DSL PPPoA

- Configure DSL PPPoA, on page 1

Configure DSL PPPoA

Use one of these methods to configure DSL PPPoA:

- Configuration group
- Feature template

Configure DSL PPPoA using a configuration group

Follow these steps to configure DSL PPPoA using a configuration group.

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 the DSL PPPoA parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 1: Basic Configuration

Parameter Name	Description
Controller Slot*	Enter the slot number of the DSL controller, in the following format: *slot*/*subslot*/*port* (for example, 0/2/0)

Parameter Name	Description
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.
Dialer Pool Member*	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b. Configure ATM.

Table 2: ATM

Parameter Name	Description
ATM Sub Interface Name*	The ATM Sub interface name is auto populated based on the controller slot. Enter a value for the ATM sub interface, in the format *subslot/port* (for example ATM0/2/0.100). In this example, ".100" is the sub interface value.
Sub Interface Description	Enter a description for the interface.
VPI/VCI*	Create an ATM permanent virtual circuit (PVC), in the following format: *vpi/vci* Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).
Encapsulation	Select the encapsulation type to use on the ATM PVC from the drop-down list: • AAL5 NLPID: Use NLPID multiplexing. • AAL5 SNAP: Multiplex two or more protocols on the same PVC. • AAL5 MUX: Dedicate the PVC to a single protocol.
PVC Mode	

Parameter Name	Description
VBR-NRT	Configure variable bit rate non-real-time parameters: • Peak Cell Rate: Enter a value from 48 through 1015 Kbps. • Sustainable Cell Rate: Enter the sustainable cell rate, in Kbps. • Maximum Burst Size: This size can be 1 through 65535.
VBR-RT	Configure variable bit rate real-time parameters: • Peak Cell Rate: Enter a value from 48 through 25000 Kbps. • Average Cell Rate: Enter the average cell rate, in Kpbs. • Maximum Burst Size: This size can be 1 through 65535.
None	Don't configure variable bit rate parameters

c. Configure PPP.

Table 3: PPP

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the MLP: • **PAP**: Enter the username and password that are provided by your ISP. *username* can be up to 254 characters. • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol.
Authentication Type	Select the type authentication from one of the following options.: • **Unidirectional**: Only the side receiving the call (NAS) authenticates the remote side (client). The remote client does not authenticate the server. • **Bidirectional**: Each side independently sends an Authenticate-Request (AUTH-REQ) and receives either an Authenticate-Acknowledge (AUTH-ACK) or Authenticate-Not Acknowledged (AUTH-NAK).
CHAP Hostname*	Enter the CHAP hostname.
CHAP Password*	Enter the CHAP password.
PAP Hostname*	Enter the PAP hostname.
PAP Password*	Enter the PAP password.

d. Configure Tunnel.

Table 4: Tunnel

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub** If you select hub topology, the following option appears: • **Bandwidth Percentage**: Enter a value for the bandwidth percentage. Default: 50
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.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
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 8 Default: 2
Cisco SD-WAN 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
Tunnel TCP MSS	TCP MSS affects any packet containing 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. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. 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

Parameter Name	Description
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator 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.
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	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on a tunnel interface 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	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
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, the router fragments packets larger than the MTU of the interface before sending the packets. the router fragments packets larger than the MTU of the interface before sending the packets. **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 list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global** and 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 following format: **ge** *slot*/*port*

Parameter Name	Description
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)
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.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, 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, 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. If the primary interfaces lose their connections to remote edges, 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 a 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.
Allow Services	Click **On** or **Off** for each service to anable or disable the service on the cellular interface.

Parameter Name	Description
Encapsulation	
Encapsulation	Enable at least one of the following encapsulation methods: • **IPsec**: 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 Preference**: From the drop-down list, select **Global** and 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 list, select **Global** and 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 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and 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 • **GRE Weight**: From the drop-down list, select **Global** and 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

e. Configure NAT.

Table 5: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

f. Configure QoS.

Table 6: QoS

Parameter Name	Description
Adaptive QoS	Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values. • **Adapt Period (Minutes)**: Choose **Global** from the drop-down list, click **On**, and enter the period in minutes. • **Shaping Rate Upstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps. • **Shaping Rate Downstream**: Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
Shaping Rate (kbps)	Choose **Global** from the drop-down list and configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps). Range: 8 through 100000000

g. Configure ACL.

Table 7: ACL

Parameter Name	Description
IPv4 Ingress Access List	Enter the name of an IPv4 access list to packets being received on the interface.
IPv4 Egress Access List	Enter the name of an IPv4 access list to packets being transmitted on the interface.
IPv6 Ingress Access List	Enter the name of an IPv6 access list to packets being received on the interface.
IPv6 Egress Access List	Enter the name of an IPv6 access list to packets being transmitted on the interface.

h. Configure advanced parameters.

Table 8: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter 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 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. 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.

What to do next

Also see Deploy a configuration group.

Configure DSL PPPoA using templates

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters.
2. Create a VPN feature template to configure VPN parameters.

Follow these steps to configure DSL PPPoA using a feature template.

To provide support for service provider digital subscriber line (DSL) functionality, configure PPP-over-ATM interfaces on routers with DSL NIM modules.

Use the VPN Interface DSL PPPoA template for Cisco IOS XE Catalyst SD-WAN devices.

You configure PPP-over-ATM interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

Procedure

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

Step 2 Click **Device Templates**.

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

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoA**.
d) From the **VPN Interface DSL PPPoA** drop-down list, click **Create Template**. The VPN Interface DSL PPPoA template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface PPP parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure basic VDSL controller functionality in a VPN.

Table 9:

Parameter Name	Description
Shutdown*	Click **No** to enable the VDSL controller interface.
Controller VDSL Slot*	Enter the slot number of the controller VDSL interface, in the format *slot*/*subslot*/*port* (for example, 0/2/0).

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • **Auto**—Default mode. • **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager. If the command is not valid, it is not executed.
SRA	Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

Step 5 Configure an ATM interface on the VDSL controller.

Table 10:

Parameter Name	Description
ATM Interface Name	Enter a name for the ATM interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
Description	Enter a description for the interface.
VPI and VCI	Create an ATM permanent virtual circuit (PVC), in the format *vpi*/*vci*, Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).
Encapsulation	Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down list: • AAL5 MUX—Dedicate the PVC to a single protocol. • AAL5 NLPID—Use NLPID multiplexing. • AAL5 SNAP—Multiplex two or more protocols on the same PVC.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.

Parameter Name	Description
VBR-NRT	Configure variable bit rate non-real-time parameters: • Peak Cell Rate—Enter a value from 48 through 25000 Kbps. • Sustainable Cell Rate—Enter the sustainable cell rate, in Kbps. • Maximum Burst Size—This size can be 1 cell.
VBR-RT	Configure variable bit rate real-time parameters: • Peak Cell Rate—Enter a value from 48 through 25000 Kbps. • Average Cell Rate—Enter the average cell rate, in Kpbs. • Maximum Burst Size—This size can be 1 cell.

Step 6 Configure the PPP authentication protocol.

Table 11:

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: • **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

Step 7 Configure a tunnel interface for the multilink interface.

Table 12:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select 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.

Parameter Name	Description
Control Connection	If the Cisco IOS XE Catalyst SD-WAN device 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. **Note** For control connection traffic without dropping any data, a minimum of 650-700 kbps bandwidth is recommended with default parameters configured for hello-interval (10) and hello-tolerance (12).
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 8 Default: 2
Cisco SD-WAN Validator 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 Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 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	Click **On** to enable port hopping, or click Off to disable it. 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 Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.

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.
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** and configure the following parameters:

Table 13:

Parameter Name	Description
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.
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

Parameter Name	Description
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
Carrier	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.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **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	Enter 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).
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.

Step 8 Apply a rewrite rule, access lists, and policers to a router interface.

Table 14:

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

Step 9 Configure other interface properties.

Table 15:

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 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	Click **On** to clear the Don't Fragment 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.

Parameter Name	Description
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 Cisco IOS XE Catalyst SD-WAN device 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.