



Cellular Interfaces

- [Feature history for cellular interfaces, on page 1](#)
- [Cellular interfaces, on page 2](#)
- [Supported devices, on page 3](#)
- [Guidelines, on page 4](#)
- [Configure cellular interface, on page 5](#)
- [Reset the profile configuration of a cellular modem using CLI commands, on page 24](#)
- [Troubleshoot LTE modem crash, on page 24](#)

Feature history for cellular interfaces

Table 1: Feature History

| Feature Name | Release Information | Description |
|---|---|--|
| Configure Cellular Interfaces | Cisco Catalyst SD-WAN Manager Release 18.1.1 | You can configure cellular interfaces on devices with cellular modules to enable LTE connectivity. |
| Ability to Configure APNs under Running Configurations for Single and Dual SIMs | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1 | This feature allows you to create a data profile for a cellular device. |
| Cellular Module Support for Cisco Catalyst Rugged Series Routers | Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4 | Support for cellular modules on Cisco Catalyst IR1101, IR1800 and IR18340 Rugged Series Routers. |

| Feature Name | Release Information | Description |
|---|--|--|
| Reset the Profile Configuration of Cellular Modem | Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1 | This sub-feature of the Cellular Controller feature enables you to reset the configuration of a cellular modem operating on a device using CLI. |
| Band Select Support in Controller Mode | Cisco Catalyst SD-WAN Manager Release 20.18.1 | This sub-feature of the Cellular Controller feature introduces the Cellular Band Select feature-parcel, enabling you to specify which cellular bands to use. |

Cellular interfaces

A cellular interface is a network interface that

- enables wireless communication over a cellular network, and
- provides wireless connectivity when all wired WAN tunnel interfaces on the device are unavailable.

You can also use a cellular network as the primary WAN link for a branch office, depending on usage patterns within the branch office and the data rates supported by the core of the service provider's cellular network.

Cellular module

A cellular module

- is installed in a router to enable LTE connectivity,
- provides wireless connectivity over a service provider's cellular network, and
- supports network access for use cases such as branch office connectivity.

Data profile

A data profile for a cellular device

- defines parameters for how the device connects to a cellular network, and
- uses the parameters for communication with the service provider.

Supported devices

Table 2: Supported Platforms and Modules

| Platform | Minimum Supported Release | Supported Modules |
|-----------------------------|--|--|
| IR1101 Rugged Series Router | Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1 | P-LTE-MNA, P-LTE-VZ, P-LTE-US, P-LTE-GB, P-LTE-IN, P-LTE-JN, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL, P-5GS6-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4 | P-LTEA7-JP, P-LTEA7-NA, P-LTEA7-EAL, P-5GS6-R16SA-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.x | P-LTE-450 |
| IR8100 Rugged Series Router | Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1 | IRMH-LTE-MNA, IRMH-LTEA-EA, IRMH-LTEA-LA, IRMH-LTEAP18-GL, IRMH-5GS6-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1 | IRMH-LTE7-NA-900, IRMH-5GR16SA, IRMH-LTE7-EAL |
| IR1800 Rugged Series Router | Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1 | P-LTE-MNA, P-LTE-VZ, P-LTE-US, P-LTE-GB, P-LTE-IN, P-LTE-JN, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL, P-5GS6-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4 | P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.x | P-LTE-450 |
| IR8340 Rugged Series Router | Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1 | P-LTE-MNA, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL P-5GS6-GL |
| | Cisco IOS XE Catalyst SD-WAN Release 17.15.4 Cisco Catalyst SD-WAN Manager 20.15.4 | P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL |
| Cisco ESR 6300 Series | Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1 | P-LTE-MNA, P-LTEA-EA, P-LTEA-LA, P-LTEAP18-GL |

Guidelines

Circuit of last resort

An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit.

- When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.
- Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
- Use the **last-resort-circuit** command to configure a cellular interface to be a circuit of last resort. **last-resort-circuit** is not limited to cellular interfaces. The operating principle for cellular interfaces also applies to GigabitEthernet interfaces.

Active circuit

You can choose to use a cellular interface as an active circuit, perhaps because it is the only last-mile circuit or to always keep the cellular interface active so that you can measure the performance of the circuit. In this scenario the amount of bandwidth utilized to maintain control and data connections over the cellular interface can become a concern. Here are some best practices to minimize bandwidth usage over a cellular interface:

- Increase control packet timers—To minimize control traffic on a cellular interface, you can decrease how often protocol update messages are sent on the interface. OMP sends Update packets every second, by default. You can increase this interval to a maximum of 65535 seconds (about 18 hours) by including the **omp timers advertisement-interval** configuration command. BFD sends Hello packets every second, by default. You can increase this interval to a maximum of 5 minutes (300000 milliseconds) by including the **bfd color hello-interval** configuration command. (Note that you specify the OMP Update packet interval in seconds and the BFD Hello packet interval in milliseconds.)
- Prioritize Cisco SD-WAN Manager control traffic over a non-cellular interface: When a edge device has both cellular and non-cellular transport interfaces, by default, the edge device chooses one of the interfaces to use to exchange control traffic with the Cisco SD-WAN Manager. You can configure the edge device to never use the cellular interface to exchange traffic with the Cisco SD-WAN Manager, or you can configure a lower preference for using the cellular interface for this traffic. You configure the preference by including the **vmanage-connection-preference** command when configuring the tunnel interface. By default, all tunnel interface have a Cisco SD-WAN Manager connection preference value of 5. The value can range from 0 through 8, where a higher value is more preferred. A tunnel with a preference value of 0 can never exchange control traffic with the Cisco SD-WAN Manager.

At least one tunnel interface on the edge device must have a non-0 Cisco SD-WAN Manager connection preference value. Otherwise, the device has no control connections.

Configure cellular interface

A cellular interface is a network interface that enables wireless communication over a cellular network.

Use one of the methods to configure cellular interface.

- [Configure cellular interfaces using a configuration group](#)
- [Configure cellular interfaces using the CLI](#)
- [Configure cellular interfaces using feature templates](#)

Configure cellular interfaces using a configuration group

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, Cisco Catalyst SD-WAN Manager Release 20.16.1

Before you begin

On the **Configuration > Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration > Configuration Groups** .

Step 2 Create and configure a [Transport VPN](#) feature in a Transport & Management profile.

- Configure the basic configuration parameters, such as the VPN.

Table 3: Basic Configuration

| Field | Description |
|---------------------|--|
| VPN | Enter the numeric identifier of the VPN. |
| Enhance ECMP Keying | Enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. Default: Disabled |

- Configure DNS.

Table 4: DNS

| Field | Description |
|------------------------------|--|
| Add DNS | |
| Primary DNS Address (IPv4) | Enter the IP address of the primary IPv4 DNS server in this VPN. |
| Secondary DNS Address (IPv4) | Enter the IP address of a secondary IPv4 DNS server in this VPN. |

| Field | Description |
|-------------------------------------|--|
| Add DNS IPv6 | |
| Primary DNS Address (IPv6) | Enter the IP address of the primary IPv6 DNS server in this VPN. |
| Secondary DNS Address (IPv6) | Enter the IP address of a secondary IPv6 DNS server in this VPN. |

- c. Configure host mapping.

Table 5: Host Mapping

| Field | Description |
|-----------------------------|---|
| Add New Host Mapping | |
| Hostname* | Enter the hostname of the DNS server. The name can be up to 128 characters. |
| List of IP* | Enter up to 14 IP addresses to associate with the hostname. Separate the entries with commas. |

- d. Configure routes.

Table 6: Route

| Field | Description |
|------------------------------|--|
| Add IPv4 Static Route | |
| Network address* | Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN. |
| Subnet Mask* | Enter the subnet mask. |
| Gateway* | Choose one of the following options to configure the next hop to reach the static route: <ul style="list-style-type: none"> • nextHop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv4 address. • Administrative distance*: Enter the administrative distance for the route. • dhcp • null0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • Administrative distance: Enter the administrative distance for the route. |
| Add IPv6 Static Route | |

| Field | Description |
|----------------------------|---|
| Prefix* | Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN. |
| Next Hop/Null 0/NAT | Choose one of the following options to configure the next hop to reach the static route: <ul style="list-style-type: none"> • Next Hop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv6 address. • Administrative distance*: Enter the administrative distance for the route. • Null 0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • IPv6 Route Null 0*: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • NAT: When you choose this option, the following field appears: <ul style="list-style-type: none"> • IPv6 NAT*: Choose NAT64 or NAT66. |
| Add BGP Routing | Choose a BGP route. |

- e. Configure services.

Table 7: Service

| Field | Description |
|---------------------|--|
| Add Service | |
| Service Type | Choose the service available in the VPN. Value: TE |

Step 3

Configure a [Cellular Interface](#) feature to associate with the Transport VPN.

- Adjacent to the Transport VPN feature, click + and add a Cellular Interface feature as a subfeature.
- Configure the basic parameters.

| Field | Description |
|------------------------|--|
| Shutdown* | Enable or disable the interface. |
| Interface Name* | Enter the name of the interface. |
| Description* | Enter a description of the cellular interface. |

| Field | Description |
|--------------------|--|
| DHCP Helper | 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. |

c. Configure the tunnel parameters.

| Field | Description |
|----------------------------|---|
| Tunnel Interface | Enable this option to create a tunnel interface. |
| Carrier | Choose the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default |
| Color | Choose a color for the TLOC. |
| Color Description | Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color. |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 600000 milliseconds Default: 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 6000 seconds Default: 12 seconds |
| Last-Resort Circuit | Enable this option to use the tunnel interface as the circuit of last resort. |
| Restrict | Enable this option to limit the remote TLOCs that the local TLOC can establish BFD sessions with. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color. |
| Group | Enter a group number. Range: 1 through 4294967295 |
| Border | Enable this option to set the TLOC as a border TLOC. |

| Field | Description |
|--------------------------------------|---|
| Maximum Control Connections | Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 100 Default: 2 |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds |
| Validator As Stun Server | Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT. |
| Exclude Controller Group List | Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allowed to connect to. Range: 1 through 100 |
| Manager Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5 |
| Full Port Hop | Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled |
| Port Hop | Enable port hopping. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the Full Port Hop option. See the Full Port Hop field. |
| Low-Bandwidth Link | Enable the low-bandwidth feature. |

| Field | Description |
|----------------------------|---|
| Tunnel TCP MSS | Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None |
| Clear-Dont-Fragment | Enable this option 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 the MTU of the interface are fragmented before being sent. |
| Network Broadcast | Enable this option to accept and respond to network-prefix-directed broadcasts. |
| Allow Service | Allow or disallow the following services on the interface: <ul style="list-style-type: none"> • All • BGP • DHCP • NTP • SSH • DNS • ICMP • HTTPS • OSPF • STUN • SNMP • NETCONF • BFD |
| Encapsulation | |
| GRE | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. 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. |
| GRE Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 |

| Field | Description |
|-------------------------|---|
| GRE Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 |
| IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. 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. |
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 |

d. Configure NAT.

| Field | Description |
|---------------------|--|
| NAT | Enable this option to have the interface act as a NAT device. |
| UDP Timeout* | Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minutes |
| TCP Timeout* | Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour) |

e. Configure ACL/QoS.

f. Configure the advanced parameters.

| Field | Description |
|--------------------|---|
| MAC Address | Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation. |

| Field | Description |
|-----------------------|---|
| IP MTU | Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes |
| Interface MTU | Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes |
| TCP MSS | Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None |
| 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 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. Note TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface. |
| Tracker | 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, Cisco Catalyst SD-WAN periodically probes the path to the internet to determine whether it is up. If Cisco Catalyst SD-WAN 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 Cisco Catalyst SD-WAN detects that the path to the internet is again functioning, the route to the internet is reinstalled. Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |

| Field | Description |
|------------------------------|--|
| IP Directed-Broadcast | <p>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.</p> <p>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.</p> <p>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.</p> |

Step 4 Click **Add New Feature** to create and configure a [Cellular Controller](#) feature.

Configure the basic parameters, mostly related to SIMs.

Table 8: Basic Settings

| Field | Description |
|-----------------------------|---|
| Type | Choose a feature from the drop-down list. |
| Feature Name | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| Description | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |
| Cellular ID | Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0. |
| Primary SIM slot | Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable. |
| SIM Failover Retries | <p>Specify the maximum number of times to retry connecting to the secondary SIM when service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.</p> <p>Range: 0 through 65535</p> <p>Default: 10</p> |
| SIM Failover Timeout | <p>Specify how long to wait before switching from the primary SIM to the secondary SIM if service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.</p> <p>Range: 3 to 7 minutes</p> <p>Default: 3 minutes</p> |

| Field | Description |
|--------------------------|---|
| Firmware Auto Sim | By default, this option is enabled. AutoSIM analyzes any active SIM card and determines which service provider network is associated with that SIM. Based on that analysis, AutoSIM automatically loads the appropriate firmware. |

Step 5 Configure a [Cellular Profile](#) feature to associate with the Cellular Controller.

- a. Adjacent to the Cellular Controller feature, click + and add a Cellular Profile feature as a subfeature.
- b. Configure the basic parameters.

Table 9: Basic Settings

| Field | Description |
|---------------------------------|---|
| Type | Choose a feature from the drop-down list. |
| Feature Name | Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters. |
| Description | Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters. |
| Profile ID | Enter the identification number of the profile to use on the router. Range: 1 through 15 |
| Access Point Name | Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long. |
| Authentication | Choose the authentication method used for the connection to the cellular network. It can be none , pap , chap , or pap_chap . |
| Profile Username | Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces. |
| Profile Password | Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form. |
| Packet Data Network Type | Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6. |
| No Overwrite | Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled. |
| Slot | Enter the associated SIM slot for the profile. |

Step 6 If you need to configure specific cellular bands, do this:

- a) In the **Cellular Controller** area, click + and choose **Cellular Band Select**.
- b) Enable **Cellular Band Select**.
- c) Configure the basic parameters.

Table 10: Cellular Band Select

| Field | Description |
|---|---|
| Name | Specify the name of cellular band select. |
| Description (Optional) | Provide a description for the cellular band select. |
| Enable Cellular Band Select (Optional) | Enable/Disable cellular band. |
| All UMTS 3G only | Enable all UMTS3g bands in the cellular modem. |
| All LTE only | Enable all LTE bands in the cellular modem. |
| LTE 4G | Specify the LTE indices. |
| Indices | Enable/Disable cellular band indices. |
| UMTS 3G | Specify the 3G indices. |
| NR 5G | Specify the 5G SA indices. |
| NR 5G NSA | Specify the 5G NSA indices |

Note

This sub-feature is applicable to both SD-Routing and SD-WAN modes.

What to do next

Also see [Deploy a configuration group](#).

Configure cellular interfaces using CLI

The following example enables a cellular interface:

Procedure

Use the `interface Cellular` command to enable a cellular interface.

Example:

```
interface Cellular0/2/0
  description Cellular interface
  no shutdown
  ip address negotiated
  ip mtu 1428
  mtu 1500
```

```

exit

controller Cellular 0/2/0
lte sim max-retry 1
lte failovertimer 7
profile id 1 apn Broadband authentication none pdn-type ipv4

```

Configure cellular interfaces using templates

To configure cellular interfaces using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Cellular feature template to configure cellular module parameters
2. Create a Cellular Profile template to configure the profiles used by the cellular modem.
3. Create a VPN feature template to configure VPN parameters.

If your deployment includes devices with cellular interface, you must include cellular controller templates in Cisco SD-WAN Manager, even if these templates are not used.

If the device has the LTE or cellular controller module configured and the cellular controller feature template does not exist, then the device tries to remove the cellular controller template. For releases earlier than Cisco IOS XE Release 17.4.2, the following error message is displayed.

```

bad-cli - No controller Cellular 0/2/0, parser-context - No controller Cellular 0/2/0,
parser-response % Cannot remove controllers this way

```

For devices running on Cisco IOS XE Release 17.4.2 and later, the device will return an access-denied error message.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.

Step 2 Click **Feature Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Click **Add Template**.

Step 4 Select the type of device for which you are creating the template.

Step 5 Click **VPN Interface Cellular**.

Step 6 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list.

Step 8 Configure cellular interface.

- a) Configure basic cellular interface functionality.

Table 11:

| Parameter Name | Description |
|----------------------|--|
| Shutdown* | Click No to enable the interface. |
| Interface Name* | Enter the name of the interface. It must be cellular0 . |
| Description | Enter a description of the cellular interface. |
| DHCP Helper | 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. |
| Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through $(2^{32} / 2) - 1$ kbps |
| Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. Range: 1 through $(2^{32} / 2) - 1$ kbps |
| IP MTU* | Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value. |

- b) Configure a tunnel interface on the cellular interface to configure an interface in VPN 0 to be a WAN transport connection. 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. You can generally accept the system defaults for the remainder of the tunnel interface settings.

| Parameter Name | Description |
|---------------------------|---|
| Tunnel Interface* | From the drop-down, select Global . Click On to create a tunnel interface. |
| Per-tunnel QoS | From the drop-down, select Global . Click On to create per-tunnel QoS. You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies. |
| Per-tunnel QoS Aggregator | From the drop-down, select Global . Click On to create per-tunnel QoS. Note 'bandwidth downstream' is required for per-Tunnel QoS feature to take effect as spoke role. |
| Color* | From the drop-down, select Global . Select a color for the TLOC. The color typically used for cellular interface tunnels is lte . |
| Color Description | Minimum supported release: SD-WAN Manager 20.18.1 Enter a description associated to the TLOC color. |
| Groups | From the drop-down, select Global . Enter the list of groups in the field. |
| Border | From the drop-down, select Global . Click On to set TLOC as border TLOC. |

| Parameter Name | Description |
|-------------------------------|---|
| Maximum Control Connections | Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2 |
| vBond As STUN Server | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT. |
| Exclude Control Group List | Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with. Range: 0 through 100 |
| vManage Connection Preference | Set the preference for using the tunnel to exchange control traffic with the Cisco SD-WAN Manager. Range: 0 through 9 Default: 5 If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between the Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager. To have a tunnel interface never connect to the Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference. |
| Full Port Hop | Minimum release: SD-WAN Manager 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled |
| Port Hop | From the drop-down, select Global . Click Off to allow port hopping on tunnel interface. Default: On , which disallows port hopping on tunnel interface. Starting from SD-WAN Manager 20.18.1, this field is deprecated. Instead use the Full Port Hop option. See the Full Port Hop field. |
| Low-Bandwidth Link | Click On to set the tunnel interface as a low-bandwidth link. Default: Off |

| Parameter Name | Description |
|---------------------|--|
| Tunnel TCP MSS | <p>TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU.</p> <p>Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None</p> |
| Clear-Dont-Fragment | <p>Configure Clear-Dont-Fragment for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent.</p> <p>Click On to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.</p> <p>Note Clear-Dont-Fragment clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.</p> |
| Network Broadcast | <p>From the drop-down, select Global. Click On to accept and respond to network-prefix-directed broadcasts. Turn this On only if the Directed Broadcast is enabled on the LAN interface feature template.</p> <p>Default: Off</p> |
| Allow Service | <p>Click On or Off for each service to allow or disallow the service on the cellular interface.</p> |

To configure additional tunnel interface parameters, click **Advanced Options** and configure the following parameters:

Table 12:

| Parameter Name | Description |
|----------------|--|
| GRE | <p>From the drop-down, select Global. Click On to use GRE encapsulation on the tunnel interface. By default, GRE is disabled.</p> <p>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.</p> |
| GRE Preference | <p>From the drop-down, select Global. Enter a value to set GRE preference for TLOC.</p> <p>Range: 0 to 4294967295</p> |

| Parameter Name | Description |
|----------------------|--|
| GRE Weight | From the drop-down, select Global . Enter a value to set GRE weight for TLOC. Default: 1 |
| IPsec | From the drop-down, select Global . Click On to use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. 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. |
| IPsec Preference | From the drop-down, select Global . Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0 |
| IPsec Weight | From the drop-down, select Global . Enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1 |
| Carrier | From the drop-down, select Global . From the Carrier drop-down, select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. The interface name has the format ge slot/port . |
| Last-Resort Circuit | From the drop-down, select Global . Click On to use the tunnel interface as the circuit of last resort. By default, it is disabled. Note An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. |
| NAT Refresh Interval | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds. |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second). |

| Parameter Name | Description |
|-----------------|---|
| Hello Tolerance | <p>Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.</p> <p>Range: 12 through 60 seconds. Default: 12 seconds.</p> <p>The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the no track-transport disable regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the 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 edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.</p> |

- c) Configure the cellular interface as a NAT device.

Table 13:

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

To create a port forwarding rule, click **Add New Port Forwarding Rule** and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 14:

| Parameter Name | Description |
|------------------|---|
| Port Start Range | Enter a port number to define the port or first port in the range of interest. Range: 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. Range: 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. Range: 0 through 65530 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

- d) Configure a shaping rate to a cellular interface and apply a QoS map, a rewrite rule, access lists, and policers to a router interface.

Table 15: Access Lists Parameters

| 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 – IPv4 | Click On , and specify the name of an IPv4 access list to packets being received on the interface. |
| Egress ACL– IPv4 | Click On , and specify the name of an IPv4 access list to packets being transmitted on the interface. |
| Ingress ACL – IPv6 | Click On , and specify the name of an IPv6 access list to packets being received on the interface. |
| Egress ACL– IPv6 | Click On , and specify the name of an IPv6 access list 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. |

- e) Add ARP table entries.

Table 16:

| 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. |

- f) Configure other interface properties.

Table 17: Cellular Interfaces Advanced Parameters

| Parameter Name | Description |
|-----------------------|--|
| 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. |
| TCP MSS | Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: 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. Range: 0 through 7 |
| 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 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. |
| Tracker | Enter the name of a tracker to track the status of transport interfaces that connect to the internet. |
| IP Directed-Broadcast | From the drop-down, select Global . Click On for IP directed-broadcast. Default: Off |

- Step 9** Click **Save**.

Reset the profile configuration of a cellular modem using CLI commands

From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, when you need to switch from one cellular provider to another, you can reset the cellular modem to clear existing profile configurations and apply new settings using the **cellular slot lte profile reset** command.

Resetting the profile configuration of a modem prevents remnants of previous carrier settings (such as Access Point Name (APN) or authentication details) from interfering with new configurations, which is vital for successful network attachment and operation.

Procedure

For routers, use the command with a 3-tuple slot identifier. For cellular gateways, the `slot` variable is 1.

Example:

Routers:

```
CellularGateway# cellular 0/2/0 profile-reset
```

Cellular gateways:

```
CellularGateway# cellular 1 profile-reset
```

Troubleshoot LTE modem crash

In the event that an LTE modem crashes, `crash dump` is the information stored in the device bootflash that:

- makes troubleshooting easier by appearing in the admin-tech file
- helps diagnose the cause of the crash

When enabled, this command instructs the device to automatically collect a crash dump from the LTE modem upon a crash event. This dump contains various diagnostic logs and memory states that are essential for analyzing why the modem crashed.

Before you begin

Ensure that the device has sufficient bootflash storage available to accommodate the large amount of data collected.

Procedure

Use the **lte modem crash-action auto-collect** command to automatically gather and store detailed operational data in the event of an LTE modem crash.

What to do next

Use the following command to verify the crash-dump progress.

```
Device#show cellular 0/2/0 logs modem-crashdump
Modem crashdump logging = off
Device#
```

When a crash-dump is in progress, it is displayed as follows:

```
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = on
Progress = 44%
Router#
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = on
Progress = 98%
Router#show cellular 0/3/0 logs modem-crashdump
Modem crashdump logging = off
```

Once the collection is complete, the status will return to off.

