

Transport and Management

The Transport and Management Profile helps you configure a VRF at WAN level. For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

- Information about the Transport and Management profile, on page 2
- ACL IPv4, on page 2
- ACL IPv6 , on page 4
- BGP Routing, on page 5
- Cellular Controller, on page 14
- Cellular Band Select, on page 15
- Cellular Profile, on page 16
- Ethernet Interface, on page 17
- GPS, on page 27
- GRE, on page 28
- IPSEC, on page 32
- IPv6 Tracker, on page 37
- IPv6 Tracker Group, on page 38
- Managed Cellular Activation - eSIM Controller, on page 39
- Management VPN, on page 39
- OSPF Routing, on page 42
- OSPFv3 IPv4 Routing, on page 47
- OSPFv3 IPv6 Routing, on page 50
- Raw socket without VRF, on page 54
- Route Policy, on page 55
- T1/E1 Controller, on page 56
- Tracker, on page 58
- Tracker Group, on page 60
- Transport VPN, on page 60
- VPN Interface Multilink , on page 63
- Ethernet PPPoE, on page 69
- Cellular Interface, on page 76

Information about the Transport and Management profile

This section describes the features available in the Transport and Management profile.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

ACL IPv4

See Configure ACLs Using a Configuration Group.

1. In the **Add Feature** window, choose **ACL IPv4** from the drop-down list.
2. Enter the **Feature Name** and the **Description** for the ACL feature.
3. Click **Add ACL Sequence**. The **Add ACL Sequence** window appears.
4. Enter the name in the **ACL Sequence Name** field.
5. Select the required condition from the **Condition** drop-down list.
6. Select the action types **Accept** or **Reject** from the **Action Type** drop-down list.
7. For the **Accept** action type, choose the accept condition from the **Accept Condition** drop-down list.
8. Click **Save**.

   To copy, delete, or rename the ACL policy sequence rule, click **...** next to the rule's name and select the desired option.
9. If no packets match any of the ACL policy sequence rules, the default action is to drop the packets. To change the default action:
   a. Click **Default Action** in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to **Accept**.
   d. Click **Save**.
10. Click **Save ACL IPv4 Policy**.

The following table describe the options for configuring the ACL IPv4 feature.

Table 1: ACL IPv4

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.

Field	Description
Condition	Specifies the ACL condition. The options are: • DSCP • Packet Length • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • ICMP Message (Only in Cisco Catalyst SD-WAN Manager Release 20.15.1)
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • DSCP • Log • Next Hop • Service Chain • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile configuration groups.

Traffic Class action in IPv4 ACL

Configuring traffic class is not supported in ACL IPv4 feature under configuration groups. This change was introduced because forwarding class is part of QoS configuration, which is managed through policy groups. To provide a consistent configuration workflow, the traffic class action was removed from configuration group ACLs.

If you still require ACL-based traffic class configuration, you can configure it by using CLI add-on feature.

To configure traffic class, refer to Configure QoS policy under policy groups.

ACL IPv6

See Configure ACLs Using a Configuration Group.

1. In the **Add Feature** window, choose **ACL IPv6** from the drop-down list.
2. Enter the **Feature Name** and the **Description** for the ACL feature.
3. Click **Add ACL Sequence**. The **Add ACL Sequence** window appears.
4. Enter the name in the **ACL Sequence Name** field.
5. Select the required condition from the **Condition** drop-down list.
6. Select the action types **Accept** or **Reject** from the **Action Type** drop-down list.
7. For the **Accept** action type, choose the accept condition from the **Accept Condition** drop-down list.
8. Click **Save**.

   To copy, delete, or rename the ACL policy sequence rule, click **...** next to the rule's name and select the desired option.
9. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
   a. Click **Default Action** in the left pane.
   b. Click the Pencil icon.
   c. Change the default action to **Accept**.
   d. Click **Save**.
10. Click **Save ACL IPv6 Policy**.

The following table describe the options for configuring the ACL IPv6 feature.

Table 2: ACL IPv6

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.

Field	Description
Condition	Specifies the ACL condition. The options are: • Next Header • Packet Length • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Traffic Class • ICMP Message (Only in Cisco Catalyst SD-WAN Manager Release 20.15.1)
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: • Counter • Log • Next Hop • Traffic Class • Service Chain • Policer

You can select the specific ACL sequence in the ACL Policy window to edit, delete or add.

Note You can also configure **ACL Policy** features from Transport and Service Profile configuration groups.

BGP Routing

See Configure BGP Routing in a Transport Profile Using a Configuration Group.

This feature helps you configure the Border Gateway Protocol (BGP) routing in VPN 0 or the WAN VPN.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

Basic Configuration

Table 3: Basic Configuration

Field	Description
AS Number	Enter the local AS number.
Router ID	Enter the BGP router ID, in decimal four-part dotted notation.
Propagate AS Path	Enable this option to carry BGP AS path information into OMP.
Propagate Community	Enable this option to propagate BGP communities between Cisco Catalyst SD-WAN sites, across VPNs using OMP redistribution.
External Routes Distance	Specify the BGP route administrative distance for routes learned from other sites in the overlay network. Range: 1 through 255 Default: 20
Internal Routes Distance	Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 1 through 255 Default: 200
Local Routes Distance	Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP. Range: 1 through 255 Default: 20

Unicast Address Family

Table 4: Unicast Address Family

Field	Description
IPv4 Settings	
Maximum Paths	Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing. Range: 0 to 32
Originate	Enable this option to allow the default route to be artificially generated and injected into the BGP Route Information Base (RIB), regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers.
Redistribute	

Field	Description
Protocol*	Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, **eigrp**, and **nat**. At a minimum, choose **connected**, and then under **Route Policy**, specify a route policy that has BGP advertise the loopback interface address to its neighbors. Route policy is not supported in Cisco vManage Release 20.9.1.
Route Policy	Enter the name of the route policy to apply to redistributed routes. Route policy is not supported in Cisco vManage Release 20.9.1.
Network	
Network Prefix*	Enter a network prefix to be advertised by BGP. The network prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0.
Aggregate Address	
Aggregate Prefix*	Enter the prefix of the addresses to aggregate for all BGP sessions. The aggregate prefix is composed of the IPv4 subnet and the mask. For example, 192.0.2.0 and 255.255.255.0.
AS Set Path	Enable this option to generate set path information for the aggregated prefixes.
Summary Only	Enable this option to filter out more specific routes from BGP updates.
Table Map	
Policy Name	Enter the route map that controls the downloading of routes. Route policy is not supported in Cisco vManage Release 20.9.1.
Filter	When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map. When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
IPv6 Settings	
Maximum Paths	Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing. Range: 0 to 32

Field	Description
Originate	Enable this option to allow the default route to be artificially generated and injected into the BGP Route Information Base (RIB), regardless of whether it is present in the routing table. The newly injected default is advertised to all the BGP peers.
Redistribute	
Protocol*	Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are **static**, **connected**, **ospf**, **omp**, and **eigrp**. At a minimum, choose **connected**, and then under **Route Policy**, specify a route policy that has BGP advertise the loopback interface address to its neighbors. Route policy is not supported in Cisco vManage Release 20.9.1.
Route Policy	Enter the name of the route policy to apply to redistributed routes. Route policy is not supported in Cisco vManage Release 20.9.1.
Network	
Network Prefix*	Enter a network prefix to be advertised by BGP. The IPv6 network prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64.
Aggregate Address	
Aggregate Prefix*	Enter the prefix of the addresses to aggregate for all BGP sessions. The IPv6 aggregate prefix is composed of the IPv6 address and the prefix length (1-128). For example, the IPv6 subnet is 2001:DB8:0000:0000:: and the prefix length is 64.
AS Set Path	Enable this option to generate set path information for the aggregated prefixes.
Summary Only	Enable this option to filter out more specific routes from BGP updates.
Table Map	
Policy Name	Enter the route map that controls the downloading of routes. Route policy is not supported in Cisco vManage Release 20.9.1.
Filter	When you enable this option, the route map specified in the **Policy Name** field controls whether a BGP route is to be downloaded to the Route Information Base (RIB). A BGP route is not downloaded to the RIB if it is denied by the route map. When you disable this option, the route map specified in the **Policy Name** field is used to set certain properties, such as the traffic index, of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.

MPLS Interface

Table 5: MPLS Interface

Field	Description
Interface Name*	Enter a name for the MPLS interface.

Neighbor

Table 6: Neighbor

Field	Description
IPv4 Settings	
Address*	Specify the IP address of the BGP neighbor.
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Interface Name	Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface.
Allows in Number	Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used.
AS Override	Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router.
Shutdown	Disable this option to enable BGP for the VPN.
Advanced Options	
Next-Hop Self	Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor.
Send Community	Enable this option to send the BGP community attribute of the local router to the BGP neighbor.
Send Extended Community	Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor.
EBGP Multihop	Set the time to live (TTL) for BGP connections to external peers. Range: 1 to 255 Default: 1

Field	Description
Password	Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number.
Keepalive Time (seconds)	Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)
Hold Time (seconds)	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive time)
Send Label	Enable this option to allow the routers advertise to each other so that they can send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all the outgoing BGP updates.
Add Neighbor Address Family	
Family Type*	Choose the BGP IPv4 unicast address family.
In Route Policy	Specify the name of a route policy to apply to prefixes received from the neighbor. Route policy is not supported in Cisco vManage Release 20.9.1.
Out Route Policy	Specify the name of a route policy to apply to prefixes sent to the neighbor. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes. • **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down.
IPv6 Settings	
Address*	Specify the IP address of the BGP neighbor.
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Interface Name	Enter the interface name. This interface is used as the source of the TCP session when establishing neighborship. We recommend that you use a loopback interface.
Allowas in Number	Enter the number of times to allow the advertisement of the autonomous system number (ASN) of a provider edge (PE) device. The range is 1 to 10. If no number is specified, the default value of three times is used.
AS Override	Enable this option to replace the AS number of the originating router with the AS number of the sending BGP router.
Shutdown	Disable this option to enable BGP for the VPN.

Field	Description
Advanced Options	
Next-Hop Self	Enable this option to configure the router to be the next hop for routes advertised to the BGP neighbor.
Send Community	Enable this option to send the BGP community attribute of the local router to the BGP neighbor.
Send Extended Community	Enable this option to send the BGP extended community attribute of the local router to the BGP neighbor.
EBGP Multihop	Set the time to live (TTL) for BGP connections to external peers. Range: 1 to 255 Default: 1
Password	Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number.
Keepalive Time (seconds)	Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. Specify the keepalive time for the neighbor, to override the global keepalive time. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)
Hold Time (seconds)	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor, to override the global hold time. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive time)
Add IPv6 Neighbor Address Family	
Family Type*	Choose the BGP IPv6 unicast address family.
In Route Policy	Specify the name of a route policy to apply to prefixes received from the neighbor. Route policy is not supported in Cisco vManage Release 20.9.1.
Out Route Policy	Specify the name of a route policy to apply to prefixes sent to the neighbor. Route policy is not supported in Cisco vManage Release 20.9.1.

Field	Description
Maximum Prefix Reach Policy*	Choose one of the following options: • **Policy Off**: Policy is off. • **Policy On - Restart**: Configure the time interval at which a peering session is re-established by a device when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. When you choose this option, the following fields appear: • **Maximum Number of Prefixes***: Enter the maximum prefix limit. Range: 1 to 4294967295 • **Threshold (percentage)**: Enter the threshold value: Range: 1 to 100 Default: 75 • **Restart Interval (minutes)***: Enter the time interval. Range: 1 to 65535 minutes • **Policy On - Warning message**: Configure the device to disable the restart capability to allow you to adjust a peer that is sending too many prefixes. • **Policy On - Disable Peer Neighbor**: When the device receives too many prefixes from a peer, and the maximum prefix limit is exceeded, the peering session is disabled or brought down.

Advanced

Table 7: Advanced

Field	Description
Keepalive (seconds)	Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. This keepalive time is the global keepalive time. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)

Field	Description
Hold Time (seconds)	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. This hold time is the global hold time. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive time)
Compare MED	Enable this option to compare the router IDs among BGP paths to determine the active path.
Deterministic MED	Enable this option to compare MEDs from all routes received from the same AS regardless of when the route was received.
Missing MED as Worst	Enable this option to consider a path as the worst path if the path is missing a MED attribute.
Compare Router ID	Enable this option to always compare MEDs regardless of whether the peer ASs of the compared routes are the same.
Multipath Relax	Enable this option to have the BGP best-path process select from routes in different ASs. By default, when you are using BGP multipath, the BGP best-path process selects from routes in the same AS to load-balance across multiple paths.

Cellular Controller

This feature helps you configure a cellular controller in VPN 0 or the WAN VPN.

Configuring a cellular interface requires configuring the Cellular Controller feature and configuring a Cellular Profile feature. When both are configured, associate a cellular profile with a cellular controller. See Configure cellular interfaces using a configuration group.

The following table describes the options for configuring the Cellular Controller feature.

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.

Field	Description
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	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. Range: 0 through 65535 Default: 10
SIM Failover Timeout	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. Range: 3 to 7 minutes Default: 3 minutes
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.

Cellular Band Select

Add a new **Cellular Band**.

After enabling cellular band select, you can configure either **All UMTS 3G only** or **All LTE only**.

Table 9: 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.

Field	Description
NR 5G NSA	Specify the 5G NSA indices

Cellular Profile

This feature helps you configure a cellular profile in VPN 0 or the WAN VPN.

The following table describes the options for configuring the Cellular Profile feature.

Basic Settings

Table 10: 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.

Ethernet Interface

This feature helps you configure Ethernet interface in VPN 0 or the WAN VPN.

The following table describes the options for configuring the Ethernet Interface feature.

Field	Description
Type	Choose a feature from the drop-down list.
Associated VPN	Choose a VPN.
Associated Tracker/Trackergroup	Choose a tracker or tracker group.
Associated IPv6-Tracker/IPv6-Trackergroup	Choose an IPv6- tracker or tracker group.

Basic Configuration

Field	Description
Shutdown	Enable or disable the interface.
Interface Name*	Enter a name for the interface. Spell out the interface names completely (for example, GigabitEthernet0/0/0). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.
Description	Enter a description for the interface.
Auto Detect Bandwidth	Enable this option to automatically detect the bandwidth for WAN interfaces. The device detects the bandwidth by contacting an iPerf3 server to perform a speed test.
IPv4 Settings	Configure an IPv4 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change.
Dynamic DHCP Distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IP Address	Enter a static IPv4 address. This option is available when you choose **Static**.

Field	Description
Subnet Mask	Enter the subnet mask. From Cisco Catalyst SD-WAN Control Components Release 20.15.1, if you enter a variable in the IP Address field, this field automatically uses a variable.
Configure Secondary IP Address	Enter up to four secondary IPv4 addresses for a service-side interface. • **IP Address**: Enter the IP address. • **Subnet Mask:** Enter the subnet mask.
DHCP Helper	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers.
IPv6 Settings	Configure an IPv6 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change. • **None**
IPv6 Address Primary	Enter a static IPv6 address. This option is available when you choose **Static**.
Add Secondary Ipv6	
IP Address	Enter up to two secondary IPv6 addresses for a service-side interface.
Bandwidth Upstream	Enter upstream bandwidth reference value.
Bandwidth Downstream	Enter downstream bandwidth reference value.

Ether Channel

Field	Description
Port Channel	Enable this option to configure a EtherChannel as a port channel.
Member Interface	Enable this option to configure a EtherChannel as a member-link interface.
Port Channel Mode	To designate a specific mode to the port channel.
QoS Aggregate	Enable this option to configure aggregate EtherChannel Quality of Service to a port channel's main interface.

ACL/Qos

Field	Description
Adaptive QoS	To enable or disable adaptive QoS on an ethernet interface on the transport side.
Shaping Rate	Enter the shaping rate to control the maximum rate of traffic sent.
ACL	To define IPv4 and IPv6 ACL as ingress and egress.

Tunnel

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
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.
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.
Groups	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.
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
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

Field	Description
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. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). 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 this option to characterize the tunnel interface as a low-bandwidth link.
Tunnel 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: 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.
CTS SGT Propagation	Enable CTS SGT propagation on an interface.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.

Field	Description
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
Encapsulation	

Field	Description
Encapsulation*	Choose an encapsulation type: • **gre**: Use GRE encapsulation on the tunnel interface. • **ipsec**: Use IPsec encapsulation on the tunnel interface. **Note** 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. When you choose **gre**, the following fields appear: • **GRE Preference**: Enter a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **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 When you choose **ipsec**, the following fields appear: • **IPSEC Preference**: Enter 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
Multi-Region Fabric **Note** These options appear only when Multi-Region Fabric is enabled.	

Field	Description
Connect to Core Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the access region and core region. • **Keep Exclusive to Core Region**: Use the interface only for the core region.
Connect to Secondary Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to an edge router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the primary and secondary regions. • **Keep Exclusive to Secondary Region**: Use the interface only for the secondary region.

NAT

Field	Description
IPv4 Settings	
NAT	Enable this option to have the interface act as a NAT device.
NAT Type	Choose the NAT translation type for IPv4: • **interface** • **pool** • **loopback** Default: **interface**. It is supported for NAT64.
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 8947 minutes Default: 1 minute
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 8947 minutes Default: 60 minutes (1 hour)

Field	Description

Add Multiple NAT	Choose the NAT type:
	• **Interface**: This is the default value.
	• **Pool**: Configure the following:
	  • **Pool ID**: Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
	  • **Range Start**: Enter a starting IP address for the NAT pool.
	  • **Range End**: Enter a closing IP address for the NAT pool.
	  • **Prefix length**: Specify the maximum number of source IP addresses that can be NATed in the NAT pool.
	  • **Overload**: Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
	  Default: Disabled
	• **Loopback**: Provide a value for the NAT inside source loopback interface.

Configure New Static NAT	Add a static NAT mapping
Source IP	Enter the source IP address to be translated.
Translate IP	Enter the translated source IP address.
Direction	Choose the direction in which to perform network address translation. • **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router. • **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device.
Source VPN	Enter the source VPN ID.
IPv6 Settings	
IPv6 NAT	Enable this option to have the interface act as a NAT device.

Field	Description
Select NAT	Choose NAT64 or NAT66. When you choose NAT66, the following fields appear: • **Source Prefix**: Enter the source IPv6 prefix. • **Translated Source Prefix**: Enter the translated source prefix. • **Source VPN ID**: Enter the source VPN ID. • **Egress Interface**: Enable this option to have the interface act as an egress interface.

ARP

Field	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.

Advanced

Field	Description
Duplex	Specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. 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 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet) Default: 1500 bytes
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: 500 to 1460 bytes Default: None

Field	Description
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, 1000, 2500, or 10000 Mbps
ARP Timeout	ARP timeout controls how long we maintain the ARP cache on a router. Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2147483 seconds Default: 1200 seconds
Autonegotiate	Enable this option to turn on autonegotiation.
Media Type	Specify the physical media connection type on the interface. Choose one of the following: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media.
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.
GRE tunnel source IP	Enter the IP address of the extended WAN interface.
XConnect	Enter the name of a physical interface on the same router that connects to the WAN transport.
Load Interval	Enter an interval value for interface load calculation.

Field	Description
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. 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. 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.
ICMP Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

GPS

Use the GPS feature to detect the device location and to monitor GPS coordinates of Cisco IOS XE Catalyst SD-WAN devices.

The following tables describe the options for configuring the GPS feature.

Table 11: GPS

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 2,048 characters and can contain only alphanumeric characters.
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**: Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor. • **Standalone**: Use satellite information when determining position.

Field	Description
NMEA	Click **On** to enable the use of NMEA streams to help with determining position. NMEA streams data from the router's cellular module to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address*	Enter the IP address of the router's interface that connects to the external device reading the NMEA.
Destination Address*	Enter the IP address of the external device's interface that's connected to router.
Destination Port*	Enter the number of the port to use to send NMEA data to the external device's interface.

GRE

Use the GRE feature for all Cisco IOS XE Catalyst SD-WAN devices.

See Configure VPN interface GRE on transport VPN using a configuration group

The following tables describe the options for configuring the GRE feature.

Basic Configuration

Table 12: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface. Range: 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

Tunnel

Table 13: Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

IKE

Table 14: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1

Field	Description
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

IPSEC

Table 15: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds

Field	Description
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

Advanced

Table 16: Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.

Field	Description
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Based on your choice in the **Tunnel Mode** option, 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 through 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.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

IPSEC

Use the IPsec feature to configure IPsec tunnels on Cisco IOS XE Catalyst SD-WAN devices that are being used for Internet Key Exchange (IKE) sessions.

See Configure IPSEC on Transport Side Using a Configuration Group

Edge devices using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier

If...

- you are running SD-WAN Manager releases from SD-WAN Manager 20.15.1 to SD-WAN Manager 20.15.3, and
- you are using the IPSEC feature to configure an edge device using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier,

then you must also configure a command using a CLI add-on profile. This command provides backward compatibility for edge devices using Cisco IOS XE Catalyst SD-WAN Release 17.12.x or earlier. Without this, the tunnel does not operate correctly.

To do this, create the CLI add-on profile and add it to the configuration group that you are using the configure the device. In the profile, include the **tunnel mode ipsec ipv4-old** command.

Using the CLI add-on profile with the **tunnel mode ipsec ipv4-old** command is not necessary in these releases:

- SD-WAN Manager 20.15.4 and later releases of 20.15.x
- SD-WAN Manager 20.18.1 and later releases

Parameter scope

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the following table:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.
Device Specific (Indicated by a host icon)	Use a device-specific value for the parameter. Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the field. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Default (indicated by a check mark)	The default value appears for parameters that have a default setting.

The following tables describe the options for configuring the VPN Interface IPsec feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Basic Configuration

Table 17: Basic Configuration

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.
Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **ipv4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. IPv4 underlay is the default value. • **ipv6**: IPsec tunnel with IPv6 overlay and IPv6 underlay. • **ipv4-v6overlay**: IPsec tunnel with IPv6 overlay and IPv4 underlay.

Field	Description
Multiplexing	Choose **Yes** to enable multiplexing, if there is a tunnel in the transport VPN. Default: No
Interface Address	Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.
Mask	Enter the subnet mask.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.
Associated Tracker / Tracker Group	Choose a tracker or a tracker group from the drop-down list to associate with the IPsec tunnel.
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the source IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address that is based on your selection in the **Tunnel Mode** option. This address is on the local router. • **Interface**: Enter the physical interface in the **IPsec Source Interface** field, which is the source of the IPsec tunnel.

Tunnel Destination	Enter the destination IP address of the IPsec tunnel interface. This address is on a remote device.
	• **Address**: Enter the destination IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address based on your selection in the **Tunnel Mode** option.
	• **Application**: Choose an application from the drop-down list.
	  • **None**
	  • **Sig**

Internet Key Exchange

Table 18: Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1

Field	Description
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote endpoint identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you choose IKEv2.

IPSEC

Table 19: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds (1 hour)

Field	Description
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024 bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048 bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072 bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096 bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

Advanced

Table 20: Advanced

Field	Description
Associated VPN	Select a VPN from the drop-down list to associate with the IPsec tunnel.
Tunnel Route Via	Specify the tunnel route details to steer the application traffic through. **Note** You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3

Field	Description
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 through 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.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the interface.

IPv6 Tracker

This feature helps you configure the IPv6 tracker for the VPN interface.

The following table describes the options for configuring the IPv6 Tracker feature.

Table 21: IPv6 Tracker

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Tracker Name*	Name of the tracker. The name can be up to 128 alphanumeric characters.
Endpoint Tracker Type*	Choose a tracker type to configure endpoint trackers: • **ipv6-interface** **Note** This tracker type is available only in Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier. • **http** • **icmp** This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.

Field	Description
Endpoint	Choose an endpoint type: • **Endpoint DNS Name**: When you choose this option, the following field appears: **Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters. • **Endpoint IP**: When you choose this option, the following field appears: **Endpoint IP**: IPv6 address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint. The IPv6 address can be a valid IPv6 address in dotted-decimal notation. • **Endpoint API URL**: When you choose this option, the following field appears: **API url of endpoint**: API URL of the endpoint. The API URL can be a valid URL as described by RFC 3986.
Interval	Time interval between probes to determine the status of the configured endpoint. From Cisco Catalyst SD-WAN Manager Release 20.13.1, this option is called **Probe Interval**, allowing you to configure the time interval between probes. Range: 20 to 600 seconds Default: 60 seconds (1 minute) From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you select **icmp** as the endpoint tracker type, the default probe interval is 2 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

IPv6 Tracker Group

This feature helps you configure the IPv6 tracker froup for the VPN interface.

The following table describes the options for configuring the IPv6 tracker group feature.

Table 22: IPv6 Tracker Group

Field	Description
Tracker Name	Enter a tracker name.
Tracker Elements	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to an interface.
Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group, report that the interface is active.

Managed Cellular Activation - eSIM Controller

You can associate a Managed Cellular Activation cellular profile with a Managed Cellular Activation cellular controller.

1. Enter a feature name and description for **Managed Cellular Activation-eSIM Controller**.
2. Configure the Cellular ID based on the slot configuration of your device (for example, Cisco Catalyst 8200 Series, Cisco Catalyst 8300 Series, and ISR1000). Enter the interface slot and port number in which the cellular PIM card is installed.
3. To associate a Managed Cellular Activation cellular profile with a Managed Cellular Activation cellular controller, in the **Attach Profile** and **Data Profile** sections, choose the cellular profile.
4. Click **Save**.

Management VPN

This feature helps you configure VPN 512 or the management VPN.

See Configure management VPN using a configuration group

The following table describes the options for configuring the Management VPN feature.

Table 23: Management VPN

Field	Description
Type	Choose a feature from the drop-down list.

Field	Description
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Basic Configuration

Table 24: Basic Configuration

Field	Description
VPN	Management VPN carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices.
Name	Enter a name for the interface.

DNS

Table 25: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IPv4 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IPv4 address of a secondary DNS server in this VPN.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IPv6 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IPv6 address of a secondary DNS server in this VPN.

Host Mapping

Table 26: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.

Field	Description
List of IP Address*	Enter IP addresses to associate with the hostname. Separate the entries with commas.

IPv4/IPv6 Static Route

Table 27: IPv4/IPv6 Static Route

Field	Description
Add IPv4 Static Route	
IP 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:
	• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **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:
	  • **Administrative distance**: Enter the administrative distance for the route.

Add IPv6 Static Route	
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.

Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **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: • **NULL0***: 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: • **IPv6 NAT**: Choose NAT64 or NAT66.

OSPF Routing

Use the OSPF feature to configure transport-side routing, to provide reachability to networks at the local site.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.
Device Specific (Indicated by a host icon)	Use a device-specific value for the parameter. Choose **Device Specific** to provide a value for the key in the **Enter Key** field. The key is a unique string that helps identify the parameter. To change the default key, type a new string in the **Enter Key** field. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Default (indicated by a check mark)	The default value is shown for parameters that have a default setting.

The following tables describe the options for configuring the OSPF Routing feature.

Field	Description
Type	Choose a feature from the drop-down list.

Field	Description
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Basic Configuration

Field	Description
Router ID	Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address associated with the router for OSPF adjacencies. Default: <Device specific IPv4 system_ip >
Distance for External Routes	Specify the OSPF route administration distance for routes learned from other domains. Range: 1 through 255 Default: 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. Range: 1 through 255 Default: 110
Distance for Intra-Area Routes	Specify the OSPF route administration distance for routes within an area. Range: 0 through 255 Default: 110

Redistribute

Field	Description
Add Redistribute	
Protocol	Choose the protocol from which to redistribute routes into OSPF. • **Static** • **Connected** • **BGP** • **NAT**
Select Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

Maximum Metric (Router LSA)

Field	Description
Add Router LSA	
Type	Configure OSPF to advertise a maximum metric so that other routers do not prefer this router as an intermediate hop in their Shortest Path First (SPF) calculation. Choose a type: • **administrative**: Force the maximum metric to take effect immediately, through operator intervention. • **on-startup**: Advertise the maximum metric for the specified time. **Note** You can configure a maximum of one router LSA.

Area

Field	Description
Add Area	
Area Number*	Enter the number of the OSPF area. Allowed value: Any 32-bit integer
Set the area type	Choose the type of OSPF area: • **Stub** • **NSSA** **Note** The **Set the area type** option won't appear if you have entered 0 as a value for **Area Number***.
Add Interface	Configure the properties of an interface in an OSPF area.
Name*	Enter the name of the interface. For example, GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1.
Hello Interval (seconds)	Specify how often the router sends OSPF hello packets. Range: 1 through 65535 seconds Default: 10 seconds

Field	Description
Dead Interval (seconds)	Specify how often the router must receive an OSPF hello packet from its neighbor. If no packet is received, the router assumes that the neighbor is down. Range: 1 through 65535 seconds Default: 40 seconds (four times the default hello interval)
LSA Retransmission Interval (seconds)	Specify how often the OSPF protocol retransmits LSAs to its neighbors. Range: 1 through 65535 seconds Default: 5 seconds
Interface Cost	Specify the cost of the OSPF interface. Range: 1 through 65535
Designated Router Priority	Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the router with the highest router ID becomes the DR or the backup DR. Range: 0 through 255 Default: 1
OSPF Network Type	Choose the OSPF network type to which the interface is to connect: • **Broadcast network** • **Point-to-point network** • **Non-broadcast network** • **Point-to-multipoint network**
Passive Interface	Specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol. Default: Disabled
Authentication Type	Specify the key ID and authentication key if you use message digest (MD5): • **Message Digest Key ID**: Enter the key ID for message digest (MD5 authentication). The input value must be an integer. Range: 1 through 255 • **Message Digest Key**: Enter the MD5 authentication key. Range: 1 through 127 characters
Add Range	Configure the area range of an interface in an OSPF area.
IP Address*	Enter the IP address.
Subnet Mask*	Enter the subnet mask.

Field	Description
Cost	Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777214
No-advertise*	Enable this option to not advertise the Type 3 summary LSAs.

Advanced

Field	Description
Reference Bandwidth (Mbps)	Specify the reference bandwidth for the OSPF auto-cost calculation for the interface. Range: 1 through 4294967 Mbps Default: 100 Mbps
RFC 1583 Compatible	By default, the OSPF calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328.
Originate	Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
SPF Calculation Delay (milliseconds)	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)
Select Route Policy	Enter the name of a localized control policy to apply to routes coming from OSPF neighbors.

OSPFv3 IPv4 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv4 link-state routing protocol for IPv4 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv4 Routing feature.

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.

Basic Settings

Table 28: Basic Settings

Field	Description
Router ID	Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured.
Add Redistribute	
Protocol	Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions. • **Connected** • **Static** • **Nat-route** • **BGP**
Select Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

Area

Table 29: Area

Field	Description
Area Number*	Enter the number of the OSPFv3 area. Allowed value: Any 32-bit integer

Field	Description
Area Type	Choose the type of OSPFv3 area: • **Stub** - no external routes • **NSSA**: not-so-stubby area, allows external routes • **Normal** **Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**.
Interface	
Add Interface	Configure the properties of an interface in an OSPFv3 area.
Name*	Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1.
Cost	Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI	Specifies the Security Policy Index (SPI) value. Range: 256 through 4294967295
Authentication Key	Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long.
Passive Interface	Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol. Default: Disabled
IPv4 Range	
Add IPv4 Range	Configure the area range of an interface in an OSPFv3 area.
Network Address*	Enter the IPv4 address.
Subnet Mask*	Enter the subnet mask.
No Advertise*	Enable this option to not advertise the Type 3 summary LSAs.

Field	Description
Cost	Specify the cost of the OSPFv3 interface. Range: 1 through 65535

Advanced

Table 30: Advanced

Field	Description
Route Policy	Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors.
Reference Bandwidth (Mbps)	Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface. Range: 1 through 4294967 Mbps Default: 100 Mbps
RFC 1583 Compatible	By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328.
Originate	Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
Distance	Define the OSPFv3 route administration distance based on route type. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110

Field	Description
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 Default: 110
SPF Calculation Timers	Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm.
SPF Calculation Delay (milliseconds)	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. Range: 1 through 600000 ms (600 seconds) Default: 200 ms
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)
Maximum Metric (Router LSA)	Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this Cisco vEdge Device as an intermediate hop in their Shortest Path First (SPF) calculation. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds Maximum metric is disabled by default.

OSPFv3 IPv6 Routing

Use this feature to configure the Open Shortest Path First version 3 (OSPFv3) IPv6 link-state routing protocol for IPv6 unicast address families.

The following tables describe the options for configuring the OSPFv3 IPv6 Routing feature.

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.

Field	Description
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

Basic Settings

Table 31: Basic Settings

Field	Description
Router ID	Enter the OSPF router ID, in decimal four-part dotted notation. This value is the IP address that is associated with the router for OSPF adjacencies. Default: No Router ID is configured.
Add Redistribute	
Protocol	Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions. • **Connected** • **Static** • **BGP**
Select Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

Area

Table 32: Area

Field	Description
Area Number*	Enter the number of the OSPFv3 area. Allowed value: Any 32-bit integer
Area Type	Choose the type of OSPFv3 area: • **Stub**: No external routes • **NSSA**: Not-so-stubby area, allows external routes • **Normal** **Note** You can't enter a value for **Area type** if you have entered 0 as a value for **Area Number**.
Interface	

Field	Description
Add Interface	Configure the properties of an interface in an OSPFv3 area.
Name*	Enter the name of the interface. Examples of interface names: GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1.
Cost	Specify a number for the Type 3 summary link-state advertisement (LSA). OSPFv3 uses this metric during its SPF calculation to determine the shortest path to a destination. Range: 0 through 16777215
Authentication Type	Specify the SPI and authentication key if you use IPSec SHA1. • **no-auth**: Select no authentication. • **ipsec-sha1**: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.
SPI	Specifies the Security Policy Index (SPI) value. Range: 256 through 4294967295
Authentication Key	Provide a value for the authentication key. When IPSEC SHA-1 authentication is used, the key must be 40 hex digits long.
Passive Interface	Specify whether to set the OSPFv3 interface to be passive. A passive interface advertises its address, but does not actively run the OSPFv3 protocol. Default: Disabled
IPv6 Range	
Add IPv6 Range	Configure the area range of an interface in an OSPFv3 area.
Network Address*	Enter the IPv6 address.
Subnet Mask*	Enter the subnet mask.
No Advertise*	Enable this option to not advertise the Type 3 summary LSAs.
Cost	Specify the cost of the OSPFv3 interface. Range: 1 through 65535

Advanced

Table 33: Advanced

Field	Description
Route Policy	Enter the name of a localized control policy to apply to routes coming from OSPFv3 neighbors.

Field	Description
Reference Bandwidth (Mbps)	Specify the reference bandwidth for the OSPFv3 autocost calculation for the interface. Range: 1 through 4294967 Mbps Default: 100 Mbps
RFC 1583 Compatible	By default, the OSPFv3 calculation is done per RFC 1583. Disable this option to calculate the cost of summary routes based on RFC 2328.
Originate	Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear: • **Always**: Enable this option to always advertise the default route in an OSPF routing domain. • **Default Metric**: Set the metric used to generate the default route. Range: 0 through 16777214 Default: 10 • **Metric Type**: Choose to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
Distance	Define the OSPFv3 route administration distance based on route type. Default: 100
Distance for External Routes	Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110
Distance for Inter-Area Routes	Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110
Distance for Intra-Area Routes	Set the distance for routes within an area. Range: 0 through 255 Default: 110
SPF Calculation Timers	Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm.
SPF Calculation Delay (milliseconds)	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. Range: 1 through 600000 ms (600 seconds) Default: 200 ms

Field	Description
Initial Hold Time (milliseconds)	Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms
Maximum Hold Time (milliseconds)	Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)
Maximum Metric (Router LSA)	Configure OSPFv3 to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation. • **Immediately**: Force the maximum metric to take effect immediately, through operator intervention. • **On-startup**: Advertise the maximum metric for the specified number of seconds after the router starts up. Range: 5 through 86400 seconds Maximum metric is disabled by default.

Raw socket without VRF

Use the Raw Socket feature to configure a raw socket with VRF.

See Configure Raw Socket without VRF using a Configuration Group.

Table 34: Raw socket

Field	Description
Loopback configuration	You can enable or disable the loopback configuration. Note that loopback is supported only on Cisco Catalyst IR8340 rugged series routers.
Interface name	Enter a name for the interface.
Packet length	Specify the length of the packet.
Packet time	Define the time duration to send packets.
Special character	Defines a specific character that triggers the router to send all buffered data to the raw socket peer.

Field	Description
Encapsulation	Choose TCP or UDP as the protocol to encapsulate and transport serial data. If you select TCP, configure the following options: • Set the local port. • Specify the local IP. • Choose the TCP mode. • Configure any advanced TCP options as needed. If you select UDP, configure the relevant UDP connection fields.

Route Policy

Use this feature to configure the policy-based routing if you want certain packets to be routed through a specific path other than the obvious shortest path.

See Configure Route Policy Using a Configuration Group

The following table describes the options for configuring the route policy feature.

Table 35: Route Policy

Field	Description
Routing Sequence Name	Specifies the name of the routing sequence.
Protocol	Specifies the internet protocol. The options are IPv4, IPv6, or Both.
Condition	Specifies the routing condition. The options are: • **Address** • **AS Path List** • **Community List** • **Extended Community List** • **BGP Local Preference** • **Metric** • **Next Hop** • **OMP Tag** • **OSPF Tag**
Action Type	Specifies the action type. The options are **Accept** or **Reject**.

Field	Description
Accept Condition	Specifies the accept condition type. The options are: • **AS Path** • **Community** • **Local Preference** • **Metric** • **Metric Type** • **Next Hop** • **OMP Tag** • **Origin** • **OSPF Tag** • **Weight**

T1/E1 Controller

Use this feature to configure the T1 or E1 network interface module (NIM) parameters for Cisco IOS XE Catalyst SD-WAN devices.

See Configure T1 or E1 controller using a configuration group

Configure a T1 Controller

To configure a T1 controller, choose **T1** and configure the following parameters. Parameters marked with an asterisk are mandatory.

Table 36: Configure a T1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.
Framing	It is an optional field. Enter the T1 frame type: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.

Parameter Name	Description
Line Code	It is an optional field. Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Cable Length	Select the cable length to configure the attenuation • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. There is no default length.
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock. • **loop-timed**: • **network**:

Configure an E1 Controller

To configure an E1 controller, choose **E1** and configure the following parameters. Parameters marked with an asterisk are mandatory.

Table 37: Configure an E1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do not use CRC4.

Parameter Name	Description
Line Code	Choose the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Choose the clock source: • **internal**: Use the controller framer as the primary clock. • **line**: Use phase-locked loop (PLL) on the interface. This is the default.

Channel Group

Table 38: Channel Group

Parameter Name	Description
Add Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number and a value for the timeslot. • **Channel Group**: Enter a value for the channel group. Range: 0 through 30 • **Time Slot**: Type a value for the timeslot. Range: 0 through 31

Tracker

This feature helps you configure the tracker for the VPN interface.

For each parameter of the feature 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 to the left of the parameter field and choose one of the following:

The following table describes the options for configuring the Tracker feature.

Table 39: Tracker

Field	Description
Tracker Name*	Name of the tracker. The name can be up to 128 alphanumeric characters.

Field	Description
Endpoint Tracker Type*	Choose a tracker type to configure endpoint trackers: • **http** • **icmp** This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.
Endpoint	Choose an endpoint type: • **Endpoint IP**: When you choose this option, the following field appears: **Endpoint IP**: IP address of the endpoint. This is the destination on the internet to which the probes are sent to determine the status of an endpoint. • **Endpoint DNS Name**: When you choose this option, the following field appears: **Endpoint DNS Name**: DNS name of the endpoint. This is the destination on the internet to which probes are sent to determine the status of the endpoint. The DNS name can contain a minimum of one character and a maximum of 253 characters. • **Endpoint API URL**: When you choose this option, the following field appears: **API URL of endpoint***: API URL for the endpoint of the tunnel. This is the destination on the internet to which probes are sent to determine the status of the endpoint.
Interval	Time interval between probes to determine the status of the configured endpoint. From Cisco Catalyst SD-WAN Manager Release 20.13.1, this option is called **Probe Interval**, allowing you to configure the time interval between probes. Range: 20 to 600 seconds Default: 60 seconds (1 minute). From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you select **icmp** as the endpoint tracker type, the default probe interval is 2 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range: 1 to 10 Default: 3

Field	Description
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds

Tracker Group

Use the Tracker Group feature profile to track the status of transport interfaces.

See Configure NAT DIA Tracker using Configuration Groups

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

The following table describes the options for configuring the Tracker Group feature.

Table 40: Tracker Group

Field	Description
Tracker Elements*	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Add the existing interface tracker names, separated with a space. When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to an interface.
Tracker Boolean	This field is displayed only if you chose **Tracker Type** as the **Tracker Group**. Select **AND** or **OR**. **OR** is the default boolean operation. An **OR** ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group reports that the interface is active. If you select the **AND** operation, the transport-interface status is reported as active if both the associated trackers of the tracker group report that the interface is active.

Transport VPN

The Transport VPN feature helps you configure VPN 0 or the WAN VPN.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

The following table describes the options for configuring the Transport VPN feature.

Basic Configuration

Table 41: 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

DNS

Table 42: 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.
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.

Host Mapping

Table 43: 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.

Route

Table 44: 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:
	• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **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:
	  • **Administrative distance**: Enter the administrative distance for the route.

Add IPv6 Static Route	
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:
	• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **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:
	  • **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:
	  • **IPv6 NAT***: Choose NAT64 or NAT66.

Field	Description
Add BGP Routing	Choose a BGP route.

NAT

Table 45: NAT

Field	Description
Add NAT64 v4 Pool	
NAT64 v4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
NAT64 Pool Range Start*	Enter a starting IP address for the NAT pool.
NAT64 Pool Range End*	Enter a closing IP address for the NAT pool.
NAT64 Overload	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

Service

Table 46: Service

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

VPN Interface Multilink

Use the VPN Interface Multilink feature to configure multilink interface properties for Cisco IOS XE Catalyst SD-WAN devices.

See Configure VPN interface multilink using a configuration group

Table 47: Basic Configuration

Parameter Name	Description
Interface Name	Enter the name of the multilink interface.

Parameter Name	Description
Multilink Group Number *	Enter the number of the multilink group. It must be the same as the number you enter in the multilink interface name parameter. Range: 1 through 65535
PPP Authentication Protocol	Select the authentication protocol used by the multilink interface: • **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.
Hostname *	Enter hostname for PPP CHAP Authentication.
CHAP Password *	Enter password for PPP CHAP Authentication.
IPv4 Address *	To configure a static address, click **Static** and enter an IPv4 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. Default: 1
Mask	Choose a value for the subnet mask.
IPv6 Address *	To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.

Multilink

Table 48: Multilink

Parameter Name	Description
Add T1/E1 Interface	
T1	
Description	Enter a description for the T1controller.

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the T1 NIM is installed. For example, 0/1/0.
Framing	Enter the T1 frame type: • **esf**: Send T1 frames as extended superframes. This is the default. • **sf**: Send T1 frames as superframes. Superframing is sometimes called D4 framing.
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send T1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • **b8zs**: Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouped into extended superframes.
Cable Length	Select the cable length to configure the attenuation • **short**: Set the transmission attenuation for cables that are 660 feet or shorter. • **long**: Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. There is no default length.
E1	
Description	Enter a description for the E1 controller.
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do no use CRC4.

Parameter Name	Description
Clock Source	Select the clock source: • **line**: Use phase-locked loop (PLL) on the interface. This is the default. When both E1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source. • **internal**: Use the controller framer as the primary clock.
Line Code	Select the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Add Channel Group	
Channel Group	To configure the serial WAN on the interface, enter a channel group number. Range: 0 through 30
Time Slot	To configure the serial WAN on the interface, enter a value for the timeslot. Range: 0 through 31
Add New A/S Serial Interface	
Interface Name	Enter the name of the serial interface.
Description	Enter a description for the serial interface.
Bandwidth	For transmitted traffic, set the bandwidth above which to generate notifications.
Clock Rate	Specify a value for the clock rate. Range: 1200 through 800000

Tunnel

Table 49: Tunnel

Parameter Name	Description
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.
Restrict	Enable this option to drop packets when a tunnel to the service is unreachable.
Groups	Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.

Parameter Name	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 8 Default: 2
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.
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 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	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on 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**
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**

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. 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 through 1460 bytes

ACL

Table 50: ACL

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

Advanced

Table 51: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the multilink interface.
Description	Enter a description for the multilink interface.
PPP Authentication Type	Select the type authentication from one of the following options.: • **Unidirectional**: The server initiates the authentication. • **Bidirectional**: Both the client and the server can initiate the authentication.

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco 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: 500 through 1460 bytes Default: 536
Disable Fragmentation	Click **On** to disable fragmentation for PPP Multilink Protocol data units (PDUs).
Fragment Max Delay	Configure the delay between the transmission of fragments in a PPP Multilink Protocol link. Range: 0 through 1000 Default: No CLI Command
Interleaving Fragments	Enable interleave fragmentation for PPP Multilink Protocol data units (PDUs).
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 MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. Range: 576 through 1804 Default: 1500 bytes
IP Directed-Broadcast	Enable the translation of a directed broadcast to physical broadcasts.
Shaping Rate (Kbps)	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).

Ethernet PPPoE

Configure the PPPoE over GigabitEthernet interfaces on Cisco IOS XE Catalyst SD-WAN devices, to provide PPPoE client support.

Basic Configuration

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the ethernet interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Dialer Pool Member *	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

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.

Tunnel

Parameter Name	Description
Tunnel Interface	

Parameter Name	Description
Per Tunnel QoS	Enable per tunnel QoS and choose **Spoke** to configure the spoke network topology
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.
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
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 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. 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 through 1460 bytes Default: None
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.

Parameter Name	Description
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 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. **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*
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.
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 allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
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

NAT

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

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

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

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.

Advanced

Parameter Name	Description
Shutdown	Choose **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.

Parameter Name	Description
Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation. Range: 64 through 1792 bytes
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.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.

Cellular Interface

This feature helps you configure the cellular interface in VPN 0 or the WAN VPN.

The following tables describe the options for configuring the Cellular Interface feature.

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Associated VPN	VPN 0 or the WAN transport VPN.
Associated Tracker	Choose a tracker.

Basic Configuration

Field	Description
Shutdown*	Enable or disable the interface.
Interface Name*	Enter the name of the interface.
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.

Tunnel

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.

Field	Description
Group	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.
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.

Field	Description
Low-Bandwidth Link	Enable the low-bandwidth feature.
Tunnel 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: 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: • **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.

Field	Description
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
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

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)

ARP

Field	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.

Advanced

Field	Description
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. 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 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: 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.

Field	Description
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.
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. 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. 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.