

---

## VPN-Interface-Cellular

You can use the VPN-Interface-Cellular feature template to configure cellular module parameters on vEdge routers.

To configure cellular interfaces using vManage templates:

1. Create a VPN-Interface-Cellular feature template to configure cellular module parameters, as described in this article.
2. Create a Cellular-Profile template to configure the profiles used by the cellular modem. See [Configure Cellular Profiles](#).
3. Create a VPN feature template to configure VPN parameters. See [Configure Segmentation \(VPNs\) on vEdge Routers](#).
4. Create a device template that incorporates the two cellular feature templates and the VPN feature template. See [Create Configuration Templates for a vEdge Router](#).

---

## 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-Cellular template.

The right pane displays the VPN-Interface-Cellular 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 from, for each parameter that has a default value, the scope is set to Default. To edit a parameter, 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 Cellular Interface Configuration

The following parameters are required (unless otherwise indicated) to create a cellular interface:



Step	Parameter Field	Procedure
1.	Template Name	Enter the template name. It can contain only alphanumeric characters.
2.	Description (Template)	Enter a description for the template. It can contain only alphanumeric characters.
3.	Technology	Enter the radio access technology (RAT) with the cellular interface. The default is <b>lte</b> . It can also be <b>auto</b> and <b>cdma</b> . (In Releases 16.2.10 and later.)
4.	Shutdown	Click No to enable the interface.
5.	Interface name	Enter the name of the interface. It must be <b>cellular0</b> .
6.	Profile ID	Enter the identification number of the cellular profile. This is the profile identifier that you configure in the Cellular-Profile template. <i>Range:</i> 1 through 15
7.	Description (optional)	Enter a description of the cellular interface.
8.	IP configuration (optional)	For an interface in VPN 0, you can select Dynamic to set the interface as a DHCP client in order to allow it to receive its IP address from a DHCP server. If you select Dynamic, you can also optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.
9.	IP address	Enter the IPv4 address for the interface.
10.	DHCP helper (optional)	To set the interface as a DHCP helper interface, enter up to four IP addresses for DHCP servers in the network, separated by commas. A DHCP helper interface forwards broadcast DHCP requests that it receives from the specified DHCP servers.
11.	Interface tunnel	Under the Interface Tunnel tab, set Tunnel Interface to On and select a Color.
12.	IP MTU	Under the Advanced tab, enter 1428 for the IP MTU. You cannot use a different value.
13.	Save	Click Save to save the feature template.

CLI equivalent:

```

vpn 0
interface cellular0
ip dhcp-client
technology technology
tunnel-interface
color color
!
mtu 1428
profile number
no shutdown
!

```



---

## Create a Tunnel Interface

To configure an interface in VPN 0 to be a WAN transport connection, you must configure a tunnel interface on the cellular interface. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select On and select a color for the interface, as described in the previous section. You can generally accept the system defaults for the remainder of the tunnel interface settings.

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

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC. The color typically used for cellular interface tunnels is <b>lte</b> .
Control Connection	The default is On, which establishes a control connection for the TLOC. If the vEdge router has multiple TLOCs, click No to have a tunnel not establish a TLOC.
Max Control Connections	Set 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	Click On or Off for each service to allow or disallow the service on the cellular interface.

To configure additional tunnel interface parameters, click Advanced Options:

Parameter Name	Description
Encapsulation	Select the encapsulation to use on the tunnel interface. The default is IPsec. You can select both IPsec and GRE encapsulation. In this case, two TLOCs are created for the tunnel interface, and they have the same IP address and color, but they have different encapsulations.
Preference	Enter a value to set the preference 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 the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1



Parameter Name	Description
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default</i> <i>Default: default</i>
Bind loopback tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the format <b>geslot/port</b> .
Last resort circuit	Use the tunnel interface as the circuit of last resort
Hold time	Set the delay before switching back to the primary tunnel interface from a circuit of last resort. <i>Range: 1000 through 10000 milliseconds (1 through 10 seconds)</i> <i>Default: 7000 milliseconds (7 seconds)</i>
NAT refresh interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range: 1 through 60 seconds</i> <i>Default: 5 seconds</i>
Hello interval	Set how often BFD sends Hello packets on the transport tunnel. <i>Range: 100 through 300000 milliseconds (5 minutes)</i> <i>Default: 1000 milliseconds (1 second)</i>
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: 12 through 600 seconds (10 minutes)</i> <i>Default: 12 seconds</i>

CLI equivalent:

```

vpn 0
interface cellular0
 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
  hold-time milliseconds
  max-control-connections number
  last-resort-circuit
  nat-refresh-interval seconds

```

## Configure the Cellular Interface as a NAT Device

To configure a cellular 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 the port name 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 name 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 traffic for the port forward rule. 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
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> 60 minutes (1 hour)
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 0
interface cellular0
  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 access lists (ACLs) to cellular interfaces, 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 0
interface cellularnumber
  access-list acl-list (in | out)
  policer policer-name (in | out)
  qos-map name
  rewrite-rule name
  shaping-rate name

```

## Configure Other Interface Properties

To configure other interface properties, select the Advanced tab:

Parameter Name	Description
IP MTU	Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value.
PMTU discovery	Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.



Parameter Name	Description
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-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	Select a queue number to use for incoming traffic. <i>Range:</i> 0 through 7
ARP timeout	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 extension	Enter the name of a physical interface on the same router that connects to the WAN transport. 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 0
interface cellular0
  arp-timeout seconds
  [no] autonegotiate
  clear-dont-fragment
  mtu 1428
  pmtu
  static-ingress-qos number
  tcp-mss-adjust bytes
  tloc-extension interface-name

```

## Release Information

Introduced in vManage NMS in Release 16.1.

In Release 16.2, add circuit of last resort and its associated hold time.

In Release 16.2.10, add support for configuration RAT.

