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 devies with cellular modules to enable LTE connectivity.
Cellular Module Support for Cisco Catalyst Rugged Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Support for cellular modules on Cisco Cisco Catalyst IR1101, IR1800 and IR18340 Rugged Series Routers.

Cellular Interfaces

To enable LTE connectivity, configure cellular interfaces on a router that has a cellular module. The cellular module provides wireless connectivity over a service provider's cellular network. One use case is to provide wireless connectivity for branch offices.

A cellular network is commonly used as a backup WAN link, to provide network connectivity if all the wired WAN tunnel interfaces on the router become 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.

When you configure a cellular interface on a device, you can connect the device to the Internet or another WAN by plugging in the power cable of the device. The device then automatically begins the process of joining the overlay network, by contacting and authenticating with Cisco Catalyst SD-WAN Validators, Cisco Catalyst SD-WAN Controllers, and Cisco SD-WAN Manager systems.

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 17.13.1a	P-LTEA7-JP, P-LTEA7-NA, P-LTEA7-EAL, P-5GS6-R16SA-GL
IR18xx Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	P-LTEA7-JP, P-LTEA7-NA, P-LTEA7-EAL
IR1800 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL
IR8340 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL
IR1101 Rugged Series Router	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	P-LTEA7-NA, P-LTEA7-JP, P-LTEA7-EAL, P-5GS6-R16SA-GL

Configure Cellular Interfaces Using Cisco SD-WAN Manager

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

1. Create a VPN Interface Cellular feature template to configure cellular module parameters, as described in this section.

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.

Note 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.

Create VPN Interface Cellular

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

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

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional Cisco VPN 0 Templates**, click **VPN Interface Cellular**.
7. From the **VPN Interface Cellular** drop-down list, click **Create Template**. The VPN Interface Cellular template form is displayed.

   This form contains fields for naming the template, and fields for defining the VPN Interface Cellular parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. 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.

Configure Basic Cellular Interface Functionality

To configure basic cellular interface functionality, click **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface. You must also configure a tunnel interface for the cellular interface.

Table 3:

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.

To save the feature template, click **Save**.

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 reminder of the tunnel interface settings.

To configure a tunnel interface, click **Tunnel**, and configure the following parameters. Parameters marked with an asterisk (*) are required to configure a cellular interface.

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 Aggregrator	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**.
Groups	From the drop-down, select **Global**. Enter the list of groups in the field.

Parameter Name	Description
Border	From the drop-down, select **Global**. Click **On** to set TLOC as border TLOC.
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.
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.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**

Parameter Name	Description
Tunnel TCP MSS	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. 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
Clear-Dont-Fragment	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. 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. **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.
Network Broadcast	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. Default: **Off**
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** and configure the following parameters:

Table 4:

Parameter Name	Description
GRE	From the drop-down, select **Global**. Click **On** to 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.

Parameter Name	Description
GRE Preference	From the drop-down, select **Global**. Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295
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.

Parameter Name	Description
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).
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 60 seconds. Default: 12 seconds. 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.

To save the feature template, click **Save**.

Configure the Cellular Interface as a NAT Device

To configure a cellular interface to act as a NAT device for applications such as port forwarding, click **NAT**, and configure the following parameters:

Table 5:

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

Parameter Name	Description
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 6:

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.

To save a port forwarding rule, click **Add**.

To save the feature template, click **Save**.

Apply Access Lists

To configure a shaping rate to a cellular interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, click **ACL/QoS** and configure the following parameters:

Table 7: Access Lists Parameters

Parameter Name	Description
Shaping rate	Configure the aggreate 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.

Parameter Name	Description
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.

To save the feature template, click **Save**.

Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, click **ARP**. Then click **Add New ARP** and configure the following parameters:

Table 8:

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 save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

Configure Other Interface Properties

To configure other interface properties, click **Advanced** and configure the following parameters.

Table 9: 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 TPC 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.

Parameter Name	Description
Clear-Dont-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**

To save the feature template, click **Save**.

Configure Cellular Interfaces Using Configuration Groups

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Create Configuration Groups** or edit an existing configuration group.
3. In the **Transport & Management Profile** menu, create a new profile.
4. Click the **Transport VPN** menu and choose an existing Transport VPN feature or create a new one.
5. Click + and choose **Cellular Interface** to add a new cellular interface. Cisco SD-WAN Manager adds it as a subfeature.
6.
7. In the **Cellular Interface** menu, choose an existing Cellular Interface feature or create a new one.
8. Click **Add New Feature** and choose **Cellular Controller**.
9. In the **Cellular Controller** menu, choose an existing Cellular Controller feature or create a new one.
10. Configure the fields for Cellular Controller. See Cellular Controller.
11. In the **Cellular Controller** area, click + and choose **Cellular Profile**.
12. Configure the fields for Cellular Profile. See Cellular Profile.

Configure Cellular Interfaces Using CLI

The following example enables a cellular interface:

```
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
```

Data Profile

Table 10: Feature History

Feature Name	Release Information	Description
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.

A data profile for a cellular device defines the following parameters, which the device uses for communication with the service provider. You can configure the following parameters by using the **profile id** command in cellular configuration mode. For more information about the following parameters, see profile id.

- Identification number of the data profile
- Name of the access point network of the service provider
- Authentication type used for APN access: No authentication, CHAP authentication only, PAP authentication only, or either CHAP or PAP authentication
- Username and password that are provided by the service provider for APN access authentication, if authentication is used
- Type of packet data matching that is used for APN access: IPv4 type bearer, IPv6 type bearer, or IPv4v6 type bearer
- SIM slot that contains the SIM to configure

Best Practices for Configuring Cellular Interfaces

Cellular technology on edge devices can be used in a number of ways:

- 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.

- 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:

  - When a device with cellular interface is deployed as a spoke, and data tunnels are established in a hub-and-spoke manner, you can configure the cellular interface as a low-bandwidth interface. To do this, include the **low-bandwidth-link** command when you configure the cellular interface's tunnel interface. When the cellular interface is operating as a low-bandwidth interface, the device spoke site is able to synchronize all outgoing control packets. The spoke site can also proactively ensure that no control traffic, except for routing updates, is generated from one of the remote hub nodes. Routing updates continue to be sent, because they are considered to be critical updates.

  - 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-celluar 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.

Note 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.