



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.

- [ACL IPv4, on page 1](#)
- [ACL IPv6 , on page 3](#)
- [BGP Routing, on page 4](#)
- [Cellular Controller, on page 13](#)
- [Cellular Profile, on page 14](#)
- [Ethernet Interface, on page 15](#)
- [GPS, on page 24](#)
- [GRE, on page 25](#)
- [IPSEC, on page 29](#)
- [IPv6 Tracker, on page 33](#)
- [IPv6 Tracker Group, on page 34](#)
- [Managed Cellular Activation - eSIM Controller, on page 35](#)
- [Management VPN, on page 36](#)
- [OSPF Routing, on page 38](#)
- [OSPFv3 IPv4 Routing, on page 42](#)
- [OSPFv3 IPv6 Routing, on page 46](#)
- [Route Policy, on page 50](#)
- [T1/E1 Controller, on page 51](#)
- [Tracker, on page 53](#)
- [Tracker Group, on page 54](#)
- [Transport VPN, on page 55](#)
- [VPN Interface Multilink , on page 58](#)

ACL IPv4

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.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: <ul style="list-style-type: none"> • DSCP • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Peer
Action Type	Specifies the action type. The options are: Accept or Reject.

Field	Description
Accept Condition	Specifies the accept condition type. The options are: <ul style="list-style-type: none"> • Counter • DSCP • Log • Next Hop • Mirror List • Class • 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.

ACL IPv6

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.

Field	Description
ACL Sequence Name	Specifies the name of the ACL sequence.
Condition	Specifies the ACL condition. The options are: <ul style="list-style-type: none"> • Next Header • Packet Length • PLP • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port • TCP • Class • Traffic Class
Action Type	Specifies the action type. The options are: Accept or Reject.
Accept Condition	Specifies the accept condition type. The options are: <ul style="list-style-type: none"> • Counter • Log • Next Hop • Traffic Class • Mirror List • Class • 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

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

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

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*	<p>Choose the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are static, connected, ospf, omp, eigrp, and nat.</p> <p>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.</p> <p>Route policy is not supported in Cisco vManage Release 20.9.1.</p>
Route Policy	<p>Enter the name of the route policy to apply to redistributed routes.</p> <p>Route policy is not supported in Cisco vManage Release 20.9.1.</p>
Network	
Network Prefix*	<p>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.</p>
Aggregate Address	
Aggregate Prefix*	<p>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.</p>
AS Set Path	<p>Enable this option to generate set path information for the aggregated prefixes.</p>
Summary Only	<p>Enable this option to filter out more specific routes from BGP updates.</p>
Table Map	
Policy Name	<p>Enter the route map that controls the downloading of routes.</p> <p>Route policy is not supported in Cisco vManage Release 20.9.1.</p>
Filter	<p>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.</p> <p>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.</p>
IPv6 Settings	
Maximum Paths	<p>Specify the maximum number of parallel internal BGP paths that can be installed into a route table to enable internal BGP multipath load sharing.</p> <p>Range: 0 to 32</p>

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

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

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
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.

Field	Description
Keepalive Time (seconds)	<p>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.</p> <p>Range: 0 through 65535 seconds</p> <p>Default: 60 seconds (one-third the hold-time value)</p>
Hold Time (seconds)	<p>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.</p> <p>Range: 0 through 65535 seconds</p> <p>Default: 180 seconds (three times the keepalive time)</p>
Send Label	<p>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.</p>
Add Neighbor Address Family	
Family Type*	<p>Choose the BGP IPv4 unicast address family.</p>
In Route Policy	<p>Specify the name of a route policy to apply to prefixes received from the neighbor.</p> <p>Route policy is not supported in Cisco vManage Release 20.9.1.</p>
Out Route Policy	<p>Specify the name of a route policy to apply to prefixes sent to the neighbor.</p> <p>Route policy is not supported in Cisco vManage Release 20.9.1.</p>

Field	Description
Maximum Prefix Reach Policy*	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • 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. <p>When you choose this option, the following fields appear:</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 neighborhood. 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.

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*	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • 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. <p>When you choose this option, the following fields appear:</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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

Field	Description
Keepalive (seconds)	<p>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.</p> <p>Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)</p>
Hold Time (seconds)	<p>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.</p> <p>Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive time)</p>

Field	Description
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.

The following table describes the options for configuring the Cellular Controller 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.
Cellular ID	Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0.
Primary SIM slot	Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable.
SIM Failover Retries	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

Field	Description
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.

After configuring the above parameters, choose a cellular profile to associate with the cellular controller and click **Save**.

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.

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.

Field	Description
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.

Field	Description
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. <ul style="list-style-type: none"> • 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 .
Subnet Mask	Enter the subnet mask.
Configure Secondary IP Address	Enter up to four secondary IPv4 addresses for a service-side interface. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Tunnel

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.

Field	Description
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
Color	Choose a color for the TLOC.
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
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
Port Hop	Enable port hopping. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). Default: Enabled
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 TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None

Field	Description
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.
Allow Service	<p>Allow or disallow the following services on the interface:</p> <ul style="list-style-type: none"> • All • BGP • DHCP • NTP • SSH • DNS • ICMP • HTTPS • OSPF • STUN • SNMP • NETCONF • BFD
Encapsulation	

Field	Description
Encapsulation*	<p>Choose an encapsulation type:</p> <ul style="list-style-type: none"> • gre: Use GRE encapsulation on the tunnel interface. • ipsec: Use IPsec encapsulation on the tunnel interface. <p>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.</p> <p>When you choose gre, the following fields appear:</p> <ul style="list-style-type: none"> • 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 <p>When you choose ipsec, the following fields appear:</p> <ul style="list-style-type: none"> • 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
<p>Multi-Region Fabric</p> <p>Note These options appear only when Multi-Region Fabric is enabled.</p>	
Connect to Core Region	<p>(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1)</p> <p>(Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface:</p> <ul style="list-style-type: none"> • 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.

Field	Description
Connect to Secondary Region	<p>(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1)</p> <p>(Applicable to an edge router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface:</p> <ul style="list-style-type: none"> • 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	<p>Choose the NAT translation type for IPv4:</p> <ul style="list-style-type: none"> • interface • pool • loopback <p>Default: interface. It is supported for NAT64.</p>
UDP Timeout	<p>Specify when NAT translations over UDP sessions time out.</p> <p>Range: 1 through 8947 minutes</p> <p>Default: 1 minute</p>
TCP Timeout	<p>Specify when NAT translations over TCP sessions time out.</p> <p>Range: 1 through 8947 minutes</p> <p>Default: 60 minutes (1 hour)</p>

Field	Description
Add Multiple NAT	<p>Choose the NAT type:</p> <ul style="list-style-type: none"> • Interface: This is the default value. • Pool: Configure the following: <ul style="list-style-type: none"> • 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	<p>Choose the direction in which to perform network address translation.</p> <ul style="list-style-type: none"> • 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	<p>Choose NAT64 or NAT66. When you choose NAT66, the following fields appear:</p> <ul style="list-style-type: none"> • 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	<p>Specify whether the interface runs in full-duplex or half-duplex mode.</p> <p>Default: full</p>
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	<p>Specify the maximum MTU size of packets on the interface.</p> <p>Range: 576 through 9216</p> <p>Default: 1500 bytes</p>
Interface MTU	<p>Enter the maximum transmission unit size for frames received and transmitted on the interface.</p> <p>Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet)</p> <p>Default: 1500 bytes</p>
TCP MSS	<p>Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.</p> <p>Range: 500 to 1460 bytes</p> <p>Default: None</p>

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: <ul style="list-style-type: none"> • 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	<p>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.</p> <p>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.</p> <p>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.</p>
ICMP Redirect Disable	<p>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.</p> <p>By default, an interface allows ICMP redirect messages.</p>

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.

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	<p>Select the GPS mode:</p> <ul style="list-style-type: none"> • 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.

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

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: <ul style="list-style-type: none"> • 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

Field	Description
Source	<p>Enter the source of the GRE interface:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Destination	<p>Enter the source of the GRE interface:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Mask*: Enter the subnet mask. • IPv6 Address: Enter the destination IPv6 or address for the GRE tunnel.

IKE

Field	Description
IKE Version	<p>Enter 1 to choose IKEv1.</p> <p>Enter 2 to choose IKEv2.</p> <p>Default: IKEv1</p>
IKE Integrity Protocol	<p>Choose one of the following modes for the exchange of keying information and setting up IKE security associations:</p> <ul style="list-style-type: none"> • 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. <p>Default: Main mode</p>

Field	Description
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

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
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

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • None • Sig

Advanced

Field	Description
Shutdown	Click Off to enable the interface.
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 TCP 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

Field	Description
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.

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

Field	Description
Interface Name	Enter the name of the IPsec interface.
Description	Enter a description of the IPsec interface.

Field	Description
Tunnel Mode	Choose from one of the following IPsec tunnel modes: <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • None • Sig

Internet Key Exchange

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

Field	Description
IKE Integrity Protocol	<p>Choose one of the following modes for the exchange of keying information and setting up IKE security associations:</p> <ul style="list-style-type: none"> • 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. <p>Default: Main mode</p>
IPsec Rekey Interval	<p>Specify the interval for refreshing IKE keys.</p> <p>Range: 3600 through 1209600 seconds (1 hour through 14 days)</p> <p>Default: 14400 seconds (4 hours)</p>
IKE Cipher Suite	<p>Specify the type of authentication and encryption to use during IKE key exchange.</p> <p>Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2</p> <p>Default: aes256-cbc-sha1</p>
IKE Diffie-Hellman Group	<p>Specify the Diffie-Hellman group to use in IKE key exchanges.</p> <p>Values: 2, 14, 15, 16, 19, 20, 21, 24</p> <p>Default: 16</p>
IKE ID for Local End Point	<p>If the remote IKE peer requires a local endpoint identifier, specify it.</p> <p>Range: 1 through 64 characters</p> <p>Default: Source IP address of the tunnel</p>
IKE ID for Remote End Point	<p>If the remote IKE peer requires a remote endpoint identifier, specify it.</p> <p>Range: 1 through 64 characters</p> <p>Default: Destination IP address of the tunnel</p> <p>There is no default option if you choose IKEv2.</p>

IPSEC

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

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: <ul style="list-style-type: none"> • 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

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 TCP 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 IPv6 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 1: 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: <ul style="list-style-type: none"> • ipv6-interface <p>Note This tracker type is available only in Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier.</p> <ul style="list-style-type: none"> • http • icmp <p>This tracker type is available from Cisco Catalyst SD-WAN Manager Release 20.13.1.</p>

Field	Description
Endpoint	<p>Choose an endpoint type:</p> <ul style="list-style-type: none"> • 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	<p>Time interval between probes to determine the status of the configured endpoint.</p> <p>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.</p> <p>Range: 20 to 600 seconds</p> <p>Default: 60 seconds (1 minute)</p> <p>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.</p>
Multiplier	<p>Number of times probes are sent before declaring that the endpoint is down.</p> <p>Range: 1 to 10</p> <p>Default: 3</p>
Threshold	<p>Wait time for the probe to return a response before declaring that the configured endpoint is down.</p> <p>Range: 100 to 1000 milliseconds</p> <p>Default: 300 milliseconds</p>

IPv6 Tracker Group

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

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

Table 2: 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.

The following table describes the options for configuring the Management VPN 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

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

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

Field	Description
Add New Host Mapping	

Field	Description
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP Address*	Enter IP addresses to associate with the hostname. Separate the entries with commas.

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*	<p>Choose one of the following options to configure the next hop to reach the static route:</p> <ul style="list-style-type: none"> • nextHop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv4 address. • Administrative distance*: Enter the administrative distance for the route. • dhcp • null0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • Administrative distance: Enter the administrative distance for the route.
Add IPv6 Static Route	
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	<p>Choose one of the following options to configure the next hop to reach the static route:</p> <ul style="list-style-type: none"> • Next Hop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv6 address. • Administrative distance*: Enter the administrative distance for the route. • Null 0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)	<p>Enter a value for the parameter and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>
Device Specific (Indicated by a host icon)	<p>Use a device-specific value for the parameter.</p> <p>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.</p> <p>Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.</p>
Default (indicated by a check mark)	<p>The default value is shown for parameters that have a default setting.</p>

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. <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Choose a type:</p> <ul style="list-style-type: none"> • administrative: Force the maximum metric to take effect immediately, through operator intervention. • on-startup: Advertise the maximum metric for the specified time. <p>Note You can configure a maximum of one router LSA.</p>

Area

Field	Description
Add Area	
Area Number*	<p>Enter the number of the OSPF area.</p> <p>Allowed value: Any 32-bit integer</p>
Set the area type	<p>Choose the type of OSPF area:</p> <ul style="list-style-type: none"> • Stub • NSSA <p>Note The Set the area type option won't appear if you have entered 0 as a value for Area Number*.</p>
Add Interface	
Name*	<p>Enter the name of the interface. For example, GigabitEthernet0/0/1, GigabitEthernet0/1/2.1, GigabitEthernet0, or Loopback1.</p>
Hello Interval (seconds)	<p>Specify how often the router sends OSPF hello packets.</p> <p>Range: 1 through 65535 seconds</p> <p>Default: 10 seconds</p>
Dead Interval (seconds)	<p>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.</p> <p>Range: 1 through 65535 seconds</p> <p>Default: 40 seconds (four times the default hello interval)</p>

Field	Description
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: <ul style="list-style-type: none"> • 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): <ul style="list-style-type: none"> • 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.
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: <ul style="list-style-type: none"> • 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

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. <ul style="list-style-type: none"> • 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

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: <ul style="list-style-type: none"> • Stub - no external routes • NSSA: not-so-stubby area, allows external routes • Normal <p>Note You can't enter a value for Area type if you have entered 0 as a value for Area Number.</p>
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. <ul style="list-style-type: none"> • 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.
Cost	Specify the cost of the OSPFv3 interface. Range: 1 through 65535

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: <ul style="list-style-type: none"> • 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 Cisco vEdge Device as an intermediate hop in their Shortest Path First (SPF) calculation. <ul style="list-style-type: none"> • 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.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

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	

Field	Description
Protocol	Choose the protocol from which to redistribute routes into OSPFv3, for all OSPFv3 sessions. <ul style="list-style-type: none"> • 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

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: <ul style="list-style-type: none"> • Stub: No external routes • NSSA: Not-so-stubby area, allows external routes • Normal <p>Note You can't enter a value for Area type if you have entered 0 as a value for Area Number.</p>
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. <ul style="list-style-type: none"> • no-auth: Select no authentication. • ipsec-sha1: Enter the value for the IPSEC Secure Hash Algorithm 1 (SHA-1) authentication.

Field	Description
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

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.

Field	Description
Originate	<p>Enable this option to generate a default external route into an OSPF routing domain. When you enable this option, the following fields appear:</p> <ul style="list-style-type: none"> • 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	<p>Define the OSPFv3 route administration distance based on route type. Default: 100</p>
Distance for External Routes	<p>Set the OSPFv3 distance for routes learned from other domains. Range: 0 through 255 Default: 110</p>
Distance for Inter-Area Routes	<p>Set the distance for routes coming from one area into another. Range: 0 through 255 Default: 110</p>
Distance for Intra-Area Routes	<p>Set the distance for routes within an area. Range: 0 through 255 Default: 110</p>
SPF Calculation Timers	<p>Configure the amount of time between when OSPFv3 detects a topology and when it runs its SPF algorithm.</p>
SPF Calculation Delay (milliseconds)	<p>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</p>
Initial Hold Time (milliseconds)	<p>Specify the amount of time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 1000 ms</p>
Maximum Hold Time (milliseconds)	<p>Specify the longest time between consecutive SPF calculations. Range: 1 through 600000 ms (600 seconds) Default: 10000 ms (10 seconds)</p>

Field	Description
Maximum Metric (Router LSA)	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>Range: 5 through 86400 seconds</p> <p>Maximum metric is disabled by default.</p>

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.

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

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	<p>Specifies the routing condition. The options are:</p> <ul style="list-style-type: none"> • 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	<p>Specifies the accept condition type. The options are:</p> <ul style="list-style-type: none"> • 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.

Configure a T1 Controller

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

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	<p>It is an optional field. Enter the T1 frame type:</p> <ul style="list-style-type: none"> • esf: Send T1 frames as extended superframes. This is the default. • sf: Send T1 frames as superframes. Superframing is sometimes called D4 framing.
Line Code	<p>It is an optional field. Select the line encoding to use to send T1 frames:</p> <ul style="list-style-type: none"> • 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

Parameter Name	Description
Cable Length	<p>Select the cable length to configure the attenuation</p> <ul style="list-style-type: none"> • 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 than 660 feet. <p>There is no default length.</p>
Clock Source	<p>Select the clock source:</p> <ul style="list-style-type: none"> • 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.

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	<p>Enter the E1 frame type:</p> <ul style="list-style-type: none"> • crc4: Use cyclic redundancy check 4 (CRC4). This is the default. • no-crc4: Do not use CRC4.
Line Code	<p>Choose the line encoding to use to send E1 frames:</p> <ul style="list-style-type: none"> • ami: Use alternate mark inversion (AMI) as the linecode. • hdb3: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	<p>Choose the clock source:</p> <ul style="list-style-type: none"> • internal: Use the controller framer as the primary clock. • line: Use phase-locked loop (PLL) on the interface. This is the default.

Channel Group

Parameter Name	Description
Add Channel Group	<p>To configure the serial WAN on the E1 interface, enter a channel group number and a value for the timeslot.</p> <ul style="list-style-type: none"> • 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.

Field	Description
Tracker Name*	Name of the tracker. The name can be up to 128 alphanumeric characters.
Endpoint Tracker Type*	<p>Choose a tracker type to configure endpoint trackers:</p> <ul style="list-style-type: none"> • http

Field	Description
Endpoint	<p>Choose an endpoint type:</p> <ul style="list-style-type: none"> • 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	<p>Time interval between probes to determine the status of the configured endpoint.</p> <p>Range: 20 to 600 seconds</p> <p>Default: 60 seconds (1 minute).</p>
Multiplier	<p>Number of times probes are sent before declaring that the endpoint is down.</p> <p>Range: 1 to 10</p> <p>Default: 3</p>
Threshold	<p>Wait time for the probe to return a response before declaring that the configured endpoint is down.</p> <p>Range: 100 to 1000 milliseconds</p> <p>Default: 300 milliseconds</p>

Tracker Group

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

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.

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

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

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.

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

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

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*	<p>Choose one of the following options to configure the next hop to reach the static route:</p> <ul style="list-style-type: none"> • nextHop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv4 address. • Administrative distance*: Enter the administrative distance for the route. • dhcp • null0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • Administrative distance: Enter the administrative distance for the route.
Add IPv6 Static Route	
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	<p>Choose one of the following options to configure the next hop to reach the static route:</p> <ul style="list-style-type: none"> • Next Hop: When you choose this option and click Add Next Hop, the following fields appear: <ul style="list-style-type: none"> • Address*: Enter the next-hop IPv6 address. • Administrative distance*: Enter the administrative distance for the route. • Null 0: When you choose this option, the following field appears: <ul style="list-style-type: none"> • IPv6 Route Null 0*: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • NAT: When you choose this option, the following field appears: <ul style="list-style-type: none"> • IPv6 NAT*: Choose NAT64 or NAT66.
Add BGP Routing	Choose a BGP route.

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	<p>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.</p> <p>Default: Disabled</p>

Service

Field	Description
Add Service	
Service Type	<p>Choose the service available in the VPN.</p> <p>Value: TE</p>

VPN Interface Multilink

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

Basic Configuration

Parameter Name	Description
Interface Name	Enter the name of the multilink interface.
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: <ul style="list-style-type: none"> • CHAP: Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters. • PAP: Enter the username and password provided by your ISP. <i>username</i> can be up to 255 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

Parameter Name	Description
Add T1/E1 Interface	
T1	
Description	Enter a description for the T1 controller.
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 than 660 feet. <p>There is no default length.</p>
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: <ul style="list-style-type: none"> • crc4: Use cyclic redundancy check 4 (CRC4). This is the default. • no-crc4: Do not use CRC4.

Parameter Name	Description
Clock Source	Select the clock source: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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

Parameter Name	Description
Color	Choose a color for the TLOC.
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
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
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
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

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

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.: <ul style="list-style-type: none"> • Unidirectional: The server initiates the authentication. • Bidirectional: Both the client and the server can initiate the authentication.
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.

Parameter Name	Description
IP MTU	<p>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.</p> <p>Range: 576 through 1804</p> <p>Default: 1500 bytes</p>
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).

