
VPN-Interface-Ethernet

You can use the VPN-Interface-Ethernet template for all Viptela devices.

To configure the Ethernet interfaces in a VPN using vManage templates:

1. Create a VPN-Interface-Ethernet feature template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the Configuration ► Templates ► [VPN](#) help topic.
3. Optionally, on vEdge routers, to enable DHCP server functionality on the interface, create a DHCP-Server feature template. See the Configuration ► Templates ► [DHCP-Server](#) help topic.
4. Create a device template that incorporates the VPN-Interface-Ethernet, VPN, and DHCP-Server feature templates. See the Configuration ► [Templates](#) help topic.

Navigate to the Template Screen

1. In vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select one or more devices. The right pane displays the available templates for the selected devices.
5. Select the VPN-Interface-Ethernet template.

The right pane displays the VPN-Interface-Ethernet template form.

- The top of the form contains fields for naming the template.
- The bottom contains fields for defining parameters applicable to that template.
- A drop-down menu to the left of each parameter field defines the scope of the parameter. When you first open a feature template form, for each parameter that has a default value, the scope is set to Default. To edit a parameter field, change the scope to Global or Device Specific. Note that if a parameter's scope is Device Specific, you cannot enter a value for it in the feature template. Instead, you enter a value when you attach the template to a device.
- A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.

Minimum Interface Configuration

The following parameters are required (unless otherwise indicated) to configure a VPN interface on a vEdge router:



Step	Parameter Field	Procedure
1.	Template Name	Enter a name for the template. It can be up to 128 characters and can contain only alphanumeric characters.
2.	Description (Template)	Enter a description for the template. It can be up to 2048 characters and can contain only alphanumeric characters.
3.	Shutdown	Click No to enable the interface.
4.	Interface name	Enter a name for the interface
5.	Description (optional)	Enter a description for the interface.
6.	IP configuration	For an interface in VPN 0, you can select Dynamic to set the interface as a DHCP client, to allow the interface to receive its IP address from a DHCP server. If you select Dynamic, you can set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default administrative distance is 1.
7.	IP address	Enter the IPv4 address of the interface if the interface is not receiving its IP address from a DHCP server.
8.	DHCP helper (optional, on vEdge routers)	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
9.	Save	Click Save to save the feature template.

CLI equivalent:

```

vpn vpn-id
interface interface-name
  description text
  dhcp-helper ip-address (on vEdge routers only)
  (ip address address/subnet | ip dhcp-client [dhcp-distance number])
  [no] shutdown

```

Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

On vSmart controllers and vManage NMSs, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport



interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab:

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection (on vEdge routers)	If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.
Max Control Connections (on vEdge routers)	Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. <i>Range:</i> 0 through 8 <i>Default:</i> 2
Allow Service	Select On or Off for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click Advanced Options:

Parameter Name	Description
Encapsulation (on vEdge routers)	Select the encapsulation type to use on the tunnel interface, either IPsec or GRE. The default is IPsec. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
Preference (on vEdge routers)	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. <i>Range:</i> 0 through 4294967295 <i>Default:</i> 0
Weight (on vEdge routers)	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind loopback tunnel (on vEdge routers)	Enter the name of a physical interface to bind to a loopback interface.



Parameter Name	Description
Hello interval (on vSmart and vManage devices)	Set the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 1000 milliseconds (1 second)
Hello tolerance (on vSmart and vManage devices)	Set how long to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

CLI equivalent:

```

vpn 0
  interface interface-name
    tunnel-interface
      allow-service service-name
      bind interface-name (on vEdge routers only)
      carrier carrier-name
      color color
      encapsulation (gre | ipsec) (on vEdge routers only)
      preference number
      weight number
      hello-interval milliseconds (on vSmart and vManage devices only)
      hello-tolerance seconds (on vSmart and vManage devices only)
      max-control-connections number (on vEdge routers only)

```

Configure the Interface as a NAT Device (on vEdge Routers)

To configure an interface to act as a NAT device, select the NAT tab, click On, and click the plus sign (+) to add a port forwarding rule:

Parameter Name	Description
Port Forward	Define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.
Port Start Range	Enter a port number to define the port or first port in the range of interest. <i>Range:</i> 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. <i>Range:</i> 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. <i>Range:</i> 0 through 65530



Parameter Name	Description
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

To configure other NAT parameters, click Advanced Options:

Parameter Name	Description
Refresh mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). <i>Default:</i> Outbound
UDP timeout	Specify when NAT translations over UDP sessions time out. <i>Range:</i> 1 through 65536 minutes <i>Default:</i> 1 minutes
TCP timeout	Specify when NAT translations over TCP sessions time out. <i>Range:</i> 1 through 65536 minutes <i>Default:</i> 60 minutes (1 hour)
Block ICMP	Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages. <i>Default:</i> Off
Respond to Ping	Select On to have the vEdge router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

CLI equivalent:

```

vpn vpn-id
interface interface-name
  nat
  block-icmp-error
  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
  tcp-timeout minutes
  udp-timeout minutes

```

Configure VRRP (on vEdge Routers)

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab and click the plus sign (+) to add a VRRP group:



Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. <i>Range:</i> 1 through 255
Priority	Enter the 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. <i>Range:</i> 1 through 254 <i>Default:</i> 100
Timer	Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. <i>Range:</i> 1 through 3600 seconds <i>Default:</i> 1 second
Track OMP Track Prefix List	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. 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, configure one of the following: Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the master VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the master VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP.

CLI equivalent:

```
vpn vpn-id
interface geslot/port[.subinterface]
  vrrp group-number
  ipv4 ip-address
  priority number
  timer seconds
  (track-omp | track-prefix-list list-name)
```

Apply Access Lists (on vEdge Routers)

To configure a shaping rate to a router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL tab:



Parameter Name	Description
Shaping rate	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite rule	Click On, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL	Click On, and specify the name of the access list to apply to packets being received on the interface.
Egress ACL	Click On, and specify the name of the access list to apply to packets being transmitted on the interface.
Ingress policer	Click On, and specify the name of the policer to apply to packets being received on the interface.
Egress policer	Click On, and specify the name of the policer to apply to packets being transmitted on the interface.

CLI equivalent:

```
vpn vpn-id
interface interface-name
  access-list acl-list (in | out)
  policer policer-name (in | out)
  qos-map name
  rewrite-rule name
  shaping-rate name
```

Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab and click the plus sign (+):

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

To add another ARP table entry, click the plus sign (+).

To delete an ARP table entry, click the trash icon on the right side of the entry.

CLI equivalent:

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

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab:



Parameter Name	Description
Duplex	Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. <i>Default:</i> full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes
PMTU discovery	Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.
Flow control	Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. <i>Values:</i> autonet, both, egress, ingress, none <i>Default:</i> autoneg
TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. <i>Values:</i> 10, 100, or 1000 Mbps <i>Default:</i> Autonegotiate (10/100/1000 Mbps)
Clear-Don't-Fragment	Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static ingress QoS (on vEdge routers)	Specify a queue number to use for incoming traffic. <i>Range:</i> 0 through 7
ARP timeout (on vEdge routers)	Specify how long it takes for a dynamically learned ARP entry to time out. <i>Range:</i> 0 through 2678400 seconds (744 hours) <i>Default:</i> 1200 seconds (20 minutes)
Autonegotiate	Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration



Parameter Name	Description
Extension (on vEdge routers)	then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.

CLI equivalent:

```

vpn vpn-id
interface interface-name
  arp-timeout seconds (on vEdge routers only)
  [no] autonegotiate
  clear-dont-fragment
  duplex (full | half)
  flow-control control
  mac-address mac-address
  mtu bytes
  pmtu
  speed speed
  static-ingress-qos number (on vEdge routers only)
  tcp-mss-adjust bytes
  tloc-extension interface-name (on vEdge routers only)

```

Release Information

Introduced in vManage NMS Release 15.2.

