 groups.  
Range: 1 through 255 |
| **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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>15.2</td>
<td>Tracking by prefix list added.</td>
</tr>
<tr>
<td>18.3</td>
<td>You can configure a maximum of 24 VRRP groups on a router.</td>
</tr>
</tbody>
</table>

Example: Configure VRRP in VPN 1, on the subinterface ge0/1.3 on vEdge Devices

```bash
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

```bash
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
        vrrp v2
            address 10.180.4.1
            priority 90
            timers advertise 1000
            exit
        exit
```

Note: For Cisco XE SD-WAN devices, the VRRP timer range is 100 to 3600 milliseconds

Related Topics

- timers, on page 580
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 181
- [radius](#), on page 488
**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**

<table>
<thead>
<tr>
<th><code>radio-band</code></th>
<th>WLAN Frequency:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select the radio band for the WLAN channel to use:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The allowable channels and the maximum transmission power for these channels are country specific.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>
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+IEZB2vcQpeEoSR4ia9JqgDsPN0HukAb8fVxAg5I=
    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 488
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.3</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Examples

Set a WPA password for a VAP interface (that is, for an SSID)

```
vEdge# show running-config wlan 5GHz 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 197
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpn</code></td>
<td>VPN: Numeric identifier of the VPN. Range: 0 through 65530</td>
</tr>
<tr>
<td><code>vpn-id</code></td>
<td>Zone Name: Name of the zone.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 652
  zone-pair, on page 654
  zone-to-nozone-internet, on page 656
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**

<table>
<thead>
<tr>
<th><code>zone-policy-name</code></th>
<th>Zone Policy Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 650
  zone-pair, on page 654
  zone-to-nozone-internet, on page 656
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-zone zone-name</td>
<td>Destination Zone: Name of the destination zone. This is the zone to which traffic flows are destined, and that you configured with the <code>policy zone</code> command.</td>
</tr>
<tr>
<td>source-zone zone-name</td>
<td>Source Zone: Name of the source zone. This is the zone from which traffic flows are sent, and that you configured with the <code>policy zone</code> command.</td>
</tr>
<tr>
<td>zone-policy zone-policy-name</td>
<td>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 <code>policy zone-based-policy</code> command.</td>
</tr>
<tr>
<td>pair-name</td>
<td>Zone Pair Name: Name of the zone pairing.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Examples**

**Configure and apply a simple zone-based firewall policy**

```plaintext
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 650
  zone-based-policy, on page 652
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**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 650
- zone-based-policy, on page 652
- zone-pair, on page 654