

---

## VPN-Interface-PPP

You can use the VPN-Interface-PPP template for vEdge Cloud and vEdge router devices.

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. PPP properties are associated with a PPPoE-enabled interface on vEdge routers to connect multiple users over an Ethernet link.

To configure PPPoE on vEdge routers using vManage templates:

1. Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface, as described in this article.
2. Create a VPN-Interface-PPP-Ethernet feature template to configure a PPPoE-enabled interface. See the Configuration ► Templates ► [VPN-Interface-PPP-Ethernet](#) help topic.
3. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the Configuration ► Templates ► [VPN](#) help topic.
4. Create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN 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-PPP template.

The right pane displays the VPN-Interface-PPP 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 PPP Virtual Interface Configuration

The following parameters are required (unless otherwise indicated) to create a PPP virtual 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 PPP virtual interface.
4.	Interface Name	Enter the number of the PPP interface. It can be a number from 1 through 31.
5.	Description (optional)	Enter a description for the PPP virtual interface.
6.	Authentication Protocol	In the PPP tab, select the authentication protocol used by PPPoE: <ul style="list-style-type: none"><li>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters.</li><li>• PAP—Enter the username and password provided by your ISP. <i>username</i> can be up to 255 characters.</li></ul>
7.	Save	Click Save to save the feature template.

CLI equivalent:

```
vpn 0
interface pppnumber
  ppp
  authentication
    chap hostname name password password
    pap password password sent-username name
  [no] shutdown
```

## Configure the Access Concentrator Name

To configure the access concentrator name, select the PPP tab:

Parameter Name	Description
AC Name	Name of the access concentrator used by PPPoE to route connections to the Internet.

CLI equivalent:

```
vpn 0
interface pppnumber
  ppp
```



## 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.

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	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	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	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	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	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to



Parameter Name	Description
	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	Enter the name of a physical interface to bind to a loopback interface.
Hello interval	Set how often BFD sends Hello packets on the transport tunnel. <i>Range:</i> 100 through 300000 milliseconds (5 minutes) <i>Default:</i> 1000 milliseconds (1 second)
Hello tolerance	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 600 seconds (10 minutes) <i>Default:</i> 12 seconds

CLI equivalent:

```

vpn 0
  interface interface-name
  tunnel-interface
  allow-service service-name
  bind interface-name
  carrier carrier-name
  color color
  encapsulation (gre | ipsec)
  preference number
  weight number
  hello-interval milliseconds
  hello-tolerance seconds
  max-control-connections number

```

## Configure the Interface as a NAT Device

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.



Parameter Name	Description
	<i>Range:</i> 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter the larger number to apply it to a range or 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 65535
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

```

## Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab:

Parameter Name	Description
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 0
interface pppnumber
access-list acl-list (in | out)
policer policer-name (in | out)
rewrite-rule name

```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab:

Parameter Name	Description
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
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
Clear Dont	Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.



Parameter Name	Description
Fragment	When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration 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
  clear-dont-fragment
  mac-address mac-address
  mtu bytes
  tcp-mss-adjust bytes
  tloc-extension interface-name

```

## Release Information

Introduced in vManage NMS in Release 15.3.

