Cisco Catalyst SD-WAN Interfaces Configuration Guide, Releases 26.x and Later

First Published: 2026-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **Network Interfaces** 3

Network Interfaces 3

CHAPTER 3 **Cellular Interfaces** 5

Feature history for cellular interfaces 5

Cellular interfaces 6

Supported devices 7

Guidelines 8

Configure cellular interface 9

Configure cellular interfaces using a configuration group 9

Configure cellular interfaces using CLI 19

Configure cellular interfaces using templates 20

Reset the profile configuration of a cellular modem using CLI commands 28

Troubleshoot LTE modem crash 28

CHAPTER 4 **DSL IPoE** 31

Configure DSL IPoE 31

Configure DSL IPoE using a configuration group 31

Configure DSL IPoE using templates 38

CHAPTER 5 **DSL PPPoA** 49

Configure DSL PPPoA 49

Configure DSL PPPoA using a configuration group 49

Configure DSL PPPoA using templates 57

CHAPTER 6 DSL PPPoE 67

Feature history for DSL PPPoe 67

Configure DSL PPPoE 67

Configure DSL PPPoE using a configuration group 68

Configure DSL PPPoE using templates 75

CHAPTER 7 Dynamic Interfaces 85

Feature history for dynamic interfaces 85

Configure dynamic interfaces 85

CHAPTER 8 EtherChannels 89

Feature history for EtherChannels 89

EtherChannels on the service side 90

EtherChannels on the service side 90

Supported devices for service side EtherChannel 90

Prerequisites for EtherChannels on the service side 91

Restrictions for EtherChannels on the service side 92

Load balancing for service side EtherChannels using CLI commands 92

Enable load balancing on an individual port channel 92

Enable hash algorithms for flow-based load balancing on a global level 94

Enable hash algorithms flow-based load balancing on an individual port channel interface 94

Enable VLAN load balancing per port channel on the service side 95

Configure load balancing for EtherChannels on the service side using CLI commands 96

Configure a service-side port channel and member link interface using configuration groups 97

EtherChannels on the transport side 98

Supported devices for transport side EtherChannel 98

Prerequisites for EtherChannels on the transport side 99

Restrictions for EtherChannels on the transport side 99

Configure a transport side EtherChannels using a CLI template 100

Configure load balancing for EtherChannels on the Transport Side using CLI Commands 102

Enable load balancing on individual portchannel interface on the transport side 104

Enable load balancing globally for EtherChannels on the transport side 104

Enable hash algorithms globally for EtherChannels on the transport side 105

Monitor configured EtherChannel using CLI 107
Aggregate EtherChannel Quality of Service 107
Prerequisites for Aggregate EtherChannel Quality of Service 108
Restrictions for Aggregate EtherChannel Quality of Service 108
Configure Aggregate EtherChannel Quality of Service using CLI Template 108
Verify Aggregate EtherChannel Quality of Service 111

CHAPTER 9 IP Directed Broadcast 113
IP directed broadcast 113
Configure IP directed broadcast using CLI commands 113

CHAPTER 10 Loopback Interfaces 115
Feature history for loopback interfaces 115
Loopback interfaces 116
Implicit ACLs on loopback interfaces 116
Loopback TLOC interface bound to a physical WAN interface 116
Loopback TLOC interface not bound to a physical WAN interface 117
Bind mode and unbind mode 117
Configure implicit ACL on loopback interfaces using CLI commands 118
Examples of implicit ACL configurations on loopback interfaces 119
Verify implicit ACL configurations on loopback interfaces 120

CHAPTER 11 Subinterfaces 123
Subinterfaces 123
Configuration examples for subinterfaces 124
Verify configurations on subinterfaces 124

CHAPTER 12 VPN Ethernet Interface 127
Configure VPN ethernet interface 127
Configure VPN ethernet interface using a configuration group 127
Configure prefix list for VRRP using a configuration group 137
Configure VPN ethernet interface using templates 137
Configure a prefix list for VRRP 144
Configure a prefix list for VRRP in the device template 145

CHAPTER 13 VPN Interface Bridge 147
Configure VPN interface bridge 147

CHAPTER 14 VPN Interface Ethernet PPPoE 153
Configure VPN interface ethernet PPPoE 153
Configure VPN interface ethernet PPPoE using a configuration group 153
Configure VPN interface ethernet PPPoE using templates 160

CHAPTER 15 VPN Interface GRE 169
Configure VPN interface GRE 169
Configure VPN interface GRE on transport VPN using a configuration group 169
Configure GRE on service VPN using a configuration group 173
Configure VPN Interface GRE using templates 177

CHAPTER 16 VPN Interface IPsec 181
Feature history for VPN interface IPsec 181
Configure VPN interface IPsec 181
Configure IPsec on the transport VPN using a configuration group 181
Configure IPsec on the service VPN using a configuration group 186
Configure VPN interface IPsec using templates 190
Change the IKE version from IKEv1 to IKEv2 195
CLI configuration examples for VPN interface IPsec 196

CHAPTER 17 VPN Interface Multilink 199
Configure VPN interface multilink 199
Configure VPN interface multilink using a configuration group 199
Configure VPN interface multilink using templates 205

CHAPTER 18 VPN Interface SVI 213
Feature history for VPN interface SVI 213
Configure VPN interface SVI 213
Configure SVI interface using a configuration group 213

Configure SVI interface using templates 219

CHAPTER 19 VPN Interface T1/E1 223

Configure VPN interface T1/E1 223

Configure VPN interface T1/E1 using a configuration group 223

Configure T1 or E1 controller using a configuration group 230

Configure VPN interface T1/E1 using templates 232

Configure T1 or E1 controller using templates 237

CHAPTER 20 VRRP Interface Tracking 241

Feature history for VRRP interface tracking 241

VRRP 242

Configure VRRP 243

Configuring VRRP using Cisco Catalyst SD-WAN Manager 243

Configure a prefix list for VRRP using Configuration Groups 244

Configure a prefix list for VRRP using a feature template 245

Configure a prefix list for VRRP using a device template 245

Configure VRRP using CLI commands 246

VRRP tracking use cases 251

Restrictions for VRRP interface tracking 252

Configure VRRP tracking using CLI templates 252

VRRP object tracking using CLI 252

SIG container tracking 253

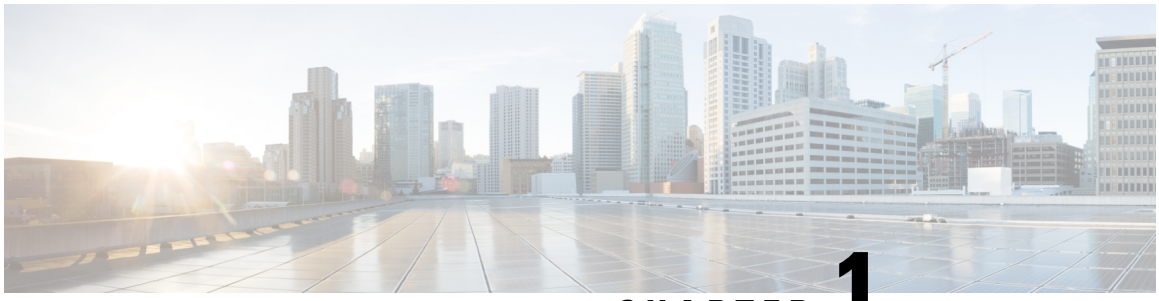
Configure VRRP tracking 254

Configure an object tracker using a feature template 254

Configure VRRP for a VPN interface template and associate interface object tracker 255

Monitor VRRP configuration 256

Verify VRRP tracking 257



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

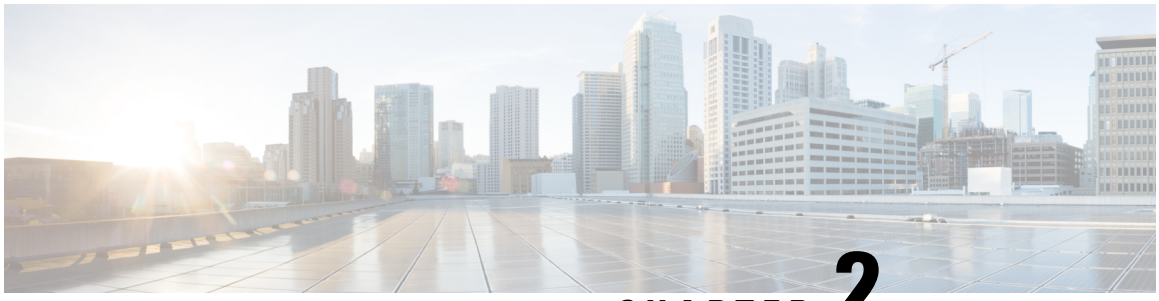
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Network Interfaces

• Network Interfaces, on page 3

Network Interfaces

A network interface in Cisco Catalyst SD-WAN is a network component that,

- is associated with a VPN, and
- is configured and enabled within that VPN.

Each interface can be present only in a single VPN. Create VPN feature templates to configure VPN parameters, and then create interface feature templates to configure the interfaces in the VPN.

Interface operational requirements

For an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

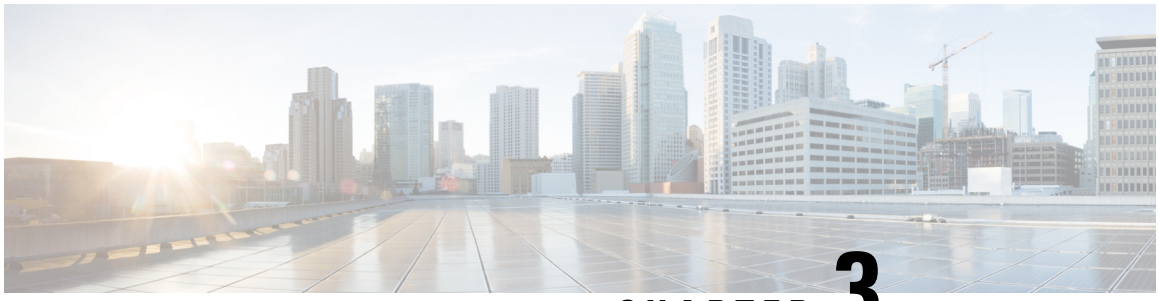
You can configure up to 512 interfaces on a Cisco IOS XE Catalyst SD-WAN device. This number includes physical interfaces, loopback interfaces, and subinterfaces.

Configure each network interface on a device with a unique IP address.

Note To maximize the efficiency of the load-balancing among Cisco SD-WAN Controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE Catalyst SD-WAN devices in the domain. Example of a sequential numbering schemes is 172.16.1.1, 172.16.1.2, 172.16.1.3, and so on.

If you try to configure an interface or sub-interface beyond the supported limit, the device generates a notification to Cisco SD-WAN Manager.

Network Interfaces



CHAPTER 3

Cellular Interfaces

- Feature history for cellular interfaces, on page 5
- Cellular interfaces, on page 6
- Supported devices, on page 7
- Guidelines, on page 8
- Configure cellular interface, on page 9
- Reset the profile configuration of a cellular modem using CLI commands, on page 28
- Troubleshoot LTE modem crash, on page 28

Feature history for cellular interfaces

Table 1: Feature History

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

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

Cellular interfaces

A cellular interface is a network interface that

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

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

Cellular module

A cellular module

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

Data profile

A data profile for a cellular device

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

Supported devices

Table 2: Supported Platforms and Modules

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

Guidelines

Circuit of last resort

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

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

Active circuit

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

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

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

Configure cellular interface

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

Use one of the methods to configure cellular interface.

- Configure cellular interfaces using a configuration group
- Configure cellular interfaces using the CLI
- Configure cellular interfaces using feature templates

Configure cellular interfaces using a configuration group

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

Before you begin

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

Procedure

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

Step 2 Create and configure a Transport VPN feature in a Transport & Management profile.

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

Table 3: Basic Configuration

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

b. Configure DNS.

Table 4: DNS

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

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

c. Configure host mapping.

Table 5: Host Mapping

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

d. Configure routes.

Table 6: Route

Field	Description
Add IPv4 Static Route	
Network address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.

Gateway*	Choose one of the following options to configure the next hop to reach the static route:
	• **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv4 address.
	  • **Administrative distance***: Enter the administrative distance for the route.
	• **dhcp**
	• **null0**: When you choose this option, the following field appears:
	  • **Administrative distance**: Enter the administrative distance for the route.

Add IPv6 Static Route	

Field	Description
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT***: Choose NAT64 or NAT66.
Add BGP Routing	Choose a BGP route.

e. Configure services.

Table 7: Service

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

Step 3 Configure a Cellular Interface feature to associate with the Transport VPN.

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

b. Configure the basic parameters.

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

Field	Description
DHCP Helper	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.

c. Configure the tunnel parameters.

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

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

Field	Description
Tunnel TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
Clear-Dont-Fragment	Enable this option to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.
Allow Service	Allow or disallow the following services on the interface: • **All** • **BGP** • **DHCP** • **NTP** • **SSH** • **DNS** • **ICMP** • **HTTPS** • **OSPF** • **STUN** • **SNMP** • **NETCONF** • **BFD**
Encapsulation	
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
GRE Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0

Field	Description
GRE Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d. Configure NAT.

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

e. Configure ACL/QoS.

f. Configure the advanced parameters.

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

Field	Description
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. **Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface.
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet. When you enable transport tunnel tracking, Cisco Catalyst SD-WAN periodically probes the path to the internet to determine whether it is up. If Cisco Catalyst SD-WAN detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When Cisco Catalyst SD-WAN detects that the path to the internet is again functioning, the route to the internet is reinstalled. Enter the name of a tracker to track the status of transport interfaces that connect to the internet.

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

Step 4 Click **Add New Feature** to create and configure a Cellular Controller feature.

Configure the basic parameters, mostly related to SIMs.

Table 8: Basic Settings

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

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

Step 5 Configure a Cellular Profile feature to associate with the Cellular Controller.

a. Adjacent to the Cellular Controller feature, click + and add a Cellular Profile feature as a subfeature.

b. Configure the basic parameters.

Table 9: Basic Settings

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

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

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

Table 10: Cellular Band Select

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

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

What to do next

Also see Deploy a configuration group.

Configure cellular interfaces using CLI

The following example enables a cellular interface:

Procedure

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

Example:

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

```
exit

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

Configure cellular interfaces using templates

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

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

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

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

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

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

Procedure

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template**.

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

Step 5 Click **VPN Interface Cellular**.

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

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

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

Step 8 Configure cellular interface.

a) Configure basic cellular interface functionality.

Table 11:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface Name*	Enter the name of the interface. It must be **cellular0**.
Description	Enter a description of the cellular interface.
DHCP Helper	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU*	Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value.

b) Configure a tunnel interface on the cellular interface to configure an interface in VPN 0 to be a WAN transport connection. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select **On** and select a color for the interface. You can generally accept the system defaults for the reminder of the tunnel interface settings.

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

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

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

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

Table 12:

Parameter Name	Description
GRE	From the drop-down, select **Global**. Click **On** to use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
GRE Preference	From the drop-down, select **Global**. Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295

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

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

c) Configure the cellular interface as a NAT device.

Table 13:

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

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

Table 14:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65530
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

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

Table 15: Access Lists Parameters

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of an IPv4 access list to packets being received on the interface.
Egress ACL– IPv4	Click **On**, and specify the name of an IPv4 access list to packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of an IPv6 access list to packets being received on the interface.
Egress ACL– IPv6	Click **On**, and specify the name of an IPv6 access list to packets being transmitted on the interface.
Ingress policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Add ARP table entries.

Table 16:

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure other interface properties.

Table 17: Cellular Interfaces Advanced Parameters

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range: 0 through 7
Autonegotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	From the drop-down, select **Global**. Click **On** for IP directed-broadcast. Default: **Off**

Step 9 Click **Save**.

Reset the profile configuration of a cellular modem using CLI commands

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

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

Procedure

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

Example:

Routers:

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

Cellular gateways:

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

Troubleshoot LTE modem crash

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

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

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

Before you begin

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

Procedure

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

What to do next

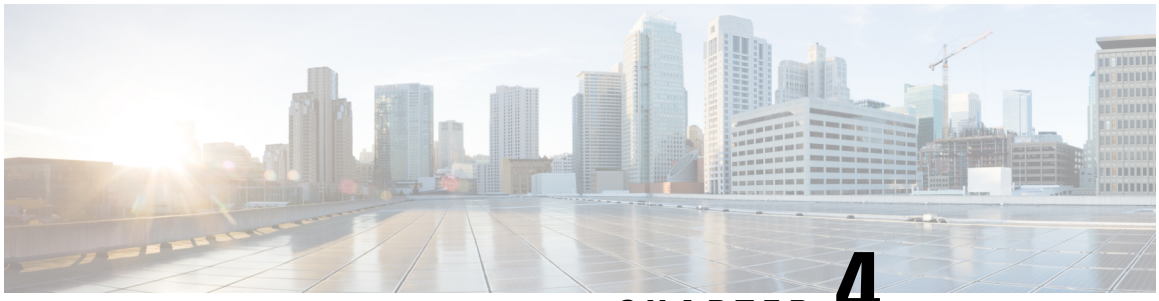
Use the following command to verify the crash-dump progress.

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

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

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

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



CHAPTER 4

DSL IPoE

- Configure DSL IPoE, on page 31

Configure DSL IPoE

Use one of these methods to configure DSL IPoE:

- Configuration group
- Feature template

Configure DSL IPoE using a configuration group

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

Before you begin

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

Procedure

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

Step 2 Create and configure the DSL IPoE parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 18: Basic Configuration

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

Parameter Name	Description
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Enabled by default. Click **No** to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

b. Configure Ethernet.

Table 19: Ethernet

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

c. Configure Tunnel.

Table 20: Tunnel

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub**
Color	Select a color for the TLOC.

Parameter Name	Description
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.

Parameter Name	Description
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds. The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to enable or disable the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable atleast one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d. Configure NAT.

Table 21: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minute

Parameter Name	Description
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

e. Configure QoS.

Table 22: QoS

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

f. Configure ACL.

Table 23: ACL

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

g. Configure advanced parameters.

Table 24: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

What to do next

Also see *Deploy a configuration group*.

Configure DSL IPoE using templates

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

You configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager templates:

1. Create a VPN Interface DSL IPoE feature template to configure IP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Procedure

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

Step 2 Click **Device Templates**, and click **Create Template**.

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

a) From the **Create Template** drop-down list, choose **From Feature Template**.
b) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
c) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
d) Under **Additional VPN 0 Templates**, click **VPN Interface DSL IPoE**.
e) From the **VPN Interface DSL IPoE** drop-down list, choose **Create Template**. The **VPN Interface DSL IPoE** template form is displayed.

This form contains fields for naming the template, fields for defining the IPoE Interface parameters. 

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

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

Step 3 Configure the basic IPoE functionality.

Table 25:

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

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • Auto—Default mode. • ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed.
SRA	Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

Step 4 Configure an Ethernet interface on the VDSL controller.

Table 26:

Parameter Name	Description
Ethernet Interface Name	Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Description	Enter a description for the interface.
Dynamic/Static	Assign a dynamic or static IPv4 address to the Ethernet interface.
IPv4 Address	Enter the static IPv4 address of the Ethernet interface.
DHCP Helper	Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.

Step 5 Configure a tunnel interface for the multilink interface.

Table 27:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.x Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 10 msec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8. Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.

Parameter Name	Description
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8. Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.x Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.x, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None

Parameter Name	Description
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Choose **On** or **Off** for each service to allow or disallow the service on the interface.

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

Table 28:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.

Parameter Name	Description
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds

Step 6 Configure an interface to act as a NAT device for applications such as port forwarding.

Table 29:

Parameter Name	Description
NAT	Click **On** to have the interface act as a NAT device.
Refresh Mode	Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minutes

TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)
Block ICMP	Select **On** to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
Respond to Ping	Select **On** to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

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

Table 30:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

Step 7 Configure ACLs to selectively indicate what traffic will enjoy the benefits of QoS

Table 31:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.

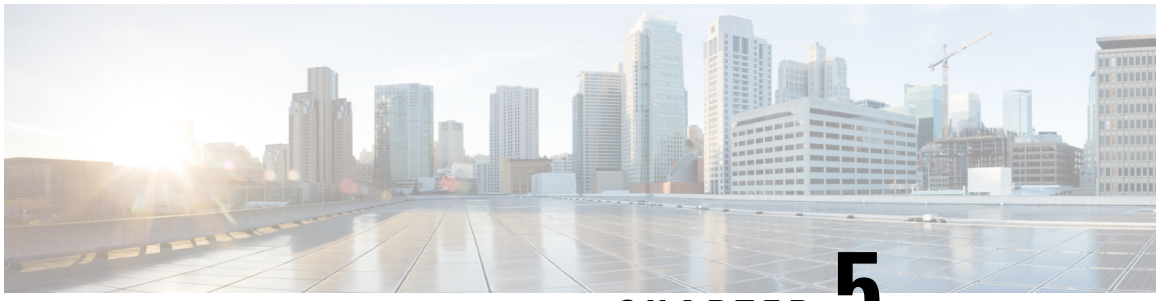
Parameter Name	Description
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL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

Step 8 Configure other interface properties.

Table 32:

Parameter Name	Description
Bandwidth Upstream	When the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Uptream issues notifications. For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	When the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager NMSs only), BW Downtream issues notifications. For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	IP MTU affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented. Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

Parameter Name	Description
TCP MSS	In a single TCP/IPv4 datagram, the TCP Maximum Segment Size (MSS) defines the maximum data that a host will accept. This TCP/IPv4 datagram might be fragmented at the IPv4 layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
TLOC Extension	Use a TLOC Extension to bind an interface and connect another Cisco IOS XE Catalyst SD-WAN device at the same physical site to the local router's WAN transport interface (on Cisco IOS XE Catalyst SD-WAN devices only). Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet. When you enable transport tunnel tracking, the software periodically probes the path to the internet to determine whether it is up. If the software detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When the software detects that the path to the internet is again functioning, the route to the internet is reinstalled. Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.



CHAPTER 5

DSL PPPoA

- Configure DSL PPPoA, on page 49

Configure DSL PPPoA

Use one of these methods to configure DSL PPPoA:

- Configuration group
- Feature template

Configure DSL PPPoA using a configuration group

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

Before you begin

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

Procedure

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

Step 2 Create and configure the DSL PPPoA parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 33: Basic Configuration

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

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

b. Configure ATM.

Table 34: ATM

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

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

c. Configure PPP.

Table 35: PPP

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

d. Configure Tunnel.

Table 36: Tunnel

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub** If you select hub topology, the following option appears: • **Bandwidth Percentage**: Enter a value for the bandwidth percentage. Default: 50
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet containing an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes

Parameter Name	Description
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on a tunnel interface Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global** and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*

Parameter Name	Description
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to anable or disable the service on the cellular interface.

Parameter Name	Description
Encapsulation	
Encapsulation	Enable at least one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

e. Configure NAT.

Table 37: NAT

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

f. Configure QoS.

Table 38: QoS

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

g. Configure ACL.

Table 39: ACL

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

h. Configure advanced parameters.

Table 40: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

What to do next

Also see Deploy a configuration group.

Configure DSL PPPoA using templates

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

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

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

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

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

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

Procedure

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

Step 2 Click **Device Templates**.

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

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

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

Step 4 Configure basic VDSL controller functionality in a VPN.

Table 41:

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

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

Step 5 Configure an ATM interface on the VDSL controller.

Table 42:

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

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

Step 6 Configure the PPP authentication protocol.

Table 43:

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

Step 7 Configure a tunnel interface for the multilink interface.

Table 44:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	If the Cisco IOS XE Catalyst SD-WAN device has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC. **Note** For control connection traffic without dropping any data, a minimum of 650-700 kbps bandwidth is recommended with default parameters configured for hello-interval (10) and hello-tolerance (12).
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.

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

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

Table 45:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0

Parameter Name	Description
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second).
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds.

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

Table 46:

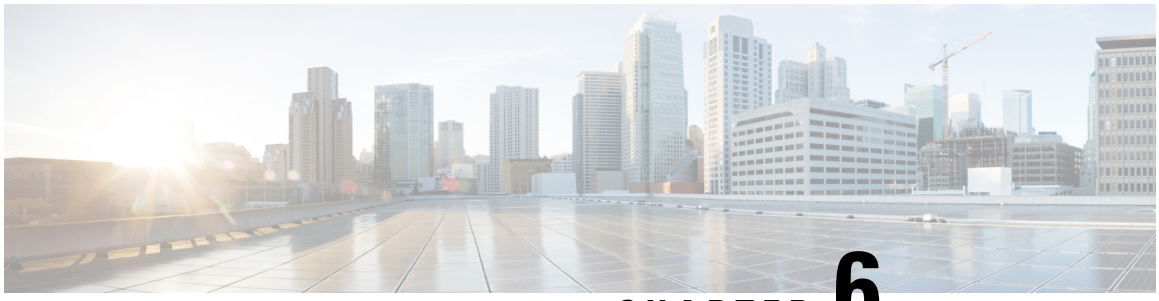
Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

Step 9 Configure other interface properties.

Table 47:

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range:0 through 7
Autonegotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.

Parameter Name	Description
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco IOS XE Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.



CHAPTER 6

DSL PPPoE

- Feature history for DSL PPPoe, on page 67
- Configure DSL PPPoE, on page 67

Feature history for DSL PPPoe

Table 48: Feature History

Feature Name	Release Information	Description
Support for Dialer Interface in DSL	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.1	This feature enables tracking of a Point-to-Point Protocol (PPP) session over a dialer interface on Cisco IOS XE Catalyst SD-WAN devices. Dialer interface is used in Digital Subscriber Line (DSL) in the deployments of Point-to-Point Protocol over Ethernet (PPPoE), Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA). Dialer interface always stay up irrespective of the PPP session status. This helps to avoid the need for additional configuration such as IP SLA and tracking for routing failover to work while using dialer interfaces. The following command is added to configure dialer down-with-vInterface which brings the dialer interface down when the PPP session goes down.

Configure DSL PPPoE

Use one of these methods to configure DSL PPPoE:

- Configuration group
- Feature template

Configure DSL PPPoE using a configuration group

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

Before you begin

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

Procedure

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

Step 2 Create and configure the DSL PPPoE parameters in a Transport and Management Profile.

a. Configure basic configuration.

Table 49: Basic Configuration

Parameter Name	Description
Controller Slot*	Enter the slot number of the controller, in the following format: *slot*/*subslot*/*port* (for example, 0/2/0)
Controller Mode	Select the operating mode of the DSL controller from the drop-down list: • **ADSL1**: Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**: Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**: Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**: Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**: Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.
SRA	Disabled by default. Enable SRA to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.
Dialer Pool Member*	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b. Configure Ethernet.

Table 50: Ethernet

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

c. Configure PPP.

Table 51: PPP

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

d. Configure Tunnel.

Table 52: Tunnel

Parameter Name	Description
Tunnel Interface	

Parameter Name	Description
Per Tunnel QoS	Enable per tunnel QoS and choose from the following values to configure hub-to-spoke network topologies: • **Spoke** • **Hub**
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.

Parameter Name	Description
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, tthis field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge***slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds

Parameter Name	Description
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable atleast one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

e. Configure NAT.

Table 53: NAT

Parameter Name	Description
UDP Timeout (Minutes)	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minute

Parameter Name	Description
TCP Timeout (Minutes)	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

f. Configure QoS.

Table 54: QoS

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

g. Configure ACL.

Table 55: ACL

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

h. Configure advanced parameters.

Table 56: Advanced

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
PPP Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation. Range: 64 through 1792 bytes
Service Provider	Specify the details of the service provider.
Bandwidth Upstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
Bandwidth Downstream (Kbps)	Specify the bandwidth value to generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds the value.
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500.
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.

What to do next

Also see Deploy a configuration group.

Configure DSL PPPoE using templates

Follow these steps to confgure DSL PPPoE using a feature template.

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

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

Procedure

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

Step 2 Click **Device Templates**.

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

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

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

Step 4 Configure the following VPN Interface DSL PPPoE parameters.

a) Configure basic VDSL controller functionality in a VPN.

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

Table 57:

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

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: • **Auto**—Default mode. • **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps. • **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps. • **ADSL2+**— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps. • **ANSI**—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2. • **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco SD-WAN Manager NMS. If the command is not valid, it is not executed.
SRA	Click **Yes** to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

b) Configure an Ethernet interface on the VDSL controller.

Table 58:

Parameter Name	Description
Ethernet Interface Name	Enter a name for the Ethernet interface, in the format *subslot*/*port* (for example 2/0). You do not need to enter the slot number, because it must always be 0.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Description	Enter a description for the interface.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.
PPP Max Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. Range: 64 through 1792 bytes
Dialer IP	Configure the IP prefix of the dialer interface. This prefix is that of the node in the destination that the interface calls. • Negotiated—Use the address that is obtained during IPCP negotiation.

c) Configure the PPP authentication protocol.

Table 59:

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

d) Configure a tunnel interface for the multilink interface.

Table 60:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps • STATE—specifies the vdaemon control state. Last Connection—If no control connection on that WAN interface, the uptime of the device is lifted. SPI Time Remaining—countdown to the next change in SPI for IPSec. The countdown starts at half of the rekey time.
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the 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

Parameter Name	Description
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled. Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **On** for each service to allow or disallow the service on the interface.

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

Table 61:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

Parameter Name	Description
NAT Refresh Interval	Enter the interval between NAT refresh packets that are sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds.
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second).
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds.

e) Configure an interface to act as a NAT device for applications such as port forwarding.

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

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

Table 62:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

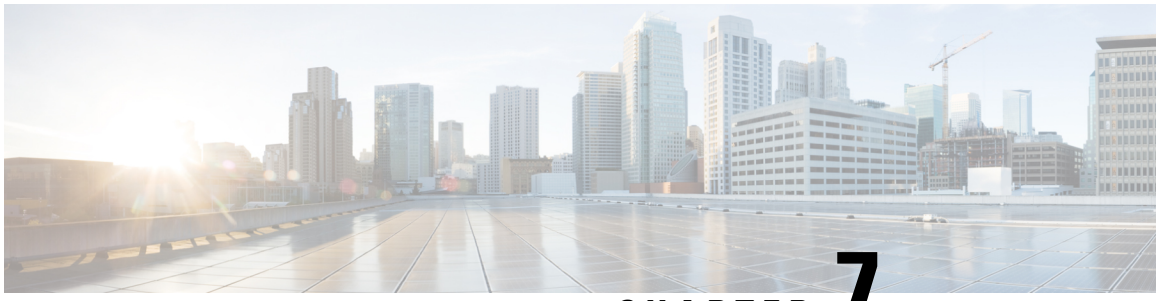
f) Apply a rewrite rule, access lists, and policers to a router interface.

Table 63:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

g) Configure other interface properties.

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804. Default: 1500 bytes.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.



CHAPTER 7

Dynamic Interfaces

- Feature history for dynamic interfaces, on page 85
- Configure dynamic interfaces, on page 85

Feature history for dynamic interfaces

Table 64: Feature History

Feature Name	Release Information	Description
Configuring Dynamic Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.3.2 Cisco vManage Release 20.3.2	This feature allows you to configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time. This feature applies only to the Cisco C8500-12X4QC router.

Configure dynamic interfaces

Configuring dynamic interfaces consists of these general steps:

1. Create a dynamic interface mode feature template. As part of this step, you define modes for the bays in a device.
2. Configure an Interface for Control Connections.
3. Associate the dynamic interface mode feature template with a device template.

You can configure dynamic interfaces for supported devices. A dynamic interface allows a device to select optimum paths in real-time.

When you create a dynamic interface mode feature template, you create a template that defines the modes for the bays in a device.

You can configure the mode for bay 1, bay 2, or both.

The mode for bay 0 is configured automatically and cannot be changed. If you configure the mode for bay 1 as 100G, bay 0 is disabled because the 10G interfaces on bay 0 do not apply in this case.

Procedure

Step 1 Create a dynamic interface mode feature template

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**.

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

c) Click the **Create Template** drop-down list and choose **Feature Template**.

d) From the **Device Model** drop-down list, choose the device for which you wish to create the template.

In **Template Name**, enter a name for the template. This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

In **Description**, enter a description of the template. This field can contain any characters and spaces.

e) From **Additional Templates**, choose the **Dynamic Interface Mode** drop-down list and click **Create Template**.

In **Template Name**, enter a name for the template. This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

In **Description**, enter a description of the template. This field can contain any characters and spaces.

f) Configure the mode for bay 1, bay 2, or both bays by choosing the desired value in the **Bay 1**, **Bay 2**, or both fields.

You cannot change the default value for bay 0.

g) Click Save.

Open a TAC case when there is a mismatch between confd and iosd configurations while changing the bay subslot mode on Cisco C8500-12X4QC router..

Step 2 Configure a new VPN 0 interface for an existing control connection to operate with the bays that you configured in Step 1.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

b) Click **Device Templates**.

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

c) Click **...** of the template for which you want to configure the interface, and then choose **Edit**.

d) Click **Transport & Management VPN** and perform these actions to create interfaces for the bays:

1. Click **VPN Interface** in the **Additional VPN 0** Template.
2. Choose the new **VPN Interface Ethernet** menu that displays, and then click **Create Template**.
3. In **Template Name**, enter a name for the template.

   This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
4. In **Description**, enter a description of the template.

   This field can contain any characters and spaces.

5. Add control connections to the bays that you configured as described in Step 1.

e) Choose **Basic Configuration** and perform these actions:

1. In **Interface Name**, enter a name for the interface.

   Enter a name in the format that this example shows: “FortyGigabitEthernet0/1/0.”

2. Configure other options on this tab as needed.

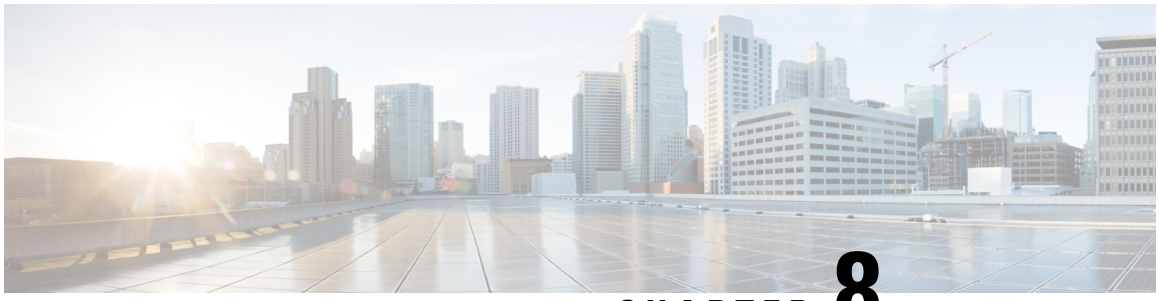
f) From **Tunnel**, set **Tunnel Interface** to **On**.
g) Click Save.
h) Choose **IPv4 Route** and perform these actions to configure an IPv4 route for the VPN0 template:

1. Click **New IPv4 Route**.
2. In **Prefix**, enter a prefix for the IPv4 route.
3. In **Gateway**, choose **Next Hop**.
4. Configure items as needed in **Next Hop**, and then click **Add**.
5. Click **Save**.

i) Click **Update**.

What to do next

After you create the dynamic interface mode feature template, associate it with a device template and attach the device template to a device. For instructions, see *Create a Device Template from Feature Templates*.



CHAPTER 8

EtherChannels

- Feature history for EtherChannels, on page 89
- EtherChannels on the service side, on page 90
- EtherChannels on the service side, on page 90
- EtherChannels on the transport side, on page 98
- Monitor configured EtherChannel using CLI, on page 107
- Aggregate EtherChannel Quality of Service, on page 107

Feature history for EtherChannels

This table describes the developments of the EtherChannels feature, by release.

Table 65: Feature history

Feature Name	Release Information	Description
EtherChannels on the service side	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to configure EtherChannels on Cisco IOS XE Catalyst SD-WAN devices on the service side. EtherChannels provide fault-tolerant, high-speed links, redundancy, and increased bandwidth between Cisco Catalyst SD-WAN devices and other network equipment. You can configure EtherChannels only using the CLI device templates and CLI add-on feature templates.
EtherChannels on the transport side	Cisco IOS XE Catalyst SD-WAN Release 17.13.1aCisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN devices. This feature also enables aggregate EtherChannel Quality of Service (QoS) on the transport side, optimizing network utilization and performance for specific traffic types. **Note** This feature has limited availability.

Feature Name	Release Information	Description
Load balancing for EtherChannels on the transport Side	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature allows you to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices.
Configuration Groups for EtherChannels	Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature allows you to configure EtherChannels on both service and transport sides using configuration groups in Cisco SD-WAN Manager.
Load balancing for EtherChannels on individual port channels	Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco Catalyst SD-WAN Manager Release 20.15.1	With this feature you can load balance EtherChannels for individual port channels on service and transport side using CLI templates.

EtherChannels on the service side

EtherChannels on the service side is a capability that

- extends EtherChannel functionality to the service-facing interfaces of Cisco IOS XE Catalyst SD-WAN device s,
- provides fault-tolerant, high-speed links, redundancy, and increased bandwidth for service-side connections, and
- is configurable through CLI device templates, CLI add-on feature templates, and configuration groups.

EtherChannels on the service side

EtherChannels on the service side is a capability that

- extends EtherChannel functionality to the service-facing interfaces of Cisco IOS XE Catalyst SD-WAN device s,
- provides fault-tolerant, high-speed links, redundancy, and increased bandwidth for service-side connections, and
- is configurable through CLI device templates, CLI add-on feature templates, and configuration groups.

Supported devices for service side EtherChannel

This section provides a list of Cisco platforms that support EtherChannel functionality, including load balancing, on the service side. This information is crucial for planning and deploying Cisco Catalyst SD-WAN solutions that leverage EtherChannels for enhanced bandwidth and redundancy on service-facing interfaces.

The following platforms support EtherChannel and also offer load balancing for EtherChannel on the service side:

- Cisco 4000 Series Integrated Services Routers
  - Cisco 4451-X Integrated Services Router
  - Cisco 4461 Integrated Services Router
  - Cisco 4431 Integrated Services Router
  - Cisco 4331 Integrated Services Router
  - Cisco 4351 Integrated Services Router
- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-X Router
  - Cisco ASR 1006-X Router
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
  - Cisco ASR 1002-X Router
- Cisco Catalyst 8000V Edge Software
- Cisco Catalyst 8200 Router
- Cisco Catalyst 8300 Router
- Cisco Catalyst 8500 Series Edge Router

Supported NIMs

Any L3 Ethernet interface on Network Interface Modules (NIMs) or Service Modules (SMs) can support EtherChannels on the service side.

Note Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.

Prerequisites for EtherChannels on the service side

Before configuring EtherChannels on the service side, ensure that the following prerequisties are met. These prerequisites are essential for your EtherChannel configuration.

- All the LAN ports in each EtherChannel must be of the same speed.
- All the LAN ports must be configured on Layer 3 service-side ports.
- All member interfaces in a port channel must have the same speed and duplex, when using platforms that support multiple rate SFPs on the same port.

Restrictions for EtherChannels on the service side

Maximum port channels

The maximum number of port channel interfaces that a device can support varies, depending on the particular model of the device.

Port channel configuration

You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.

Hardware and interface compatibility

- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the service side.
- The EtherChannel Quality of Service (QoS) feature on port channels is not supported on the service side.
- The Aggregate EtherChannel QoS feature on port channels is not supported on the service side.
- An EtherChannel does not support Digital Signal Processor (DSP) farm services and voice services.
- Sub interfaces cannot be added as member of EtherChannel.

Load balancing for service side EtherChannels using CLI commands

This topic describes the CLI commands and methods for configuring load balancing on service side EtherChannels, including enabling load balancing on individual port channels, configuring global and per-port-channel flow-based hash algorithms, and enabling VLAN load balancing.

The following tasks detail how to configure load balancing options for service side EtherChannels using the CLI commands:

- Enable load balancing on an individual port channel, on page 92
- Enable hash algorithms for flow-based load balancing on a global level, on page 94
- Enable hash algorithms flow-based load balancing on an individual port channel interface, on page 94
- Enable VLAN load balancing per port channel on the service side, on page 95
- Configure load balancing for EtherChannels on the service side using CLI commands, on page 96

Note From Cisco Catalyst SD-WAN Manager Release 20.15.1, you can use any other hash algorithims for load balancing on the service side.

The Hash Algorithms For Flow-based Load Balancing feature is supported only on Cisco Aggregation Services Routers platforms, where the hardware load-balancing for Etherchannel is supported. This command is not supported on Cisco Integrated Services Routers and Cisco Catalyst Router platforms.

Enable load balancing on an individual port channel

Use this procedure to apply load balancing on an individual port channel.

Before you begin

You must be in global configuration mode and have an existing port channel created.

Complete these steps to enable load balancing on an individual port channel.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel channel-number
```

Step 2 Enable load balancing on an individual port channel.

```
load-balancing flow
```

The specified port channel now uses the configured load balancing method, overriding any global settings.

This example shows how to set the load-balancing method to flow, when VLAN-manual method is configured globally:

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# load-balancing flow
```

This example shows how to set the load-balancing method to VLAN:

```
Device# config-transaction
Device(config)# interface port-channel 1
Device(config-if)# load-balancing vlan
```

This example shows a configuration where flow-based load balancing is configured on port channel 2 while the VLAN-manual method is configured globally:

```
port-channel load-balancing vlan-manual
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 load-balancing flow

interface GigabitEthernet2/1/0
 no ip address
 channel-group 2

interface GigabitEthernet2/1/1
 no ip address
 channel-group 2
```

This example shows configuration for VLAN when the load balancing is set to default on the global level:

```
port-channel load-balancing vlan-manual


interface Port-channel1
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0

interface Port-channel1.200
```

```
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0

interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

Note Interface 1 and interface 2 must be member ports of a port channel when **encapsulation dot1q** is configured.

Enable hash algorithms for flow-based load balancing on a global level

Use this procedure to configure a specific hash algorithm for flow-based load balancing globally across all port channels on the device.

Before you begin

Complete these steps to enable hash algorithms for flow-based load balancing on a global level.

Procedure

Configure the desired flow-based hash algorithm globally.

```
port-channel load-balance-hash-algo hash-algo
```

Replace *hash-algo* with one of the following supported hash algorithms:

dst-ip; *dst-macsrc-dst-ipsrc-dst-ipsrc-dst-macsrc-dst-mixed-ip-portsrc-ipsrc-mac*

The selected hash algorithm is now applied globally for flow-based load balancing on all port channels.

This example shows configuration for enabling a hash algorithm on a global level flow-based load balancing:

```
device(config)# port-channel load-balance-hash-algo src-mac
```

Enable hash algorithms flow-based load balancing on an individual port channel interface

Use this procedure to configure a flow-based hash algorithm for load balancing on an individual port channel interface

Before you begin

This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1.

Complete these steps to enable flow-based load balancing on an individual port channel interface.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel
```

Step 2 Enable flow-based load balancing hash algorithm.

```
load-balance-hash-algo hash-algo
```

Replace *hash-algo* with one of the following supported hash algorithms:

dst-ip; *dst-macsrc-dst-ipsrc-dst-ipsrc-dst-macsrc-dst-mixed-ip-portsrc-ipsrc-mac*

The specified port channel interface now uses the configured flow-based load balancing hash algorithm.

This example shows configuration of hash algorithms for flow-based load balancing on an individual port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit
device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit
device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

Enable VLAN load balancing per port channel on the service side

Use this procedure to configure VLAN-based load balancing on a specific EtherChannel port channel on the service side.

Before you begin

Complete these steps to enable VLAN load balancing per port channel on the service side.

Procedure

Step 1 Enter the port channel interface configuration mode.

```
interface Port-channel channel-number
```

Step 2 Enable vlan on per port channel.

```
load-balancing vlan
```

The specified service side port channel is now configured to use VLAN-based load balancing.

This example shows configuration for VLAN load balancing on the service side, when the flow-based load balancing is set to default on the global level:

```
interface Port-channel channel-number
interface GigabitEthernet slot/subslot/port
 channel-group channel-group-number
 interface GigabitEthernet slot/subslot/port
 channel-group channel-group-number
interface Port-channel channel-number
 load-balancing vlan
interface Port-channel channel-number
 encapsulation dot1Q vlan_id primary interface1 secondaryinterface2
```

Note Interface 1 and interface 2 must be member ports of a port channel when **encapsulation dot1q** is configured.

port-channel load-balancing vlan-manual

Note This command is available for configuration in the global configuration mode, and applies to all the port-channel configured on the device.

This example shows how the load-balancing configuration can be globally applied to define policies for handling traffic by using the **port-channel load-balancing** command.

```
port-channel load-balancing vlan-manual

!
interface Port-channel1
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
 secondary GigabitEthernet 1/2/1
 ip address 10.16.2.100 255.255.255.0
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 10.16.3.200 255.255.255.0
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 10.16.4.300 255.255.255.0
 !
interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1
```

Configure load balancing for EtherChannels on the service side using CLI commands

Use this procedure to configure load balancing for EtherChannels on the service side of your Cisco IOS XE Catalyst SD-WAN devices, ensuring efficient traffic distribution across bundled links.

Load balancing optimizes the use of aggregated bandwidth provided by EtherChannels and enhances network performance. You can choose between flow-based or VLAN-based methods and apply configurations globally or on individual port channels, depending on your network requirements.

Before you begin

Complete these steps to configure load balancing for EtherChannels on the service side using CLI commands.

Procedure

Decide on the load balancing method you want to implement, flow-based or VLAN-based:

For flow-based:

- To configure load balancing on a global level or per port channel, seee Enable load balancing on an individual port channel, on page 92.
- To enable a specific hash algorithm for flow-based load balancing across all port channels, see Enable hash algorithms for flow-based load balancing on a global level, on page 94.
- To enable a specific flow-based hash algorithm on an individual port channel interface, see Enable hash algorithms flow-based load balancing on an individual port channel interface, on page 94.

For VLAN-based:

If you choose VLAN-based load balancing, configure it per port channel, see Enable VLAN load balancing per port channel on the service side, on page 95.

Load balancing is now configured for your service side EtherChannels according to your chosen method.

What to do next

Verify your load balancing configuration using the show etherchannel load-balancing command.

Configure a service-side port channel and member link interface using configuration groups

Use this procedure to configure EtherChannel port channels and their member links on the service side using configuration groups within Cisco Catalyst SD-WAN Manager.

Before you begin

Complete these steps to configure a service-side port channel and member link interface using configuration groups in Cisco Catalyst SD-WAN Manager.

Procedure

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

Step 2 Under **Service Profile**, click **Add New** to add a new service profile or select any existing service profiles, and click **Edit**.

Step 3 Select +, and click on the **Ethernet Interface** to add a new interface.

See Ethernet Interface for more details.

Step 4 Select **Add New** from the Ethernet Interface drop-down menu.

Step 5 Under **Basic Configurations**, enter the interface name and description.

Step 6 Click **Ether Channel**, and assign the EtherChannel to a **member interface** or a **port channel** interface from the drop down menu.

Note
If you configure the EtherChannel interface as a port channel, then the default port is LACP. You can assign a different port channel mode using the **Port Channel Mode** option from Cisco SD-WAN Manager.

Note
You can create multiple interfaces which can be either member or port channel interfaces.

Step 7 Click **Save**.

Step 8 Click **Configuration** tab, and deploy the newly created port channels.

A service-side port channel and its member links are configured using configuration groups, ready for deployment to your devices.

What to do next

Monitor the status of the deployed EtherChannels and verify traffic flow on the service side. For more information, see Monitor configured EtherChannel using CLI, on page 107.

EtherChannels on the transport side

EtherChannels on the transport side is a capability that

- extends EtherChannel functionality to the transport-facing interfaces of Cisco IOS XE Catalyst SD-WAN devices
- enables advanced network services like load balancing for aggregated links.
- is configurable through CLI device templates, CLI add-on feature templates, and configuration groups.

Supported devices for transport side EtherChannel

This section provides a comprehensive list of Cisco platforms that support EtherChannel functionality on the transport side. This information is crucial for planning and deploying Cisco Catalyst SD-WAN solutions that leverage EtherChannels for enhanced connectivity and resilience on transport-facing interfaces. It also indicates which platforms support load balancing for these EtherChannels.

The following platforms support EtherChannels, and also offer load balancing for EtherChannels on the service side:

- Cisco 4000 Series Integrated Services Routers
    - Cisco 4461 Integrated Services Router

- Cisco ASR 1000 Series Aggregation Services Routers
  - Cisco ASR 1001-HX Router
  - Cisco ASR 1002-HX Router
- Cisco Catalyst 8200 Series Edge Routers
- Cisco Catalyst 8300 Series Routers
- Cisco Catalyst 8500 Series Edge Routers

Note Starting with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the load balancing configuration command **portchannel load-balance-hash-algo sdwan** is supported only on the Cisco 4461 Integrated Services Router and Cisco Catalyst 8300 Series routers.

Prerequisites for EtherChannels on the transport side

Before configuring EtherChannels on the transport side, ensure that the following prerequisties are met. These prerequisites are essential for your EtherChannel configuration.

- All the member links in each EtherChannel must be of the same speed.
- All the member links must be configured on Layer 3 transport side ports.
- All member interfaces in a portchannel must have the same speed and duplex, when using platforms that support multiple rate SFPs on the same port.

Restrictions for EtherChannels on the transport side

Maximum port channel interfaces

The maximum number of port channel interfaces that a device can support varies depending on the particular model of the device.

Port channel configuration

You can configure EtherChannels on a device by using the CLI, or using only the CLI templates or CLI add-on feature templates in Cisco SD-WAN Manager.

Hardware and platform compatibility

- Network Interface Modules (NIMs) with L2 ports do not support EtherChannels on the transport side.
- The use of port channel on virtual devices such as Cisco Catalyst 8000V is not supported.
- Platforms such as the Cisco Catalyst 8500 Series Edge Routers support multi-rate interfaces, allowing 1G SFP modules to be used in default 10G interfaces. Despite this, in the output of show commands, the interfaces appear as TenGigabitEthernet x/x/x. You can bundle the 1G SFP interfaces together to form a port channel.

Deployment

- In a deployment involving an EtherChannel Link Aggregation Group (LAG) from a Cisco IOS XE Catalyst SD-WAN device to a multichassis LAG (MC-LAG) between two upstream paths, SLA-based Application-Aware Routing (AAR) forwarding can be inaccurate if the traffic load on the two upstream paths is not symmetric.
- Cisco IOS XE Catalyst SD-WAN Release 17.13.1a does not include support for an endpoint tracker on port-channel TLOCs.

Configure a transport side EtherChannels using a CLI template

Use this procedure to create a logical EtherChannel interface on the transport side of a Cisco IOS XE Catalyst SD-WAN device, bundling multiple physical links for increased bandwidth and redundancy.

This procedure describes how to configure EtherChannels on the transport side using CLI templates in Cisco SD-WAN Manager.

In Cisco SD-WAN Manager, you can configure EtherChannels on the transport side using CLI templates.

For more information about using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

.

Note By default, CLI templates execute commands in global config mode.

Before you begin

Complete these steps to configure a transport side EtherChannel using a CLI template.

Procedure

Step 1 Configure a Layer 3 port channel.

```
interface Port-channel channel-number
ip address ip-address mask
ipv6 address ipv6-address/prefix-length
```

Step 2 Assign Interfaces to a Layer 3 port channel with LACP active or passive options.

a.

```
interface GigabitEthernet slot/subslot/port
no ip address
channel-group channel-group-number mode {active passive}
exit
```

b. Configure EtherChannel with LACP Paramaters.

```
lacp system-priority priority
```

```
interface GigabitEthernet slot/subslot/port
lacp port-priority priority
```

c. Configure a static EtherChannel.

```
interface GigabitEthernet slot/subslot/port
no ip address
channel-group channel-group-number
```

Step 3 Configure tunnels.

```
interface Tunnel tunnel-number
ip unnumbered Port-channel channel-group-number
no ip redirects
tunnel source  Port-channel channel-group-number
tunnel mode sdwan

sdwan
 interface Port-channel channel-group-number
  tunnel-interface
   encapsulation {ipsec gre}
   color color-type
```

This example shows how to configure a Layer 3 EtherChannel, and how to assign two ports to channel 1 with the LACP mode as active and passive:

```
interface Port-channel1
ip address 10.48.48.15 255.255.255.0
ip ospf priority 0
ip ospf 65535 area 51
load-interval 30
no negotiation auto

interface GigabitEthernet0/0/0
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active
end

interface GigabitEthernet0/0/4
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode passive
end
```

The following is a configuration example for creating an EtherChannel on the transport side.

```
interface Tunnel2
ip unnumbered Port-channel1
tunnel source Port-channel1
tunnel mode sdwan

interface Port-channel1
  tunnel-interface
```

```
encapsulation ipsec
color lte
```

A transport side EtherChannel is configured and operational, providing aggregated bandwidth and redundancy for your Cisco Catalyst SD-WAN transport connections.

What to do next

Verify the EtherChannel status using CLI commands like **show etherchannel summary** and **show etherchannel load-balancing**.

Configure load balancing for EtherChannels on the Transport Side using CLI Commands

Enable load balancing on individual portchannel interface

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1

Note We recommend using this method to configure load balancing for EtherChannels on the transport side.

1. Enter the port channel interface configuration mode.

   interface Portchannel *channel number*

2. Enable load balancing on an individual port channel.

   load-balance-hash-algo sdwan

Enable load balancing globally for EtherChannels on the Transport Side

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

For more information about using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

Enable load balancing globally for EtherChannels on the transport side.

```
port-channel load-balance-hash-algo sdwan
```

Note In this command, **port-channel load-balance-hash-algo sdwan**, the **sdwan** option was added in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a.

Enable hash algorithms globally for EtherChannels on the Transport Side

1. Configure the algorithm used for load balancing.

   To configure load balancing for IPv4 addresses, which is the default setting, use the following configuration:

```
sdwan
ip load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
```

To configure load balancing for IPv6 addresses, use the following configuration:

```
sdwan
ipv6 load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
```

- **src-dst-ip**: Balances traffic based on both source and destination IP addresses.
- **ip-and-ports**: Balances traffic using a combination of IP addresses and port numbers.
- **src-ip-only**: Balances traffic based solely on the source IP address.

The **ip load-sharing algorithm** command is a global configuration that applies to all Cisco Catalyst SD-WAN tunnels. Changing the algorithm with options such as **src-dst-ip** or **src-dst-mixed-ip-port** affects the load-sharing mechanism for other Cisco Catalyst SD-WAN tunnel traffic as well.

When you configure a port channel on both the service side and the transport side, using the **port-channel load-balance-hash-algo sdwan** command applies load balancing to the transport side. For the Service side, the port channel defaults to the **src-dst-ip** load balancing mode.

To change the load-balancing algorithm for the Service side when a Transport-VPN port-channel is also configured, use the **port-channel load-balance-hash-algo** command. This command allow you to switch from the default **sdwan** mode to alternative modes such as **dst-ip**, **dst-mac**, **src-dst-ip**, **src-dst-mac**, **src-dst-mixed-ip-port**, **src-ip**, or **src-mac**. However, this change disables the SD-WAN-based load balancing for the transport side.

Here's the complete configuration for enabling load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

```
port-channel load-balance-hash-algo sdwan
sdwan
 ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
sdwan
 ipv6 load-sharing algorithm src-dst-ip
```

This example shows configuration enabling load balancing for each port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit

device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit

device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

The following is a sample output to view the configuration for per-interface port channel using **show etherchannel load-balancing** command.

```
device# show etherchannel load-balancing
flow-based
LB Algo type: Source Destination IP

 Port-Channel:                        LB Method
    Port-channel1                  :  flow-based (SDWAN Inner packet LB)
    Port-channel2                  :  flow-based (Source Destination Port, IP addr)
    Port-channel3                  :  flow-based (Source Destination IP)
```

Enable load balancing on individual portchannel interface on the transport side

Use this procedure to enable load balancing on a specific EtherChannel port channel interface on the transport side.

This method is recommended for configuring load balancing on the transport side, providing granular control over traffic distribution for individual port channels. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1.

Before you begin

An EtherChannel port channel must already be configured on the transport side.

Complete these steps to enable load balancing on an individual port channel interface.

Procedure

Step 1 Enter the port channel interface configuration mode.

interface Portchannel *channel number*

Replace *channel number* with the number of your port channel.

Step 2 Enable load balancing on an individual port channel.

load-balance-hash-algo sdwan

The specified transport side port channel interface is now configured for SD-WAN load balancing.

What to do next

Verify the individual port channel load balancing configuration using the **show etherchannel load-balancing** command.

Enable load balancing globally for EtherChannels on the transport side

Use this procedure to enable load balancing globally for all EtherChannels on the transport side of your device.

This configuration applies a default load balancing method to all transport side EtherChannels for which no individual load balancing method is explicitly configured. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Before you begin

Complete these steps to enable load balancing globally for EtherChannels on the transport side.

Procedure

Enable load balancing globally for EtherChannels on the transport side.

```
port-channel load-balance-hash-algo sdwan
```

SD-WAN load balancing is now enabled globally for transport side EtherChannels.

What to do next

Verify the global load balancing configuration using the **show etherchannel load-balancing** command.

Enable hash algorithms globally for EtherChannels on the transport side

Use this procedure to configure specific hash algorithms for IP and IPv6 load balancing globally for EtherChannels on the transport side.

This global configuration applies to all Cisco Catalyst SD-WAN tunnels. Changing these algorithms affects the load-sharing mechanism for other SD-WAN tunnel traffic as well. This feature is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1.

Before you begin

Complete these steps to enable hash algorithms globally for EtherChannels on the transport side.

Procedure

Configure the algorithm used for load balancing.

- To configure load balancing for IPv4 addresses, which is the default setting, use the following configuration:

  ```
  sdwan
  ip load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
  ```

  - **src-dst-ip**: Balances traffic based on both source and destination IP addresses.
  - **ip-and-ports**: Balances traffic using a combination of IP addresses and port numbers.
  - **src-ip-only**: Balances traffic based solely on the source IP address.

- To configure load balancing for IPv6 addresses, use the following configuration:

  ```
  sdwan
  ipv6 load-sharing algorithm {src-dst-ip|ip-and-ports|src-ip-only}
  ```

  The options are the same as for IPv4 load balancing.

The **ip load-sharing algorithm** command is a global configuration that applies to all Cisco Catalyst SD-WAN tunnels. Changing the algorithm with options such as **src-dst-ip** or **src-dst-mixed-ip-port** affects the load-sharing mechanism for other Cisco Catalyst SD-WAN tunnel traffic as well.

When you configure a port channel on both the service side and the transport side, using the **port-channel load-balance-hash-algo sdwan** command applies load balancing to the transport side. For the Service side, the port channel defaults to the **src-dst-ip** load balancing mode.

To change the load-balancing algorithm for the Service side when a Transport-VPN port-channel is also configured, use the **port-channel load-balance-hash-algo** command. This command allow you to switch from the default **sdwan** mode to alternative modes such as **dst-ip**, **dst-mac**, **src-dst-ip**, **src-dst-mac**, **src-dst-mixed-ip-port**, **src-ip**, or **src-mac**. However, this change disables the SD-WAN-based load balancing for the transport side.

Here's the complete configuration for enabling load balancing and apply the desired hash algorithm for traffic distribution on the transport side of Cisco IOS XE Catalyst SD-WAN devices.

```
port-channel load-balance-hash-algo sdwan
sdwan
 ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
sdwan
 ipv6 load-sharing algorithm src-dst-ip
```

This example shows configuration enabling load balancing for each port channel interface. When **sdwan** hash algorithm is configured on the transport side, you can enable different hash algorithm options on the service side.

```
device(config)# interface Port-channel 1
device(config-if)# load-balance-hash-algo sdwan
device(config-if)# exit

device(config)# interface Port-channel 2
device(config-if)# load-balance-hash-algo src-dst-mixed-ip-port
device(config-if)# exit

device(config)# interface Port-channel 3
device(config-if)# no shut
device(config-if)# commit
device(config-if)# end
```

The following is a sample output to view the configuration for per-interface port channel using **show etherchannel load-balancing** command.

```
device# show etherchannel load-balancing
flow-based
LB Algo type: Source Destination IP

 Port-Channel:                       LB Method
    Port-channel1                  :  flow-based (SDWAN Inner packet LB)
    Port-channel2                  :  flow-based (Source Destination Port, IP addr)
    Port-channel3                  :  flow-based (Source Destination IP)
```

The specified IPv4 and IPv6 load-sharing algorithms are now applied globally for transport side EtherChannels.

What to do next

Verify the global load balancing configuration using the **show etherchannel load-balancing** command.

Monitor configured EtherChannel using CLI

This section provides CLI commands and their sample outputs for monitoring the status and configuration of EtherChannels. These commands allow you to verify the operational state, member links, and load balancing methods applied to your EtherChannels.

View EtherChannel summary

Use the **show etherchannel summary** command to display a summary of each configured channel group.

```
Device# show etherchannel summary

Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

View EtherChannel load balancing configuration

Use the **show etherchannel load-balancing** command to display the load-balancing method applied to each port channel.

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: flow-based
LB Algo type: SDWAN Inner packet LB

 Port-Channel:                       LB Method
    Port-channel1                   :  flow-based (SDWAN Inner packet LB)
```

Aggregate EtherChannel Quality of Service

The Aggregate EtherChannel Quality of Service (QoS) is a EtherChannel-related feature that

- improves quality of service on a port channel main interface or subinterface,

- effectively manages network parameters such as delay, jitter, bandwidth, and packet loss, and
- allows the application of an aggregate egress-queuing policy-map on the main or sub-interface of a port channel.

The Aggregate EtherChannel QoS facilitates QoS support on the aggregate port channel's main interface on Cisco IOS XE Catalyst SD-WAN device.

Prerequisites for Aggregate EtherChannel Quality of Service

- Identify aggregate port channel interfaces before creating them using the **platform qos port-channel-aggregate** command.
- In a port channel, all member links must be of the same speed.

Restrictions for Aggregate EtherChannel Quality of Service

Aggregate port channel member and interface limits

The aggregate port channel can support four member links and eight aggregate port channel interfaces.

QoS policy application restrictions on aggregate port channels

You can apply a policy map to the aggregate a port channel's main interface or sub-interface only. Member link QoS is not supported.

Limitations of aggregate port channel conversion

You cannot spontaneously convert port channels to and from the aggregate status. You must delete the interface port-channel from the configurations before adding or removing the matching **platform qos port-channel-aggregate** command.

Unsupported QoS applications on port channel member links

QoS applications which are used to manage, prioritize and control the behavior of data transmission over a network are not supported on port channel member links.

QoS policies applied to aggregate port channel main interfaces and port channel sub-interfaces are not supported.

Channel group modification process with aggregate QoS enabled

When you enable aggregate QoS, it is not possible to directly modify a channel group on a member link. To make changes, the old channel group needs to be removed and the new one must be added. First push one template to remove the old member link and port channel configuration, then another template to add the new configuration.

Configure Aggregate EtherChannel Quality of Service using CLI Template

Configure aggregate EtherChannel Quality of Service using a CLI template.

In SD-WAN Manager, you can configure aggregate EtherChannel QoS using the CLI templates to manage bandwidth and prioritize traffic across bundled links.

Before you begin

For more informationabout using CLI templates, see CLI add-on feature templates and CLI templates for Cisco IOS XE Catalyst SD-WAN devices.

Note By default, CLI templates execute commands in global config mode.

Follow these steps to configure aggregate EtherChannel QoS using a CLI template.

Procedure

Step 1 Create the aggregated port channel.

```
platform qos port-channel-aggregate port-channel-number
 interface Port-channel channel-number
 no shutdown
 ip address ip-address mask
```

Step 2 Assign member links to port channel.

```
 interface GigabitEthernet slot/subslot/port
  no negotiation auto
  channel-group channel-group-number mode {active passive}
  exit
```

Step 3 Configure tunnels.

```
 interface Tunnel tunnel-number
  no shutdown
  ip unnumbered port-channel-interface
  tunnel source port-channel-interface
  tunnel mode sdwan

 sdwan
  interfacechannel-group-number
   tunnel-interface
    encapsulation ipsec
    color public-internet
```

Step 4 Configure QoS.

```
 interface channel-group-number
  service-policy output pre-defined qos policy-map
```

Here's the complete configuration example for configuring aggregate EtherChannel QoS.

```
!
class-map match-any Best-Effort
 match qos-group 2
!
class-map match-any Bulk
 match qos-group 3
!
class-map match-any Business
 match qos-group 1
!
class-map match-any Critical
 match qos-group 0
!
policy-map qos_template
 class Critical
  police rate percent 15
  !
  priority level 1
 !
 class Business
  bandwidth remaining percent 55
 !
 class Best-Effort
  bandwidth remaining percent 10
 !
 class Bulk
  bandwidth remaining percent 20
 !
!
policy-map shape_Port-channel1
 class class-default
  service-policy qos_template
  shape average 100000000
 !
!
interface TenGigabitEthernet0/1/6
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface TenGigabitEthernet0/1/7
 no shutdown
 no negotiation auto
 channel-group 1 mode active
 lacp rate fast
exit
interface Port-channel1
 no shutdown
 ip address 10.1.15.15 255.255.255.0
 ipv6 nd ra suppress all
 service-policy output shape_Port-channel1
exit
interface Tunnel1
 no shutdown
 ip unnumbered Port-channel1
 tunnel source Port-channel1
 tunnel mode sdwan
exit
!
sdwan
 interface Port-channel1
  tunnel-interface
   encapsulation ipsec
```

```
  color lte
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  no allow-service bfd
 exit
exit
```

What to do next

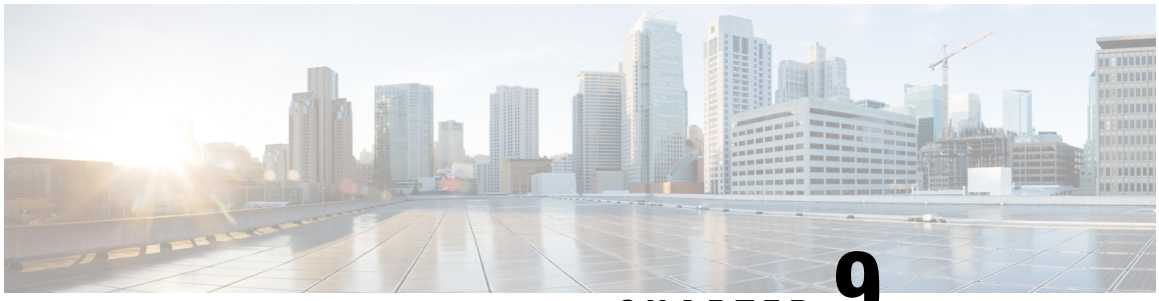
Verify aggregate EtherChannel QoS.

Verify Aggregate EtherChannel Quality of Service

To view QoS issues on a port channel interface, use the **show policy-map interface Port-channel** command.

```
Device# show policy-map interface Port-channel 1
Port-channel1

  Service-policy output: shape_Port-channel1

    Class-map: class-default (match-any)
      121 packets, 20797 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 121/20797
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000

      Service-policy : qos_template

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 121/20797

        Class-map: Critical (match-any)
          121 packets, 20797 bytes
          5 minute offered rate 2000 bps, drop rate 0000 bps
          Match: qos-group 0
          police:
              rate 15 %
              rate 15000000 bps, burst 468750 bytes
            conformed 121 packets, 20797 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 2000 bps, exceeded 0000 bps
```

```
  Priority: Strict, b/w exceed drops: 0

  Priority Level: 1

Class-map: Business (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 1
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 55%

Class-map: Best-Effort (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 2
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 10%

Class-map: Bulk (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 3
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining 20%

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```



CHAPTER 9

IP Directed Broadcast

- IP directed broadcast, on page 113
- Configure IP directed broadcast using CLI commands, on page 113

IP directed broadcast

An IP directed broadcast is a type of IP packet that

- has a destination address that is a valid broadcast address for a specific IP subnet but originates from a node outside that subnet, and
- is forwarded by devices not directly connected to the destination subnet in the same way as unicast IP packets.

The WAN edge device rewrites the destination address in the IP header of the packet to the configured IP broadcast address for the subnet, and then sends the packet as a link-layer broadcast.

Note The access control list (ACL) option for directed broadcast is not supported in Cisco SD-WAN Manager.

Configure IP directed broadcast using CLI commands

Procedure

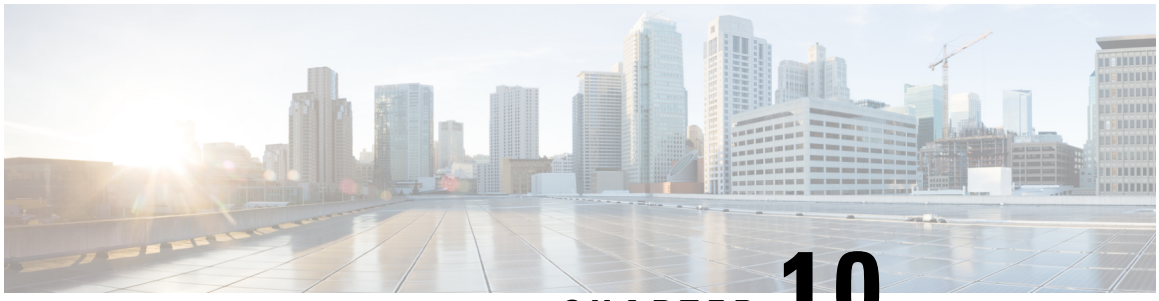
Enable the translation of a directed broadcast to physical broadcasts using the **ip directed-broadcast** command.

Note
If you enable directed broadcast on a network interface, any incoming packet that is a broadcast for that subnet is sent out to all devices on that subnet.

By default, **ip directed-broadcast** is disabled and all IP directed broadcasts are dropped.

Example:

```
device# configure-transaction
device(config)# interface ethernet 2/1
device(config-if)# ip address 10.114.114.1 255.255.255.0
device(config-if)# ip directed-broadcast
device(config-if)# end
```



CHAPTER 10

Loopback Interfaces

- Feature history for loopback interfaces, on page 115
- Loopback interfaces, on page 116
- Implicit ACLs on loopback interfaces, on page 116
- Loopback TLOC interface bound to a physical WAN interface, on page 116
- Loopback TLOC interface not bound to a physical WAN interface, on page 117
- Bind mode and unbind mode, on page 117
- Configure implicit ACL on loopback interfaces using CLI commands, on page 118
- Examples of implicit ACL configurations on loopback interfaces, on page 119
- Verify implicit ACL configurations on loopback interfaces, on page 120

Feature history for loopback interfaces

Table 66: Feature History

Feature Name	Release Information	Description
Implicit ACL on Loopback Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	When a loopback TLOC interface has its own implicit ACL, ACL rules are applied on the traffic destined for the interface. With implicit ACL enabled on the loopback TLOC interface, only limited services can be allowed, thereby enhancing your network security. When a loopback TLOC interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device, the physical interface is treated like a physical TLOC interface.

Loopback interfaces

A loopback interface is a network interface that

- enables data traffic exchange across private WANs such as MPLS or metro Ethernet networks,
- allows routers behind private networks to communicate directly with other edge routers over the private WAN, and
- is configured as a tunnel interface instead of using a physical WAN interface.

Implicit ACLs on loopback interfaces

Implicit ACLs on loopback interfaces are access control mechanism that

- consist of default rules applied to traffic destined for loopback interfaces,
- can be present by default or enabled through configuration to limit or permit traffic, and
- is applied to traffic destined for loopback interfaces configured with a Transport Location (TLOC) in both bind mode (bound to a physical interface) and unbind mode (not bound to any physical interface) on Cisco IOS XE Catalyst SD-WAN devices.

Benefits

Implicit ACL on a loopback TLOC interface protects against denial of service (DoS) attacks by allowing only limited services. This enhances your network security.

Loopback TLOC interface bound to a physical WAN interface

When a loopback interface is a TLOC and is bound to a physical WAN interface, the corresponding implicit ACL rules are applied based on where the traffic is destined:

- If the traffic that is destined to the loopback TLOC interface is received on a physical WAN interface, the implicit ACL rules configured on the loopback TLOC interface is applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured with a TLOC, then routing decisions apply.
  - Forwarded or passthrough packets are dropped when a loopback TLOC interface is bound to a physical WAN interface—the same behavior as when a physical interface is configured as a TLOC. Therefore, an explicit ACL must be configured on the bound physical interface to forward packets.
- An explicit ACL is necessary to allow passthrough packets in the following sample scenarios:
  - Branch edge routers accessing controllers hosted in on-premises data centers: This scenario presumes that the branch edge routers access the controllers through the data center hub, which is configured with a loopback interface bound to a physical WAN interface.

- Branch routers accessing cloud-hosted controllers through data center internet circuits: This scenario presumes that the branch routers are connected to the data center edge using an MPLS network. Such branch routers then access the cloud-hosted controllers through the data canter edge router, which is configured with a loopback interface bound to a physical WAN interface.

- If a physical WAN interface is configured with TLOC, implicit ACL rules of the physical TLOC interface apply. In both these scenarios explicit ACLs on the bound physical WAN interface are necessary to allow passthrough traffic.

Loopback TLOC interface not bound to a physical WAN interface

When a loopback interface is a TLOC, and is not bound to a physical WAN interface, implicit ACL rules are applied based on where the traffic is destined for:

- If the traffic that is destined for the loopback TLOC interface is received on a physical WAN interface, implicit ACL rules of the loopback TLOC are applied.
- If the traffic is not destined for the loopback TLOC interface, depending on whether the input physical WAN interface is configured for TLOC or not, the following rules apply:
  - If the physical WAN interface is not configured for TLOC, then routing decisions apply.
  - If the physical WAN interface is configured for TLOC, the configured implicit ACL rules apply.

Bind mode and unbind mode

The difference between the bind mode and the unbind mode for loopback TLOC is that in a bind mode the passthrough traffic is dropped because the bound physical interface is treated as a TLOC by itself. In an unbind mode, the passthrough traffic is allowed.

Bind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 and Loopback2 configured as TLOCs and bound to the physical interface GigabitEthernet1. The device also has another interface, Loopback3, which is not configured as a TLOC.

Physical interface GigabitEthernet1 will be treated as a TLOC interface for incoming VPN 0.

In this example:

- If the traffic is destined for Loopback1, implicit ACL rules of Loopback1 are applied.
- If the traffic is destined for Loopback2, implicit ACL rules of Loopback2 are applied.
- If the traffic is destined for Loopback3 on GigabitEthernet1, traffic is allowed.
- If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the bound interface, GigabitEthernet1, is also configured as a TLOC, the traffic to Loopback3 will be subjected to implicit ACL rules on GigabitEthernet1.

Unbind mode

A Cisco IOS XE Catalyst SD-WAN device has Loopback1 configured as a TLOC and is in unbind mode. Loopback2 is not configured as a TLOC. The device also has GigabitEthernet1 interface, which is configured as a TLOC, and GigabitEthernet4 interface, which is not configured as a TLOC.

In this example:

- If the traffic destined for Loopback1 arrives at GigabitEthernet1, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied.
- If the traffic destined for Loopback1 arrives at GigabitEthernet4, the Loopback1 implicit ACL rules are applied. If the traffic is destined for GigabitEthernet4, traffic is allowed.
- If the traffic destined for Loopback2 arrives on GigabitEthernet1, the GigabitEthernet1 implicit ACL rules are applied. If the traffic is destined for another device passing through GigabitEthernet1, it is dropped.

If the traffic is destined for another device passing through GigabitEthernet4, the traffic is forwarded.

Configure implicit ACL on loopback interfaces using CLI commands

You can configure implicit ACL on loopback interfaces using a feature template or using a CLI Add-on template in Cisco SD-WAN Manager.

To configure implicit ACL on loopback interfaces using a feature template, see *Configure VPN Ethernet Interface*.

For information on using the CLI Add-On template, see *Create a CLI Add-On Feature Template*.

Procedure

Step 1 Configure a loopback interface that emulates an interface that is always up.

Example:

```
Device(config)# sdwan
Device(config)# interface Loopback100
```

Use the interface name format **loopback** *string*, where *string* can be any alphanumeric value and may include underscores (_) and hyphens (–). The total interface name, including **loopback**, can be up to 16 characters long. Because of the flexibility of interface naming in the CLI, interfaces such as **lo0** and **loopback0** are parsed as different strings and are not interchangeable. For the CLI to recognize an interface as a loopback interface, its name must begin with the full string **loopback**.

Step 2 Configure an interface as a secure transport connection.

Example:

```
Device(config)# tunnel-interface
```

Step 3 Permit or deny a service.

- To permit all the services, use the **allow-service** *all* command.
- To permit a specific service, use the **allow-service** *service name* command.
- To deny a service, use the **no allow-service** *service name* command.

Example:

```
Device(config)# no allow-service bgp
Device(config)# allow-service dhcp
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, configuring the **allow-service** *all* command on Cisco SD-WAN Controller is only applicable for the following services **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**.

Step 4 Enable implicit ACL protection on a physical interface for incoming VPN 0 traffic.

Example:

```
Device(config)# implicit-acl-on-bind-intf
```

Use this command to enable implicit ACL protection on a physical interface in cases where a physical interface is not configured with a TLOC and bound to the loopback TLOC interface.

The following example shows implicit ACL configured on a loopback interface.

```
sdwan interface Loopback100
  tunnel-interface
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

Examples of implicit ACL configurations on loopback interfaces

Configuration Examples for Implicit ACL Configured on a Loopback Interface

Configuration Examples for Implicit ACL Configured on a Loopback Interface in Bind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in bind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
```

```
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Configuration Examples for Implicit ACL Configured on a Loopback Interface in unbind Mode with TLOC Configured

This example shows implicit ACL configured on a loopback interface in unbind mode with TLOC configured:

```
Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

Verify implicit ACL configurations on loopback interfaces

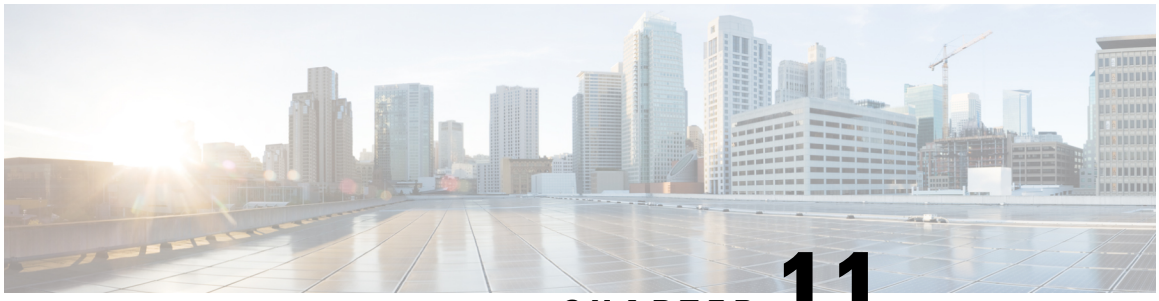
This section provides example for verifing implicit ACL configurations on loopback interfaces

Use the **show platform hardware qfp active statistics drop** command to verify implicit ACL configuration on loopback interfaces. The **show platform hardware qfp active statistics drop** command displays drop statistics that help identify implicit ACL activity on loopback interfaces.

The following is a sample output from the **show platform hardware qfp active statistics drop** command:

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-----------------------------------------------------------------------

Global Drop Stats                          Packets                 Octets
```

```
-------------------------------------------------------------------------------
Disabled                                      4                        266
Ipv4EgressIntfEnforce                        15                      10968
Ipv6NoRoute                                   6                        336
Nat64v6tov4                                   6                        480
SVIInputInvalidMac                          244                      15886
SdwanImplicitAclDrop                        160                      27163
UnconfiguredIpv4Fia                      942525                   58524580
UnconfiguredIpv6Fia                       77521                    9587636
```



CHAPTER 11

Subinterfaces

- Subinterfaces, on page 123
- Configuration examples for subinterfaces, on page 124
- Verify configurations on subinterfaces, on page 124

Subinterfaces

Subinterfaces in Cisco Catalyst SD-WAN are logical interfaces that are configured on a physical interface to enable flexible network segmentation.

Interface speed

Interface speed is the rate at which data is transmitted over a physical or logical interface. When a Cisco IOS XE Catalyst SD-WAN device starts, the Cisco Catalyst SD-WAN software autodetects the SFPs present in the router and sets the interface speed accordingly. The software then negotiates the interface speed with the device at the remote end of the connection to establish the actual operating speed. For non-physical interfaces, such as those used for the system IP address and loopback interfaces, the interface speed defaults to 10 Mbps. In Cisco SD-WAN Controller and Cisco SD-WAN Manager systems, the initial interface speed is 1000 Mbps, with the operating speed negotiated with the remote device. The controller interface speed may vary depending on the virtualization platform, the NIC used, and the drivers present in the software

Interface MTU

MTU (Maximum Transmission Unit) is the largest size, in bytes, of a packet that can be sent on an interface without fragmentation. In Cisco Catalyst SD-WAN, by default, all interfaces have an MTU of 1500 bytes.

Here is the lookup table summarizing the MTU range for Cisco IOS XE Catalyst SD-WAN devices by release and interface type:

Release	Interface Type	MTU Range (bytes)
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier		576 through 2000
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later	1 GE interfaces	576 through 9216
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and later	10 GE and 100 GE interfaces	576 through 9216

For Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers, you can configure interfaces to use ICMP to perform path MTU (PMTU) discovery. When PMTU discovery is enabled, the device automatically negotiates the largest MTU size that the interface supports in an attempt to minimize or eliminate packet fragmentation.

On Cisco IOS XE Catalyst SD-WAN device, the Cisco Catalyst SD-WAN BFD software automatically performs PMTU discovery on each transport connection (that is, for each TLOC, or color). BFD PMTU discovery is enabled by default, and it is recommended that you use it and not disable it.

Note BFD is a data plane protocol and so does not run on Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers.

Configuration examples for subinterfaces

This section provides configuration examples for subinterfaces.

When you create a subinterface that does not specify an IP MTU value, the subinterface inherits the IP MTU value from the parent interface. If you want the subinterface to have a different IP MTU value, use the **ip mtu** command in the subinterface configuration to set the IP MTU for the sub interface.

The following is a configuration example for subinterfaces:

```
interface GigabitEthernet0/0/0
 mtu 1504
 no ip address
!
interface GigabitEthernet0/0/0.9
 encapsulation dot1Q 9
 no shutdown
 ip address 192.168.9.32 255.255.255.0
!
interface Tunnel9
 no shutdown
 ip unnumbered GigabitEthernet0/0/0.9
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0.9
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0.9
 tunnel mode sdwan
!
sdwan
 interface GigabitEthernet0/0/0.9
  tunnel-interface
   encapsulation ipsec
   color private1
  !
 !
```

Verify configurations on subinterfaces

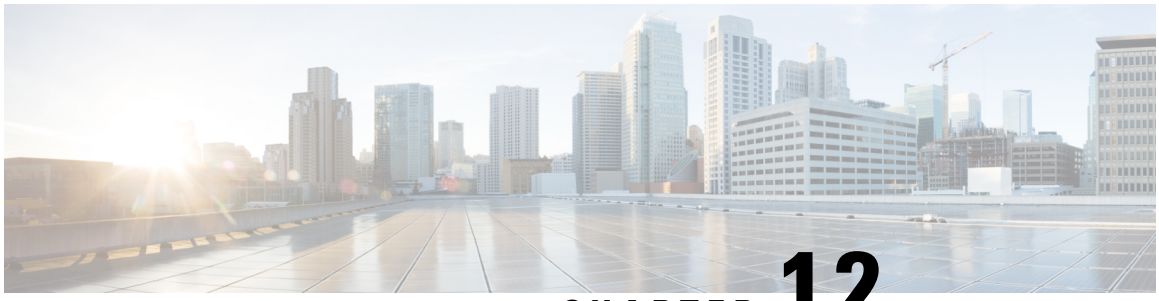
This section provides details on how to verify configurations on subinterfaces.

Configuration example to display information about interface speed and MTU

To display the actual speed of each interface, use the **show interfaces** command. The following example displays interface information on all interfaces.

```
Device# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267c (bia 084f.f99b.267c)
  Description: INET
  Internet address is 10.3.6.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     235182 packets input, 23708237 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 170048 multicast, 0 pause input
     71585 packets output, 12131971 bytes, 0 underruns
     Output 6 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267d (bia 084f.f99b.267d)
  Description: Service
  Internet address is 10.3.13.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     144332 packets input, 13390830 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 144332 multicast, 0 pause input
     13613 packets output, 5135370 bytes, 0 underruns
     Output 1 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
```

```
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
<output truncated>
```



CHAPTER 12

VPN Ethernet Interface

- Configure VPN ethernet interface, on page 127

Configure VPN ethernet interface

Use one of these methods to configure VPN ethernet interface:

- Configuration group
- Feature template

Configure VPN ethernet interface using a configuration group

Follow these steps to configure VPN ethernet interface using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure a Transport VPN feature in Transport and Management profile.

Step 3 Create and configure Ethernet Interface feature in Transport VPN.

a) Configure basic VPN parameters.

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.

Field	Description
Description	Enter a description for the interface.
Auto Detect Bandwidth	Enable this option to automatically detect the bandwidth for WAN interfaces. The device detects the bandwidth by contacting an iPerf3 server to perform a speed test.
IPv4 Settings	Configure an IPv4 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change.
Dynamic DHCP Distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IP Address	Enter a static IPv4 address. This option is available when you choose **Static**.
Subnet Mask	Enter the subnet mask.
Configure Secondary IP Address	Enter up to four secondary IPv4 addresses for a service-side interface. • **IP Address**: Enter the IP address. • **Subnet Mask:** Enter the subnet mask.
DHCP Helper	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BOOTP (broadcast) DHCP requests that it receives from the specified DHCP servers.
IPv6 Settings	Configure an IPv6 VPN interface. • **Dynamic**: Choose **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose **Static** to enter an IP address that doesn't change. • **None**
IPv6 Address Primary	Enter a static IPv6 address. This option is available when you choose **Static**.
Add Secondary Ipv6	
IP Address	Enter up to two secondary IPv6 addresses for a service-side interface.
Bandwidth Upstream	Enter upstream bandwidth reference value.
Bandwidth Downstream	Enter downstream bandwidth reference value.

b) **Apply Access Lists and QoS Parameters**

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

c) Create a tunnel interface.

Field	Description
Tunnel Interface	Enable this option to create a tunnel interface.
Per-tunnel QoS	Enable this option to apply a Quality of Service (QoS) policy on individual tunnels.
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Restrict	Enable this option to limit the remote TLOCs that the local TLOC can establish BFD sessions with. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.
Groups	Enter a group number. Range: 1 through 4294967295
Border	Enable this option to set the TLOC as a border TLOC.
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 100 Default: 2
Validator As Stun Server	Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE Catalyst SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allowed to connect to. Range: 1 through 100

Field	Description
Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Enable port hopping. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). Default: Enabled Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Enable this option to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
Clear-Dont-Fragment	Enable this option to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than the MTU of the interface are fragmented before being sent.
CTS SGT Propagation	Enable CTS SGT propagation on an interface.
Network Broadcast	Enable this option to accept and respond to network-prefix-directed broadcasts.

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

Field	Description
Encapsulation*	Choose an encapsulation type: • **gre**: Use GRE encapsulation on the tunnel interface. • **ipsec**: Use IPsec encapsulation on the tunnel interface. **Note** If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. When you choose **gre**, the following fields appear: • **GRE Preference**: Enter a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 When you choose **ipsec**, the following fields appear: • **IPSEC Preference**: Enter a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPSEC Weight**: Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Multi-Region Fabric **Note** These options appear only when Multi-Region Fabric is enabled.	
Connect to Core Region	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) (Applicable to a border router only) In a Multi-Region Fabric scenario, enable this option to specify how to use the Ethernet interface: • **Share Interface with Access Region**: Share the interface between the access region and core region. • **Keep Exclusive to Core Region**: Use the interface only for the core region.

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

d) Configure an interface as a NAT device.

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

Field	Description

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

Configure New Static NAT	Add a static NAT mapping
Source IP	Enter the source IP address to be translated.
Translate IP	Enter the translated source IP address.
Direction	Choose the direction in which to perform network address translation. • **inside**: Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router. • **outside**: Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device.
Source VPN	Enter the source VPN ID.
IPv6 Settings	
IPv6 NAT	Enable this option to have the interface act as a NAT device.
Select NAT	Choose NAT64 or NAT66. When you choose NAT66, the following fields appear: • **Source Prefix**: Enter the source IPv6 prefix. • **Translated Source Prefix**: Enter the translated source prefix. • **Source VPN ID**: Enter the source VPN ID. • **Egress Interface**: Enable this option to have the interface act as an egress interface.

e) Add ARP table entries.

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.

f) Configure advanced properties.

Field	Description
Duplex	Specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 1518 (GigabitEthernet0), 1500 through 9216 (other GigabitEthernet) Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
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.

Field	Description
Media Type	Specify the physical media connection type on the interface. Choose one of the following: • **auto-select**: A connection is automatically selected. • **rj45**: Specifies an RJ-45 physical connection. • **sfp**: Specifies a small-form factor pluggable (SFP) physical connection for fiber media.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. **Note** TLOC extension over L3 is supported only for Cisco IOS XE Catalyst SD-WAN devices. If configuring TLOC extension over L3 for a Cisco IOS XE Catalyst SD-WAN device, enter the IP address of the L3 interface.
GRE tunnel source IP	Enter the IP address of the extended WAN interface.
XConnect	Enter the name of a physical interface on the same router that connects to the WAN transport.
Load Interval	Enter an interval value for interface load calculation.
IP Directed Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.
ICMP Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

What to do next

Also see *Deploy a Configuration Group*.

Configure prefix list for VRRP using a configuration group

Follow these steps to configure prefix list for VRRP using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure Prefix List for VRRP in a Policy Object Profile.

a) Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
b) Enter the **Prefix List Name**.
c) In the **Internet Protocol** field, click **IPv4** or **IPv6**.
d) Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
e) Click **Save**.

The following table describe the options for configuring the prefix.

Table 67: Prefix List

Field	Description
Prefix List Name	Enter a name for the prefix list.
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

What to do next

Also see *Deploy a configuration group*.

Configure VPN ethernet interface using templates

Follow these steps to configure VPN ethernet interface using feature template.

Procedure

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

Step 2 Click **Device Templates**, and click **Create Template**.

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

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

Step 4 From the **Device Model** drop-down list, choose the type of device for which you are creating the template.

Step 5 To create a template for VPN 0 or VPN 512:

a) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

b) Under **Additional VPN 0 Templates**, click **Cisco VPN Interface Ethernet**.

c) From the **VPN Interface** drop-down list, click **Create Template**. The **Cisco VPN Interface Ethernet** template form displays.

This form contains fields for naming the template, and fields for defining the VPN Interface Ethernet parameters.

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

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

Step 6 Configure the VPN ethernet interface parameters.

a) Configure basic interface functionality in a VPN.

Parameter Name	IPv4 or IPv6	Options	Description
Shutdown*	Click **No** to enable the interface.		
Interface name*	Enter a name for the interface. For Cisco IOS XE Catalyst SD-WAN devices, you must: • Spell out the interface names completely (for example, GigabitEthernet0/0/0). • Configure all the router's interfaces, 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.		
IPv4 / IPv6	Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.		
Dynamic	Click **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.		
	Both	**DHCP Distance**	Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.
	IPv6	**DHCP Rapid Commit**	Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments. Click **On** to enable DHCP rapid commit. Click **Off** to continue using the regular commit process.

Parameter Name	IPv4 or IPv6	Options	Description
Static	Click **Static** to enter an IP address that doesn't change.		
	IPv4	**IPv4 Address**	Enter a static IPv4 address.
	IPv6	**IPv6 Address**	Enter a static IPv6 address.
Secondary IP Address	**IPv4**	Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.	
IPv6 Address	**IPv6**	Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.	
DHCP Helper	**Both**	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.	
Block Non-Source IP	**Yes** / **No**	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic.	

b) Configure a tunnel interface.

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template. Default: Enabled Cisco SD-WAN Manager and Cisco SD-WAN Controller default: Disabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.

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

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

Parameter Name	Description
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds

c) Configure an interface as a NAT device.

For information on how to configure NAT, see the *Cisco Catalyst SD-WAN NAT Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

d) Configure the shaping rate for an interface and apply QoS map, rewrite rules, access lists, and policers to an interface.

Parameter Name	Description
Shaping rate	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS Map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Configure static ARP table entries on the interface.

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure VRRP to allow multiple routers to share a common virtual IP address for default gateway redundancy.

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255

Parameter Name	Description
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers. Range: 100 through 40950 milliseconds Default: 1000 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. Use the 100 msec timer only if the Cisco IOS XE Catalyst SD-WAN device platform supports it, and if there are fewer tunnel groups.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Note** From Cisco Catalyst SD-WAN Manager Release 20.18.1, enabling **Track OMP** changes the device CLI command from **vrrp track omp shutdown** to **vrrp track omp decrement 10**. **Track Prefix List**—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the routers determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.

g) Configure other advanced interface properties.

Parameter Name	Description
Duplex	Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. Default: full
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
PMTU Discovery	Click **On** to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.
Flow Control	Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. Values: autonet, both, egress, ingress, none Default: autoneg
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Speed	Specify the speed of the interface for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, 1000, or 10000 Mbps
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. **Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.

Parameter Name	Description
Autonegotiation	**Note** For releases before Cisco vManage Release 20.6.1, the default value of the field is **On**. To turn autonegotiation off, click **Off**. From Cisco vManage Release 20.6.1, the default behavior of the field is as follows: • For the Gigabit Ethernet interface type, the **Autonegotiation** field is blank by default. However, the autonegotiation is set to **On** when the field is left blank. • For other interface types such as Ten Gigabit Ethernet and Hundred Gigabit Ethernet, the **Autonegotiation** field is blank by default. To turn autonegotiation on or off, click **On** or **Off** respectively. From Cisco SD-WAN Manager Release 20.12.4: In the Cisco Catalyst 8300 Series devices, for the TenGigabitEthernet interface type, do not leave the **Autonegotiation** field blank.
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 that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface.
GRE Tunnel Source IP	Enter the IP address of the extended WAN interface.
Xconnect (on IOS XE routers)	Enter the name of a physical interface on the same router that connects to the WAN transport.

Configure a prefix list for VRRP

Follow these steps to configure a prefix list for VRRP.

Procedure

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

Step 2 Click **Localized Policy**.

From the **Custom Options** drop-down list, click **Lists**.

Step 3 Click **Prefix** from the left pane, and click **New Prefix List**.

Step 4 In **Prefix List Name**, enter a name for the prefix list.

Choose **IPv4** as the **Internet Protocol**.

Step 5 In **Add Prefix**, enter the prefix entries separated by commas.

a) Click **Add**.
b) Click **Next** and configure **Forwarding Classes/QoS**.
c) Click **Next** and configure **Access Control Lists**.
d) Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.
e) From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.
f) Click **Save Match and Actions**.
g) Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.
h) Click **Save Policy**.

Configure a prefix list for VRRP in the device template

Follow these steps to configure the prefix list to the VRRP and the localized policy in the device template.

Procedure

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

Step 2 Click **Device Templates**.

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

Step 3 Select a relevant device template and click **…** and click **Edit** to edit the template details.

Step 4 From **Policy**, select the policy with the newly added prefix list.

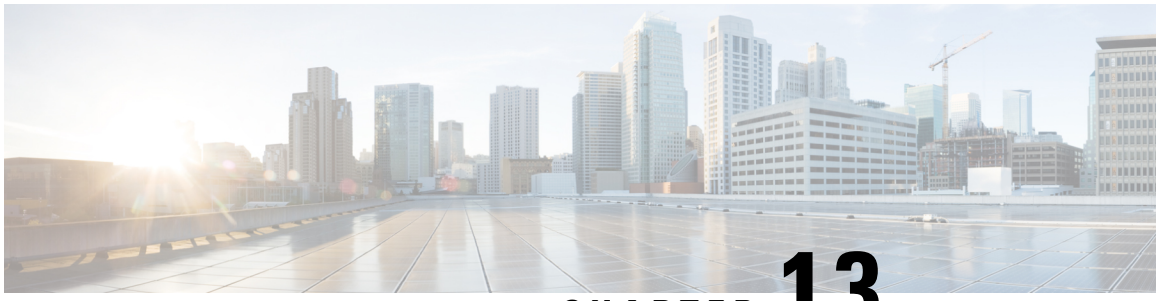
a) Click **Update**.
b) Click **Feature Templates**.
c) Select a relevant device template and click **…** and click **Edit** to edit the template details.
d) Click **VRRP**.
e) Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details.
f) Click the **Track Prefix List** drop-down list and enter the newly added prefix-list name.
g) Click **Save Changes**.

Click **Update** to save the changes.

Step 5 Click **Device Templates** and select the policy with the newly added prefix list.

Step 6 Click **…** and click **Attach Devices**.

Step 7 From **Available Devices**, double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.



CHAPTER 13

VPN Interface Bridge

• Configure VPN interface bridge, on page 147

Configure VPN interface bridge

To configure a bridge interface using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Bridge feature template to configure parameters for logical IRB interfaces.
2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters.

Integrated routing and bridging (IRB) allows Cisco IOS XE Catalyst SD-WAN devices in different bridge domains to communicate with each other. To enable IRB, create logical IRB interfaces to connect a bridge domain to a VPN. The VPN provides the Layer 3 routing services necessary so that traffic can be exchanged between different VLANs. Each bridge domain can have a single IRB interface and can connect to a single VPN, and a single VPN can connect to multiple bridge domains on a Cisco IOS XE Catalyst SD-WAN device.

Procedure

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

Step 2 Click **Device Templates**.

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

a) From the **Create Template** drop-down list, select **From Feature Template**.
b) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
c) Click **Service VPN** or scroll to the **Service VPN** section.
d) Click the **Service VPN** drop-down list.
e) From **Additional VPN Templates**, click **VPN Interface Bridge**.
f) From the **VPN Interface Bridge** drop-down list, click **Create Template**.

The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.

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

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

Step 3 Configure an interface to use for bridging servers.

Table 68:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface name*	Enter the name of the interface, in the format **irb** *number*. The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to.
Description	Enter a description for the interface.
IPv4 Address*	Enter the IPv4 address of the router.
DHCP Helper	Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Block Non-Source IP	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.
Secondary IP Address (on Cisco IOS XE Catalyst SD-WAN devices)	Click **Add** to configure up to four secondary IPv4 addresses for a service-side interface.

Step 4 Apply access lists to IRB interfaces, select the ACL tab and configure the following parameters. The ACL filter determines what is allowed in or out of a bridging domain.

Table 69:

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

Step 5 To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, choose **VRRP**. Then click **Add New VRRP** and configure the following parameters:

Table 70:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255

Parameter Name	Description
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router. Range: 100 through 40950 milliseconds Default: 1000 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface. Use the 100 msec timer only if the Cisco IOS XE Catalyst SD-WAN device platform supports it, and if there are fewer tunnel groups.
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN devices determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.

Step 6 Configure static Address Resolution Protocol (ARP) table entries on the interface.

Table 71:

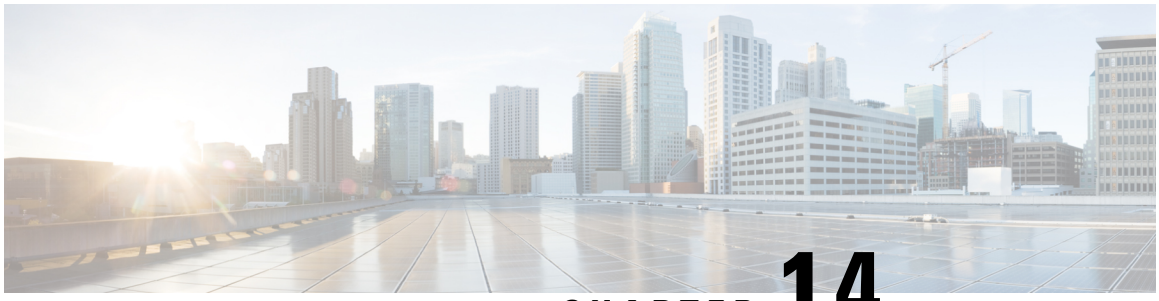
Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

Step 7 Configure other interface properties.

Table 72:

Parameter Name	Description
MAC Address	MAC addresses can be static or dynamic. A static MAC address is manually configured as opposed to a dynamic MAC address that is one learned via an ARP request. You can configure a static MAC on a router's interface or indicate a static MAC that identifies a router's interface. Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Similar to MTU, IP MTU only affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented. Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
TCP MSS	TCP MSS will affect any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS will be examined against the MSS exchanged in the three-way handshake. The MSS in the header will be lowered if the configured setting is lower than what is in the header. If the header value is already lower, it will flow through unmodified. The end hosts will use the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set it at 40 bytes lower than the minimum path MTU. Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure Clear-Dont-Fragment if there are packets arriving on an interface with the DF bit set. If these packets are larger than the MTU will allow, they are dropped. If you clear the df-bit, the packets will be fragmented and sent. Click **On** to clear the Dont Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent. **Note** Clear-Dont-Fragment clears the DF bit when there is fragmentation needed and the DF bit is set. For packets not requiring fragmentation, the DF bit is not affected.
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 2678400 seconds (744 hours) Default: 1200 seconds (20 minutes)

Parameter Name	Description
ICMP Redirect	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. To disable ICMP redirect messages on the interface, click **Disable**. By default, an interface allows ICMP redirect messages.



CHAPTER 14

VPN Interface Ethernet PPPoE

- Configure VPN interface ethernet PPPoE, on page 153

Configure VPN interface ethernet PPPoE

Use one of these methods to configure VPN interface ethernet PPPoE:

- Configuration group
- Feature template

Configure VPN interface ethernet PPPoE using a configuration group

Follow these steps to configure VPN interface ethernet PPPoE using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure a Ethernet PPPoE feature under Transport VPN in a Transport and Management profile.

a) Configure basic PPPoE functionality.

Parameter Name	Description
Ethernet Interface Name *	Enter the name of an ethernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
Description	Enter a description for the ethernet interface.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.

Parameter Name	Description
Dialer Pool Member *	Enter the number of the dialer pool to which the interface belongs. Range: 1 through 255

b) Configure the PPP Authentication Protocol.

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

c) Configure a tunnel interface for the multilink interface.

Parameter Name	Description
Tunnel Interface	
Per Tunnel QoS	Enable per tunnel QoS and choose **Spoke** to configure the spoke network topology
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Groups	Enter the list of groups in the field.

Parameter Name	Description
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**

Parameter Name	Description
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, the router fragments packets larger than the MTU of the interface before sending the packets. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). To reduce outgoing control packets on a TLOC, it is recommended that on the tunnel interface you set the hello interval to 60000 milliseconds (10 minutes) and the hello tolerance to 600 seconds (10 minutes) and include the **no track-transport disable** regular checking of the DTLS connection between the edge device and the controller. For a tunnel connection between a edge device and any controller device, the tunnel uses the hello interval and tolerance times configured on the edge device. This choice is made to minimize the traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a edge device and a controller device. Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.
Last Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
Allow Services	Click **On** or **Off** for each service to allow or disallow the service on the cellular interface.
Encapsulation	

Parameter Name	Description
Encapsulation	Enable at least one of the following encapsulation methods: • **IPsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **IPsec Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1 • **GRE**: Enter a value to set GRE preference for TLOC. Range: 0 through 4294967295 • **GRE Preference**: From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0 • **GRE Weight**: From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1

d) Configure an interface to act as a NAT device for applications such as port forwarding.

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

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

e) Configure QoS.

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

f) Configure ACL.

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

g) Configure additional tunnel interface parameters.

Parameter Name	Description
Shutdown	Choose **No** to enable the interface.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.
Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP-over-Ethernet negotiation. Range: 64 through 1792 bytes

Parameter Name	Description
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP Directed Broadcast	From the drop-down list, select **Global** to enable IP Directed Broadcast. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.
Tracker / Tracker Group	Enter the name of a tracker or tracker group to track the status of transport interfaces that connect to the internet.

What to do next

Also see Deploy a configuration group.

Configure VPN interface ethernet PPPoE using templates

Follow these steps to configure VPN interface ethernet PPPoE using a feature template.

You configure PPPoE over GigabitEthernet interfaces on Cisco IOS XE routers, to provide PPPoE client support.

Use the PPPoE template for Cisco IOS XE Catalyst SD-WAN devices.

Procedure

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

Step 2 Click **Device Templates**.

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

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

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

Step 4 Configure the following parameters in the VPN interface ethernet PPPoE template.

a) Configure the basic PPPoE functionality.

Table 73:

Parameter Name	Description
Shutdown*	Click **No** to enable the GigabitEthernet interface.
Ethernet Interface Name	Enter the name of a GigabitEthernet interface. For IOS XE routers, you must spell out the interface names completely (for example, **GigabitEthernet0/0/0**).
VLAN ID	VLAN tag of the sub-interface.
Description	Enter a description of the Ethernet-PPPoE-enabled interface.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. Range: 100 to 255.
PPP Maximum Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. Range: 64 through 1792 bytes

b) Configure the PPP Authentication Protocol.

Table 74:

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

c) Configure a tunnel interface for the multilink interface.

Table 75:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
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

Parameter Name	Description
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the 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 the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

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

Table 76:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.

Parameter Name	Description
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface. **Note** Configuring administrative distance values on primary interface routes is not supported.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second)

Parameter Name	Description
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds

d) Configure an interface to act as a NAT device for applications such as port forwarding.

Table 77:

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

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

Table 78:

Parameter Name	Description
Port Start Range	Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535

Parameter Name	Description
Port End Range	Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535
Protocol	Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.
VPN	Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65527
Private IP	Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.

e) Apply a rewrite rule, access lists, and policers to a router interface.

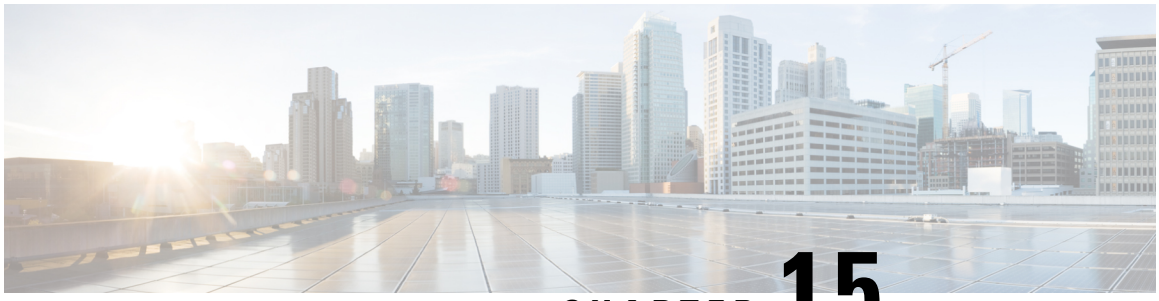
Table 79:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

f) Configure other interface properties.

Table 80:

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804. Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	Enables translation of a directed broadcast to physical broadcasts. 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.



CHAPTER 15

VPN Interface GRE

- Configure VPN interface GRE, on page 169

Configure VPN interface GRE

Use one of these methods to configure VPN interface GRE:

- Configuration group
- Feature template

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

Configure VPN interface GRE on transport VPN using a configuration group

Follow these steps to configure VPN interface GRE on transport VPN using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure the GRE feature.

a) Configure GRE parameters.

Table 81: Basic Configuration

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

b) Configure Tunnel fields.

Table 82: Tunnel

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

c) Configure IKE fields.

Table 83: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

d) Configure IPSEC fields.

Table 84: 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**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 85: 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 TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure GRE on service VPN using a configuration group

Follow these steps to configure GRE on service VPN using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure GRE in Service Profile.

a) Configure Basic Configuration fields.

Table 86: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface, in the format **grenumber**. The value for **number** can be from 1 through 255.
Interface Description	Enter a description of the GRE interface.
Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

b) Configure Tunnel Fields.

Table 87: Tunnel

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

c) Configure IKE fields.

Table 88: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

d) Configure IPSEC fields.

Table 89: IPSEC

Field	Description
IPsec Rekey Interval (Seconds)	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**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 90: 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 IPv4 or IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of the IPv4 TPC SYN packets passing through the Cisco vEdge 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
IPv6 TCP MSS	Specify the maximum segment size (MSS) of the IPv6 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure VPN Interface GRE using templates

Follow these steps to configure VPN interface GRE using a feature template.

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

1. Create a Cisco VPN Interface GRE feature template to configure a GRE interface.
2. Create a Cisco VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters.
3. Create a data policy on the Cisco SD-WAN Controller that applies to the service VPN, including a **set-service** *service-name* **local** command.

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the device to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you can create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

Procedure

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

Step 2 Click **Device Templates**.

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

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

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

Step 4 Configure the following VPN interface GRE parameters:

a) Configure a basic GRE interface.

Table 91:

Parameter Name	Description
Shutdown*	Click **Off** to enable the interface.
Interface Name*	Enter the name of the GRE interface, in the format **gre** *number*. *number* can be from 1 through 255.
Description	Enter a description of the GRE interface.
Source*	Enter the source of the GRE interface: • GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router. This address is on the local router. GRE keepalives can not be configured when source configured as IP address. • Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. GRE keepalives can not be configured when source configured as loopback interface. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.

Parameter Name	Description
Destination*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. If this tunnel connects to a Secure Internet Gateway (SIG), specify the URL for the SIG.
GRE Destination IP Address*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device
IPv4 Address	Enter an IPv4 address for the GRE tunnel.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None

b) Configure access lists on a GRE interface.

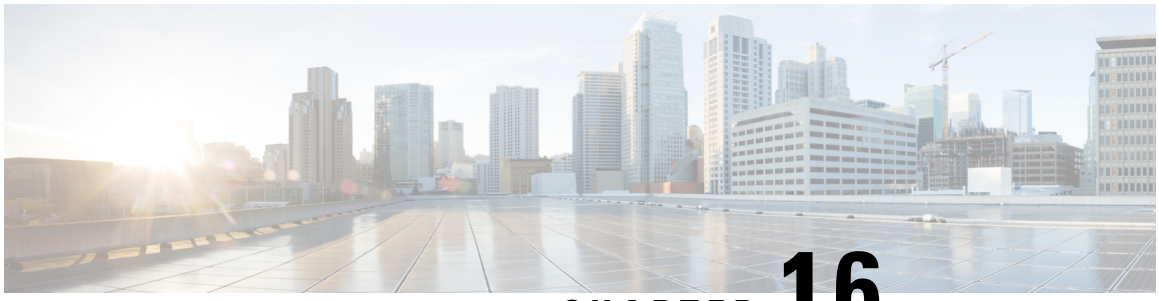
Table 92:

Parameter Name	Description
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.

c) Configure a tracker interface to track the status of a GRE interface.

Table 93:

Parameter Name	Description
Tracker	Enter the name of a tracker to track the status of GRE interfaces that connect to the Internet.



CHAPTER 16

VPN Interface IPsec

- Feature history for VPN interface IPsec, on page 181
- Configure VPN interface IPsec, on page 181
- CLI configuration examples for VPN interface IPsec, on page 196

Feature history for VPN interface IPsec

Table 94: Feature History

Feature Name	Release Information	Description
SHA256 Support for IPSec Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for `HMAC_SHA256` algorithms for enhanced security.

Configure VPN interface IPsec

Use one of these methods to configure geofencing:

- Configuration group
- Feature template

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

Configure IPsec on the transport VPN using a configuration group

Follow these steps to configure IPSEC on the transport VPN using a configuration group.

If...

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

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

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

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

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

Before you begin

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

Procedure

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

Step 2 Create and configure the basic IPSEC.

a) Configure a basic IPsec tunnel interface.

Table 95: Basic Configuration

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

Field	Description
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.
Associated Tracker / Tracker Group	Choose a tracker or a tracker group from the drop-down list to associate with the IPsec tunnel.
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the source IP address of the IPsec tunnel interface. Enter an IPv4 or IPv6 address that is based on your selection in the **Tunnel Mode** option. This address is on the local router. • **Interface**: Enter the physical interface in the **IPsec Source Interface** field, which is the source of the IPsec tunnel.

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

b) Configure Internet Key Exchange fields.

Table 96: Internet Key Exchange

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)

Field	Description
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote endpoint identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you choose IKEv2.

c) Configure IPSEC fields.

Table 97: IPSEC

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

d) Configure advanced IPsec fields.

Table 98: 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
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.

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

What to do next

Also see Deploy a configuration group.

Configure IPsec on the service VPN using a configuration group

Follow these steps to configure IPsec on the service VPN using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure the VPN interface IPsec feature.

a) Configure basic configuration fields.

Table 99: Basic Configuration

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

Field	Description
Tunnel Source	Enter the source of the IPsec interface: • **IP Address**: Enter the IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list.. This address is on the local router. • **Interface**: Enter the physical interface that is the source of the IPsec tunnel.
Tunnel Destination	Enter the destination of the IPsec interface: • **Address**: Enter the destination IPv4 or IPv6 address of the IPsec interface, based on your choice from the **Tunnel Mode** drop-down list. This address is on a remote device. • **Application**: Choose an application from the drop-down list. • None • Sig
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: 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	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

b) Configure IKE fields.

Table 100: Internet Key Exchange

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

Field	Description
IKE Integrity Protocol	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IPsec Rekey Interval (Seconds)	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.

c) Configure IPsec fields.

Table 101: IPSEC

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

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

d) Configure advanced fields.

Table 102: Advanced

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

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv4 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
Shutdown	Click **Off** to enable the interface.

What to do next

Also see Deploy a configuration group.

Configure VPN interface IPsec using templates

Follow these steps to configure VPN interface IPsec using a feature template.

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65527, except for 512.

Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. In Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

In controller mode, only Route based IPSec tunnels are supported.

Procedure

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

Step 2 Click **Feature Templates**.

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

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.

d) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
e) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following VPN interface IPsec parameters:

a) Configure a basic IPsec tunnel interface.

Parameter Name	Options/Format	Description
Shutdown*	**Yes** / **No**	Click **No** to enable the interface; click **Yes** to disable.
Interface Name*	**ipsec** *number* (1…255)	Enter the name of the IPsec interface. *Number* can be from 1 through 255.
Description	Enter a description of the IPsec interface.	
IPv4 Address*	*ipv4-prefix/length*	Enter the IPv4 address of the IPsec interface. The address must have a **/30** subnet.
Source *	Set the source of the IPsec tunnel that is being used for IKE key exchange:	
	IP Address	Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in **VPN 0**.
	Interface	Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in **VPN 0**. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name. **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.

Parameter Name	Options/Format	Description
Destination*	Set the destination of the IPsec tunnel that is being used for IKE key exchange.	
	IPsec Destination IP Address	Enter an IPv4 address that points to the destination.
	TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. *Range:* 552 to 1960 bytes *Default:* None
	IP MTU	Specify the maximum transmission unit (MTU) size of packets on the interface. *Range:* 576 through 2000 *Default:* 1500 bytes

b) Configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable.

Parameter Name	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds Default: Disabled
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. Range: 2 through 60 Default: 3

c) Configure IKE.

When you create an IPsec tunnel on a Cisco IOS XE Catalyst SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

Parameter Name	Options	Description
IKE Version	**1** IKEv1 **2** IKEv2	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. Default: IKEv1 **Note** In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

Parameter Name	Options	Description
IKE Mode	**Aggressive mode** **Main mode**	For IKEv1 only, specify one of the following modes: • Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear. • Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** IKE aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen. Default: Main mode
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 14400 seconds (4 hours)
IKE Cipher Suite	• AES 256 CBC SHA 256 • AES 256 CBC SHA 384 • AES 256 CBC SHA 512 • AES 256 CBC SHA 1 • AES 256 GCM • Nul SHA 256 • Nul SHA 384 • Nul SHA 512 • Nul SHA 1	Specify the type of authentication and encryption to use during IKE key exchange. Default: AES 256 CBC SHA 1

Parameter Name	Options	Description
IKE Diffie-Hellman Group	**2** **14** **15** **16**	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus Default: 4096-bit modulus
IKE Authentication	Configure IKE authentication.	
	Preshared Key	Enter the password to use with the preshared key.
	IKE ID for Local End Point	If the remote IKE peer requires a local end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's source IP address
	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: Tunnel's destination IP address

When you are pushing authentication from Cisco SD-WAN Manager, use the authentication string configured for the source and destination stations in double quotes as special characters are not supported. The string can be up to eight characters long.

d) Configure the IPsec tunnel that carries Internet Key Exchange (IKE) traffic.

Parameter Name	Options	Description
IPsec Rekey Interval	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
IKE Replay Window	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm

Parameter Name	Options	Description
Perfect Forward Secrecy	**2** 1024-bit modulus **14** 2048-bit modulus **15** 3072-bit modulus **16** 4096-bit modulus **none**	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: 1024-bit – group-2 2048-bit – group-14 3072-bit – group-15 4096-bit – group-16 none –disable PFS. *Default*: group-16

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, as part of the security hardening, the weaker ciphers are deprecated. As part of this change, the option to configure Diffie-Hellman (DH) groups 1, 2, and 5 is no longer supported. DH groups are used in IKE to establish session keys and are also available in IPsec as support for perfect forward secrecy.

Change the IKE version from IKEv1 to IKEv2

Follow these steps to change the IKE version.

There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

Procedure

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

Step 2 Click **Feature Templates**, and then click **Add Template**.

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

Step 3 Choose the device for which you are creating the template.

Step 4 Click **Basic Configuration**.

Step 5 Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.

Step 6 Remove the ISAKMP profile from the IPsec profile.

Step 7 Attach the IKEv2 profile with the IPsec profile.

Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

Step 8 Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

You must issue the **shutdown** operations in two separate operations.

CLI configuration examples for VPN interface IPsec

Basic configuration

The following is an example of the basic IPsec tunnel interface configuration.

```
crypto
   interface tunnel ifnum
      no shutdown
      vrf forwarding vrf_id
      ip address ip_address[mask]
      tunnel source wanif_ip
      tunnel mode {ipsec ipv4 | gre ip}
      tunnel destination gateway_ip
      tunnel protection ipsec profile ipsec_profile_name
```

Dead-Peer detection

The following is an example of Internet key exchange (IKE) dead-peer detection (DPD) configuration.

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

IKE

The following is an example of ISAKMP CLI configuration for IKEv1.

```
crypto
   isakmp
      keepalive 60-86400 2-60 {on-demand | periodic}
      policy policy_num
         encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
         hash {sha384 | sha256 | sha}
         authentication pre-share
         group {2 | 14 | 16 | 19 | 20 | 21}
         lifetime 60-86400
      profile ikev1_profile_name
         match identity address ip_address [mask]
         keyring keyring_name
```

The following is an example of IPsec CLI configuration for IKEv1.

```
profile ipsec_profile_name
         set transform-set transform_set_name
         set isakmp-profile ikev1_profile_name
         set security-association
            lifetime {kilobytes disable | seconds 120-2592000}
            replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
         set pfs group {14 | 16 | 19 | 20 | 21}
   keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
   ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
esp-sha256-hmac] mode tunnel
```

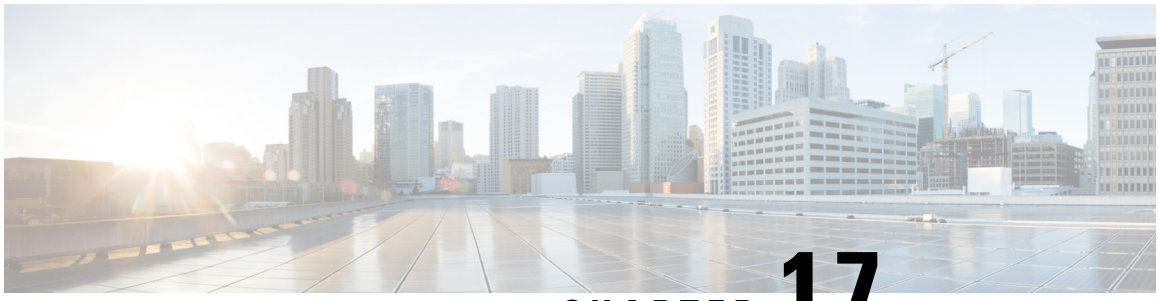
The following is an example configuration for IKE2.

```
crypto
   ikev2
      proposal proposal_name
         encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
         integrity {sha256 | sha384 | sha512}
         group {2 | 14 | 15 | 16}
      keyring idev2_keyring_name
         peer peer_name
         address tunnel_dest_ip [mask]
         pre-shared-key key_string
      profile ikev2_profile_name
         match identity remote address ip_address
         authentication {remote | local} pre-share
         keyring local ikev2_keyring_name
         lifetime 120-86400
```

IPsec tunnel

The following is an example configuration of IPsec tunnels.

```
crypto
   ipsec
      profile ipsec_profile_name
         set ikev2-profile ikev2_profile_name
         set security-association
            lifetime {seconds 120-2592000 | kilobytes disable}
            replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}
         set pfs group {2 | 14 | 15 | 16 | none}
         set transform-set transform_set_name
```



CHAPTER 17

VPN Interface Multilink

- Configure VPN interface multilink, on page 199

Configure VPN interface multilink

Use one of these methods to configure VPN interface multilink:

- Configuration group
- Feature template

Configure VPN interface multilink using a configuration group

Follow these steps to configure VPN interface multilink using a configuration group.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

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

Before you begin

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

Procedure

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

Step 2 Create and configure VPN Interface Multilink in a service profile.

a) Enter the basic configuration information.

Table 103: Basic Configuration

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

Parameter Name	Description
Multilink Group Number *	Enter the number of the multilink group. It must be the same as the number you enter in the multilink interface name parameter. Range: 1 through 65535
PPP Authentication Protocol	Select the authentication protocol used by the multilink interface: • **CHAP**: Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 254 characters. • **PAP**: Enter the username and password provided by your ISP. *username* can be up to 254 characters. • **PAP** and **CHAP**: Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.
Hostname *	Enter hostname for PPP CHAP Authentication.
CHAP Password *	Enter password for PPP CHAP Authentication.
IPv4 Address *	To configure a static address, click **Static** and enter an IPv4 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. Default: 1
Mask	Choose a value for the subnet mask.
IPv6 Address *	To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.

b) Enter multilink information

Table 104: Multilink

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

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

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

c) Enter tunnel information

Table 105: Tunnel

Parameter Name	Description
Color	Choose a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Restrict	Enable this option to drop packets when a tunnel to the service is unreachable.
Groups	Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.

Parameter Name	Description
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Validator As Stun Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100
Cisco SD-WAN Manager Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	From the drop-down list, select **Global**. Click **Off** to allow port hopping on tunnel interface. Default: **On**, which disallows port hopping on tunnel interface Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Click **On** to set the tunnel interface as a low-bandwidth link. Default: **Off**
Network Broadcast	From the drop-down list, select **Global**. Click **On** to accept and respond to network-prefix-directed broadcasts. Enable this parameter only if the **Directed Broadcast** is enabled on the LAN interface feature template. Default: **Off**

Parameter Name	Description
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. To configure TCP MSS, provide a value that is 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes

d) Enter ACL information.

Table 106: 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.

e) Enter advanced information.

Table 107: Advanced

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

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 through 1460 bytes Default: 536
Disable Fragmentation	Click **On** to disable fragmentation for PPP Multilink Protocol data units (PDUs).
Fragment Max Delay	Configure the delay between the transmission of fragments in a PPP Multilink Protocol link. Range: 0 through 1000 Default: No CLI Command
Interleaving Fragments	Enable interleave fragmentation for PPP Multilink Protocol data units (PDUs).
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds the service-side interface to the WAN transport by enabling a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.
IP MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. Range: 576 through 1804 Default: 1500 bytes
IP Directed-Broadcast	Enable the translation of a directed broadcast to physical broadcasts.
Shaping Rate (Kbps)	Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).

What to do next

Also see Deploy a Configuration Group.

Configure VPN interface multilink using templates

Follow these steps to configure VPN interface multilink using a feature template.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

Procedure

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

Step 2 Click **Feature Templates**.

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

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.

e) From the **VPN Interface Multilink Controller** drop-down list, click **Create Template**. The VPN Multilink template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN interface multilink template.

a) Configure a multilink interface.

If you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

Table 108:

Parameter Name	Description
Shutdown*	Click **No** to enable the multilink interface.
Interface Name*	Enter the number of the MLP interface. It can be a number from 1 through 65,535.
Description	Enter a description for the multilink interface.
Multilink Group Number*	Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter.
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. The default DHCP distance is 1.

Parameter Name	Description
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.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. Range: 576 through 1804 Default: 1500 bytes

b) Configure the PPP authentication protocol.

Table 109:

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

c) Configure a tunnel interface for the multilink interface.

Table 110:

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

Parameter Name	Description
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
vBond As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the device is located behind a NAT.
Exclude Controller Group List	Set the Cisco SD-WAN Controller that the tunnel interface is not allowed to connect to. Range: 0 through 100

Parameter Name	Description
vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 8 Default: 5
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Dont Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Dont Fragment bit and the Dont Fragment bit is set. For packets not requiring fragmentation, the Dont Fragment bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

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

Table 111:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295. Default: 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255. Default: 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort. **Note** An interface configured as a circuit of last resort is expected to be down and is skipped while calculating the number of control connections, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

Parameter Name	Description
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds

d) Apply a rewrite rule, access lists, and policers to a router interface.

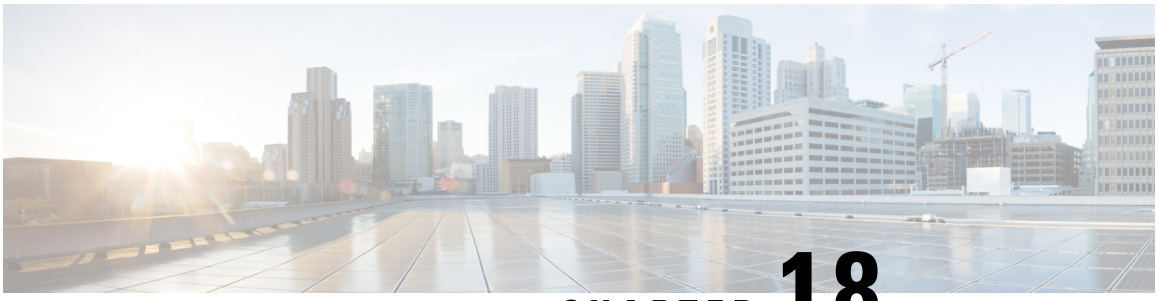
Table 112:

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
QoS map	Specify the name of the QoS map to apply to packets being transmitted out the interface.
Rewrite Rule	Click **On**, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On**, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv6	Click **On**, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

e) Configure other interface properties.

Table 113:

Parameter Name	Description
PMTU Discovery	Click **On** to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None
Clear Dont Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. Range: 0 through 7
Auto negotiate	Click **Off** to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second Cisco Catalyst SD-WAN device at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.



CHAPTER 18

VPN Interface SVI

- Feature history for VPN interface SVI, on page 213
- Configure VPN interface SVI, on page 213

Feature history for VPN interface SVI

Table 114: Feature History

Feature Name	Release Information	Description
Support for Configuring Secondary IP Address	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	You can configure up to four secondary IPv4 or IPv6 addresses, and up to four DHCP helpers. Secondary IP addresses can be useful for forcing unequal load sharing between different interfaces, for increasing the number of IP addresses in a LAN when no more IPs are available from the subnet, and for resolving issues with discontinuous subnets and classful routing protocol.

Configure VPN interface SVI

Use one of these methods to configure VPN interface SVI:

- Configuration group
- Feature template

Configure SVI interface using a configuration group

Follow these steps to configure SVI interface using a configuration group.

Configure a switch virtual interface (SVI) to create a VLAN interface.

Before you begin

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

Procedure

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

Step 2 Create and configure the SVI Interface feature.

a) Configure the SVI Interface feature.

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

b) Configure basic configuration fields.

Table 115: Basic Configuration

Field	Description
Shutdown	Enable or disable the VLAN interface.
VLAN Interface Name*	Enter a name for the VLAN interface. The name must contain a minimum of five characters. The name must be in the following format: `^Vlan(([1-9]\d|\d)/){0,2}(0|[1-9]\d*)([:|\.][1-9]\d*)?`
Interface Description	Enter a description for the interface.
Interface MTU	Enter the maximum transmission unit size for frames received and transmitted on the interface. Range: 1500 through 9216 Default: 1500 bytes
IP MTU	Enter the maximum transmission unit (MTU) size of IP packets sent on an interface. Range: 576 through 9216 Default: 1500 bytes
Configure IPV4 Address	

Field	Description
IPv4 Address Prefix*	Enter the IPv4 address for the interface.
List of DHCP helper addresses*	Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Configure IPV4 Secondary Address	
Secondary IP Address*	Enter up to four secondary IP addresses.
Configure IPV6 Address	
IPV6 address*	Enter the IPv6 address for the interface.
Configure IPV6 Secondary Address	
Address*	Enter up to four secondary IP addresses.
Configure IPV6 DHCP Helper	
Address*	Enter an IP address for DHCP servers in the network to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
VPN	VPN ID for the DHCP helper address.

c) Configure ACL fields.

Table 116: ACL

Field	Description
Configure Access List V4	
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.
Configure Access List V6	
Direction*	Choose a direction of the ACL: **in** or **out**.
Name of ACL*	Enter the name of the access list.

d) Configure VRRP fields.

Table 117: VRRP

Field	Description
Configure VRRP	

Field	Description
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority*	Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router. Range: 1 through 254 Default: 100
Timer*	Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router . Range: 100 through 40950 seconds Default: 100 seconds
Track OMP	When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.
Prefix List*	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.
Add VRRP IP Address Secondary	
Address*	Enter an IP address for the secondary VRRP router.
TLOC Preference Change	Enable or disable this option to set whether the TLOC preference can be changed or not.
Add VRRP Tracking Object	
Tracker Id*	Enter the interface object ID or object group tracker ID.
Track Action*	Choose one of the options: • **decrement** • **shutdown**

Field	Description
Decrement Value	Enter a decrement value. Range: 1-255 From Cisco vManage Release 20.10.1, this option is enabled only when you choose **decrement** in **Track Action**.
Configure VRRP IPv6	
Group ID*	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority*	Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two routers have the same priority, the one with the higher IP address is elected as the primary router. Range: 1 through 254 Default: 100
Timer*	Specify how often the primary VRRP router sends VRRP advertisement messages. If secondary routers miss three consecutive VRRP advertisements, they elect a new primary router . Range: 100 through 40950 seconds Default: 100 seconds
Track OMP*	When you enable this option, VRRP tracks the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.
Track Prefix List	Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the **Track OMP** option. In addition, if the reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
Add VRRP IPv6 Primary	
IPv6 Link Local*	Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Prefix	Enter the IPv6 address of the primary VRRP router.

e) Configure ARP fields.

Table 118: ARP

Field	Description
Configure ARP	
IP Address*	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address*	Enter the MAC address in colon-separated hexadecimal notation.

f) Configure advanced fields.

Table 119: Advanced

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1960 bytes Default: None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)
IP Directed-Broadcast	An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet. A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast. If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.
ICMP/ICMPv6 Redirect Disable	ICMP redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally. The ICMP redirect informs the sending host to forward subsequent packets to that same destination through a different gateway. By default, an interface allows ICMP redirect messages.

What to do next

Also see Deploy a configuration group.

Configure SVI interface using templates

Follow these steps to configure SVI interface using a feature template.

Use the VPN Interface SVI template to configure SVI for Cisco IOS XE Catalyst SD-WAN devices. Configure a switch virtual interface (SVI) to create a VLAN interface.

To configure DSL interfaces on Cisco routers using Cisco SD-WAN Manager templates, create a VPN Interface SVI feature template to configure VLAN interface parameters.

Procedure

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

Step 2 Click **Feature Templates**.

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

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface SVI**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface SVI**.

e) From the **VPN Interface SVI** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN Interface SVI feature template.

To get the SVI interface up and functional, ensure that the appropriate VLAN is explicitly configured on the Switch Port Access or Trunk interface.

a) Configure basic VLAN interface functionality in a VPN.

Table 120:

Parameter Name	Description
Shutdown*	Click **No** to enable the VLAN interface.

Parameter Name	Description
VLAN Interface Name*	Enter the VLAN identifier of the interface. Range: 1 through 1094.
Description	Enter a description for the interface.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1500. Default: 2000 bytes
IPv4* or IPv6	Click to configure one or more IPv4 of IPv6 addresses for the interface. (Beginning with Cisco IOS XE SD-WAN Release 17.2.)
IPv4 Address* IPv6 Address	Enter the IPv4 address for the interface.
Secondary IP Address	Click **Add** to enter up to four secondary IP addresses. (Beginning with Cisco IOS XE SD-WAN Release 17.2.)
DHCP Helper*	Enter up to eight IP addresses for DHCP servers in the network to have the interface be a DHCP helper. Separate each address with a comma. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers. Click **Add** to configure up to four DHCP helpers. (Beginning with Cisco IOS XE SD-WAN Release 17.2, for IPv6.)

b) Apply a rewrite rule, access lists, and policers to a router interface.

Table 121:

Parameter Name	Description
Ingress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress Policer	Click **On** and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click **On** and specify the name of the policer to apply to packets being transmitted on the interface.

c) To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, configure VRRP.

Table 122:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as the primary router. If two Cisco IOS XE Catalyst SD-WAN devices have the same priority, the one with the higher IP address is elected as the primary one. Range: 1 through 254 Default: 100
Timer	Specify how often the primary VRRP router sends VRRP advertisement messages. If the subordinate routers miss three consecutive VRRP advertisements, they elect a new primary router. Range: 1 through 3600 seconds Default: 1 second
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which Cisco IOS XE Catalyst SD-WAN device is the primary virtual router. if a Cisco IOS XE Catalyst SD-WAN device loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: Track OMP—Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE Catalyst SD-WAN device determines the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE Catalyst SD-WAN device and the peer running VRRP.

d) Configure static Address Resolution Protocol (ARP) table entries on the interface.

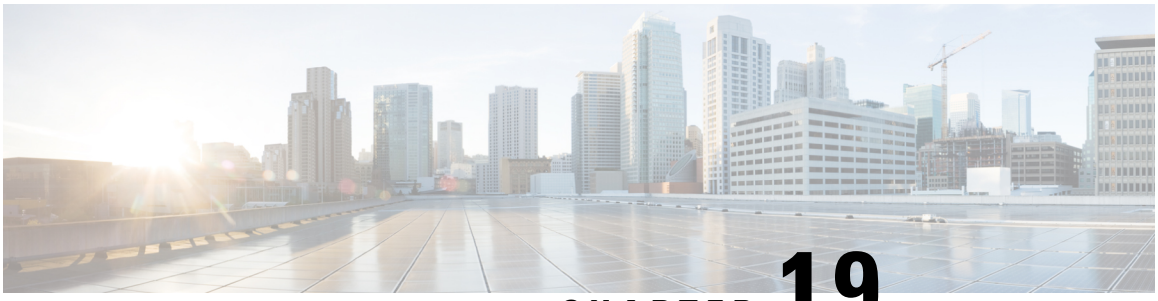
Table 123:

Parameter Name	Description
IP Address	Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.
MAC Address	Enter the MAC address in colon-separated hexadecimal notation.

e) Configure other interface properties.

Table 124:

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)



CHAPTER 19

VPN Interface T1/E1

- Configure VPN interface T1/E1, on page 223

Configure VPN interface T1/E1

Use one of these methods to configure VPN interface T1/E1:

- Configuration group
- Feature template

Configure VPN interface T1/E1 using a configuration group

Follow these steps to configure VPN interface T1/E1 using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure the Transport VPN feature in a Transport and Management Profile.

Step 3 Create and configure the T1 and E1 feature for the VPN interface.

a) Configure the basic VPN settings.

Table 125: Basic Configuration

Parameter Name	Description
Shutdown	Click **No** to enable the interface.

Parameter Name	Description
Interface name*	Enter a name for the interface. The name should be in the following format: **serial** *slot* **/** *subslot* **/** *port* **:** *channel-group* You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
More Settings	
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.
Bandwidth	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Clock Rate	Specify a value for the clock rate. Range: 1200 through 800000
Encapsulation	Choose an encapsulation method for traffic that crosses a WAN link. • **hdlc**: High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **ppp**: Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links.

b) Configure the tunnel parameters.

Table 126: Tunnel

Parameter Name	Description
Tunnel Interface*	From the drop-down list, select **Global**. Click **On** to create a tunnel interface.
Per-tunnel QoS	From the drop-down list, select **Global**. Click **On** to create per-tunnel QoS. You can apply a Quality of Service (QoS) policy on individual tunnels, and is only supported for hub-to-spoke network topologies.
Color	From the drop-down list, select **Global**. Select a color for the TLOC. The color typically used for cellular interface tunnels is **lte**.
Color Description	Enter a description associated to the TLOC color.

Parameter Name	Description
Groups	From the drop-down list, select **Global**. Enter the list of groups in the field.
Border	From the drop-down list, select **Global**. Click **On** to set TLOC as border TLOC.
Maximum Control Connections	Set the maximum number of Cisco SD-WAN Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
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 Control Group List	Set the identifiers of one or more Cisco SD-WAN Controller groups that this tunnel is not allows to establish control connections with. Range: 0 through 100
Manager Connection Preference	Set the preference for using the tunnel to exchange control traffic with Cisco SD-WAN Manager. Range: 0 through 9 Default: 5 If the edge device has two or more cellular interfaces, you can minimize the amount of traffic between Cisco SD-WAN Manager and the cellular interfaces by setting one of the interfaces to be the preferred one to use when sending updates to the Cisco SD-WAN Manager and receiving configurations from the Cisco SD-WAN Manager. To have a tunnel interface never connect to Cisco SD-WAN Manager, set the number to 0. At least one tunnel interface on the edge device must have a nonzero Cisco SD-WAN Manager connection preference.
Port Hop	From the drop-down 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**

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

Parameter Name	Description
Add Encapsulation	From the drop-down list, select **Global** and choose from one of the two encapsulation methods: • **gre**: Enter a value to set GRE preference for TLOC. Range: 0 to 4294967295 • **ipsec**: Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Preference	From the drop-down list, select **Global** and enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0
Weight	From the drop-down list, select **Global** and enter a value to set weight for balancing traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1
Advanced Options	
Carrier	From the drop-down list, select **Global**and select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the following format: **ge** *slot*/*port*.

Parameter Name	Description
Last-Resort Circuit	From the drop-down list, select **Global** and click **On** to use the tunnel interface as the circuit of last resort. By default, it is disabled. **Note** It is assumed that an interface configured as a circuit of last resort is unavailable and is skipped while calculating the number of control connections. As a result, the cellular modem becomes dormant, and no traffic is sent over the circuit. When the configurations are activated on the edge device with cellular interfaces, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down. If the primary interfaces lose their connections to remote edges, the circuit of last resort activates itself, triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are a backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode, the radio interface is turned off, and no control or data connections exist over the cellular interface.
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)

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

c) Configure ACL/QoS parameters.

Table 127: ACL/QoS

Parameter Name	Description
Shaping rate	Configure the aggreate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).
ACL	
Select ACL IPv4 Ingress	Enter the name of an IPv4 access list to packets being received on the interface.
Select ACL IPv4 Egress	Enter the name of an IPv4 access list to packets being transmitted on the interface.
Select ACL IPv6 Ingress	Enter the name of an IPv6 access list to packets being received on the interface.
Select ACL IPv6 Egress	Enter the name of an IPv6 access list to packets being transmitted on the interface.

d) Configure the advanced parameters.

Table 128: Advanced

Parameter Name	Description
TCP MSS	Enter the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 through 1460 bytes Default: 536
MTU	Enter the path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation. Default: 1500
IP MTU	Enter the maximum MTU size of packets on the interface. Range: 576 through 9216 Default: 1500
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration binds this 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.

What to do next

Also see Deploy a configuration group.

Configure T1 or E1 controller using a configuration group

Follow these steps to configure T1 or E1 controller using a configuration group.

Before you begin

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

Procedure

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

Step 2 Create and configure the T1 or E1 network interface module (NIM) parameters in a Transport and Management Profile.

a) Configure a T1 Controller.

Table 129: Configure a T1 Controller

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

b) Configure an E1 Controller.

Table 130: Configure an E1 Controller

Parameter Name	Description
Slot*	Enter the number of the slot in slot/subslot/port format, where the E1 NIM is installed. For example, 0/1/0.
Description	Enter a description for the controller.

Parameter Name	Description
Framing	Enter the E1 frame type: • **crc4**: Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**: Do not use CRC4.
Line Code	Choose the line encoding to use to send E1 frames: • **ami**: Use alternate mark inversion (AMI) as the linecode. • **hdb3**: Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Choose the clock source: • **internal**: Use the controller framer as the primary clock. • **line**: Use phase-locked loop (PLL) on the interface. This is the default.

c) Configure channel group.

Table 131: Channel Group

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

What to do next

Also see Deploy a configuration group.

Configure VPN interface T1/E1 using templates

Follow these steps to configure VPN interface T1/E1 using a feature template.

Use the VPN Interface T1/E1 template for Cisco Catalyst SD-WANs running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.

2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

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

Step 2 Click **Feature Templates**.

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

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

d) If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0), click **Service VPN** or scroll to the **Service VPN** section.

In the Service **VPN** drop-down list, enter the number of the service VPN. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface T1/E1 Serial**.

e) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
f) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
g) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following parameters in the VPN Interface T1/E1 Serial template.

a) Configure basic interface functionality in a VPN.

Table 132:

Parameter Name	Description
Shutdown*	Click **No** to enable the interface.
Interface name*	Enter a name for the interface. The name should be in the format **serial** *slot* / *subslot* / *port* : *channel-group*. You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32} / 2) – 1 kbps
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes

b) Configure a tunnel interface for the multilink interface.

Table 133:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Color Description	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enter a description associated to the TLOC color.

Parameter Name	Description
Control Connection	By default, Control Conection is set to **On**, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click **No** to have the tunnel not establish control connection for the TLOC. **Note** We recommend a minimum of 650-700 Kbps bandwidth with default 1 sec hello-interval and 12 sec hello-tolerance parameters configured to avoid any data/packet loss in connection traffic. For each BFD session, an additional average sized BFD packet of 175 Bytes consumes 1.4 Kbps of bandwidth. A sample calculation of the required bandwidth for bidirectional BFD packet flow is given below: • 650 – 700 Kbps per device for control connections. • 175 Bytes (or 1.4 Kbps) per BFD session on the device (request) • 175 Bytes (or 1.4 Kbps) per BFD session on the device (response) If the path MTU discovery (PMTUD) is enabled, bandwidth for send/receive BFD packets per tunnel for every 30 secs: A 1500 Bytes BFD request packet is sent per tunnel every 30 secs: 1500 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 400 bps (request) A 147 Bytes BFD packet is sent in response: 147 Bytes * 8 bits/1 byte * 1 packet / 30 secs = 40 bps (response) Therefore, a device with 775 BFD sessions (for example) requires a bandwidth of: 700k + (1.4k*775) + (400 *775) + (1.4k*775) + (40 *775) = ~3,5 MBps
Maximum Control Connections	Specify the maximum number of Cisco SD-WAN Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2
Cisco SD-WAN Validator As STUN Server	Click **On** to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the 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 the Cisco SD-WAN Manager NMS. Range: 0 through 8 Default: 5

Parameter Name	Description
Full Port Hop	Minimum release: Cisco Catalyst SD-WAN Manager Release 20.18.1 Enable full port hopping at the TLOC level to allow devices to establish connections with controllers by switching to the next port if the current port is blocked or non-functional. Default: Disabled
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, this field is deprecated. Instead use the **Full Port Hop** option. See the **Full Port Hop** field.
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Tunnel TCP MSS	TCP MSS affects any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS is examined against the MSS exchanged in the three-way handshake. The MSS in the header is lowered if the configured TCP MSS setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, the packets flow through unmodified. The host at the end of the tunnel uses the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set at 40 bytes lower than the minimum path MTU. Specify the MSS of TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has **Dont Fragment** configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the **Dont Fragment** bit in the IPv4 packet header for packets being transmitted out of the interface. When the **Dont Fragment** bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the **Dont Fragment** bit and the **Dont Fragment** bit is set. For packets not requiring fragmentation, the **Dont Fragment** bit is not affected.
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

Configure T1 or E1 controller using templates

Follow these steps to configure T1 or E1 controller using a feature template.

Use the T1/E1 Controller template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco SD-WAN Manager templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters.
3. Create a VPN feature template to configure VPN parameters.

Procedure

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

Step 2 Click **Feature Templates**.

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

a) Click **Add Template**.
b) Choose a Cisco IOS XE Catalyst SD-WAN device from the list.
c) If you are configuring the multilink interface in the transport VPN (VPN 0), click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.

Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface T1/E1**.

d) From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The VPN Interface SVI template form is displayed. This form contains fields for naming the template, and fields for defining multilink Interface parameters.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 3 Configure the following T1 or E1 controller parameters.

a) Configure a T1 controller.

Table 134:

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

Parameter Name	Description
Line Code	Select the line encoding to use to send T1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes. • b8zs—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default. 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.
Line Mode	If you choose the Line clock source, select whether the line is a primary or a secondary line.
Description	Enter a description for the controller.
Channel Group	Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field. Range: 0 through 30
Time Slot	Enter the time slot or time slots that are part of the channel group. Range: 1 through 24
Cable Length	Select the cable length to configure the attenuation • long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet. • short—Set the transmission attenuation for cables that are 660 feet or shorter. There is no default length.

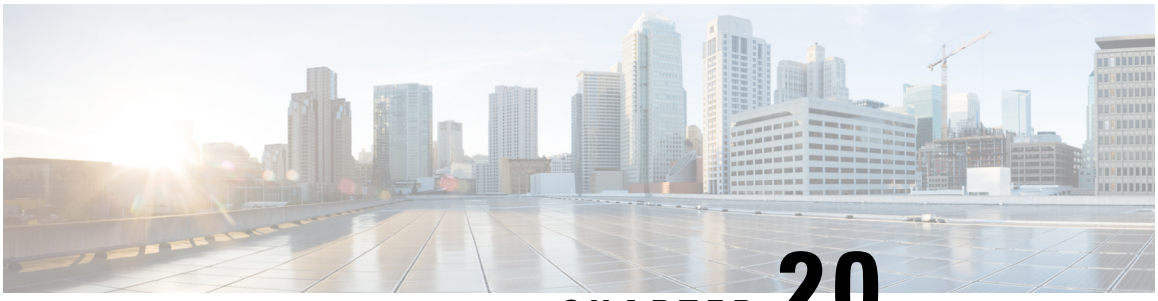
Parameter Name	Description
Length	If you specify a value in the **Cable Length Field**, enter the length of the cable. For short cables, the length values can be: • 110—Length from 0 through 110 feet • 220—Length from 111 through 220 feet • 330—Length from 221 through 330 feet • 440—Length from 331 through 440 feet • 550—Length from 441 through 550 feet • 660—Length from 551 through 660 feet For long cables, the length values can be: • 0 dB • –7.5 dB • –15 dB • –22.5 dB

b) Configure an E1 controller.

Table 135:

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.
Framing*	Enter the E1 frame type: • **crc4**—Use cyclic redundancy check 4 (CRC4). This is the default. • **no-crc4**—Do no use CRC4.
Line Code*	Select the line encoding to use to send E1 frames: • ami—Use alternate mark inversion (AMI) as the linecode. • hdb3—Use high-density bipolar 3 as the linecode. This is the default.
Clock Source	Select the clock source: • internal—Use the controller framer as the primary clock. • line—Use phase-locked loop (PLL) on the interface. This is the default.

Parameter Name	Description
Line Mode	If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line.
Description	Enter a description for the controller.
Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number. Range: 0 through 30
Time Slot	For a channel group, configure the timeslot. Range: 1 through 31



CHAPTER 20

VRRP Interface Tracking

- Feature history for VRRP interface tracking, on page 241
- VRRP, on page 242
- Configure VRRP, on page 243
- VRRP tracking use cases, on page 251
- Restrictions for VRRP interface tracking, on page 252
- Configure VRRP tracking using CLI templates, on page 252
- Configure VRRP tracking, on page 254
- Monitor VRRP configuration, on page 256
- Verify VRRP tracking, on page 257

Feature history for VRRP interface tracking

Table 136: Feature History

Feature Name	Release Information	Description
Support for Multiple VRRP Groups on the Same LAN Interface or Sub-interface	Cisco SD-WAN Release 20.3.1	This feature increases support from one VRRP group per interface to five VRRP groups per interface. Multiple VRRP groups are useful for providing redundancy and for load balancing.

Feature Name	Release Information	Description
VRRP interface tracking for Cisco IOS XE Catalyst SD-WAN devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1	This feature enables VRRP to set the Cisco IOS XE Catalyst SD-WAN device as active or standby based on the WAN Interface or SIG tracker events. It increases the TLOC preference value on a new VRRP active device to ensure traffic symmetry. From this release, you can configure VRRP interface tracking using the Cisco SD-WAN Manager feature template and the CLI template on Cisco IOS XE Catalyst SD-WAN devices.

VRRP

A Virtual Router Redundancy Protocol (VRRP) is a LAN-side protocol that

- provides redundant gateway service for switches and IP end stations,
- allows configuration on interfaces and subinterfaces using templates, and
- supports failover and election of a new primary router based on interface state, OMP session, or remote prefix reachability.

In Cisco Catalyst SD-WAN, VRRP is configured on service-side VPN interfaces or subinterfaces (excluding reserved VPNs 0 and 512), with each group identified by a unique number and assigned an IP address.

The protocol enables up to 512 groups per router, with priority values determining primary router election. Failover can be triggered by interface status, three consecutive advertisements missed, OMP session loss, or loss of prefix reachability, ensuring continuous gateway service.

For VRRP to function with IEEE 802.1Q tagging, MTU adjustments may be necessary.

This is not applicable from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later, where physical and subinterfaces can share the same MTU.

- If the primary VRRP goes down, traffic is redirected to the secondary VRRP, which then becomes the primary gateway.
- VRRP is configured per interface or subinterface within a service-side VPN; reserved VPNs (0, 512) are not supported except for physical interface configuration.
- Each VRRP group requires a unique group number and IP address, with a maximum of 512 groups per router.
- Routers in the same VRRP group act as a single virtual router; the router with the highest priority (1–254, default 100) becomes primary.
- Advertisement messages are sent by the primary every 1–3600 seconds (default: every second).

- The x710 NIC must have the `t->system-> vrrp-advt-with-phymac` command configured, for VRRP to function.

Configure VRRP

- Configure VRRP using Cisco Catalyst SD-WAN Manager
- Configure a prefix list for VRRP using configuration groups
- Configure a prefix list for VRRP using a feature template
- Configure a prefix list for VRRP using a device template
- Configure VRRP using CLI commands

Configuring VRRP using Cisco Catalyst SD-WAN Manager

Procedure

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click **Add New VRRP** and configure the following parameters:

Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. There router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer (milliseconds)	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers. Range: 100 through 40950 milliseconds Default: 100 msecs **Note** When the timer is 100 ms for the VRRP feature template on Cisco IOS XE Catalyst SD-WAN devices, the VRRP fails if the traffic is high on LAN interface.

Parameter Name	Description
Track OMP Track Prefix List	By default, VRRP uses of the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following: **Track OMP**: Click **On** for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the primary VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session. **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, enabling **Track OMP** changes the device CLI command from **vrrp track omp shutdown** to **vrrp track omp decrement 10** . **Track Prefix List**: Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the primary VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to all of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the routers determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.

Configure a prefix list for VRRP using Configuration Groups

Before you begin

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

Procedure

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

Step 2 Create and configure Prefix List for VRRP in a Policy Object Profile.

a) Choose the **Prefix** policy object from the **Select Policy Object** drop-down list.
b) Enter the **Prefix List Name**.
c) In the **Internet Protocol field**, click **IPv4** or **IPv6**.
d) Under **Add Prefix**, enter the prefix for the list. Optionally, click the **Choose a file** link to import a prefix list.
e) Click **Save** The following table describe the options for configuring the prefix.

Table 137: Prefix List

Field	Description
Prefix List Name	Enter a name for the prefix list.

Field	Description
Internet Protocol	Specifies the internet protocol. The options are IPv4 and IPv6.

What to do next

Also see Deploy a configuration group.

Configure a prefix list for VRRP using a feature template

To configure a prefix list,

Procedure

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

Step 2 From the **Custom Options** drop-down list, click **Lists**.

a) Click **Prefix** from the left pane, and click **New Prefix List**.
b) In **Prefix List Name,** enter a name for the prefix list.
c) Choose **IPv4** as the **Internet Protocol**.
d) In **Add Prefix**, enter the prefix entries separated by commas.
e) Click **Add**.

Step 3 Click **Next** and configure **Forwarding Classes/QoS**.

Step 4 Click **Next** and configure **Access Control Lists**.

Step 5 Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.

Step 6 From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.

Step 7 Click **Save Match and Actions**.

Step 8 Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.

Step 9 Click **Save Policy**.

Configure a prefix list for VRRP using a device template

To configure the Prefix List to the VRRP using a device template,

Procedure

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

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

Step 2 Select a relevant device template and click **…**, then click **Edit** to edit the template details.

Step 3 From **Policy**, select the policy with the newly added prefix list and click **Update**.

Step 4 Click **Feature Templates**.

Step 5 Select a relevant device template and click **…** and click **Edit** to edit the template details.

Step 6 Click **VRRP**.

Step 7 Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details and click the **Track Prefix List** drop-down to enter the newly added prefix-list name.

Step 8 Click **Save Changes** and then **Update**. Click **Device Templates** and select the policy with the newly added prefix list.

Step 9 Click **…** and click **Attach Devices**. From **Available Devices,** double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.

Configure VRRP using CLI commands

To provide redundant gateway service on Cisco Catalyst SD-WAN devices by configuring VRRP on service-side interfaces using CLI commands.

Before you begin

- VRRP must be configured on service-side VPNs (not on VPN 0 or 512, except for the physical interface when using subinterfaces).
- Ensure required interfaces and subinterfaces are created and enabled.
- Adjust MTU for 802.1Q tagging if needed (not required for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and later).

Procedure

Step 1 Enter the target VPN .

Example:

```
vpn <vpn-id>
```

Step 2 Select and enable the interface (or subinterface). Select and enable the interface (or subinterface).

Example:

```
interface <irbnumber>[.<subinterface>]
no shutdown
```

Step 3 Assign an IP address to the interface.

Example:

```
ipv4 ip-address
```

Step 4 Within each VRRP group, the router with the higher priority value is elected as primary VRRP. By default, each virtual router IP address has a default primary election priority of 100, so the router with the higher IP address is elected as primary. You can modify the priority value, setting it to a value from 1 through 254.

Example:

```
priority number
```

Step 5 The primary VRRP periodically sends advertisement messages, indicating that it is still operating. If backup routers miss three consecutive VRRP advertisements, they assume that the primary VRRP is down and elect a new primary VRRP. By default, these messages are sent every second. You can change the VRRP advertisement time to be a value from 1 through 3600 seconds.

Example:

```
timer seconds
```

Step 6 By default, VRRP uses the state of the interface on which it is running, to determine which router is the primary virtual router. This interface is on the service (LAN) side of the router. When the interface for the primary VRRP goes down, a new primary VRRP virtual router is elected based on the VRRP priority value. Because VRRP runs on a LAN interface, if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following:

a) Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.

Example:

```
track-omp
```

If all OMP sessions are lost on the primary VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current primary VRRP router. With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. Until the hold timer expires and a new primary VRRP is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as primary VRRP even before it learns and installs OMP routes from the Cisco Catalyst SD-WAN Controllers. Until the routers are learned, traffic is also dropped.

b) Track both the OMP session and a list of remote prefixes. *list-name* is the name of a prefix list configured with the policy lists **prefix-list** command on the Cisco vEdge device :

Example:

```
track-prefix-list list-name
```

If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp**option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the router determines the primary VRRP.

As discussed above, the IEEE 802.1Q protocol adds 4 bytes to each packet's length. Hence, for packets to be transmitted, either increase the MTU size on the physical interface in VPN 0 (the default MTU is 1500 bytes) or decrease the MTU size on the VRRP interface.

For devices running on Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and later, adjusting the MTU size is not required, both the physical interface and sub interface can have the same MTU size.

Here is an example of configuring VRRP on redundant physical interfaces. For subinterface 2, vEdge1 is configured to act as the primary VRRP, and for subinterface 3, vEdge2 acts as the primary VRRP.

```
vEdge1# show running-config vpn 1
vpn 1
```

```
 interface ge0/6.2
  ip address 10.2.2.3/24
  mtu      1496
  no shutdown
  vrrp 2
   ipv4 10.2.2.1
   track-prefix-list vrrp-prefix-list1
  !
 !
 interface ge0/6.3
  ip address 10.2.3.5/24
  mtu      1496
  shutdown
  vrrp 3
   ipv4 10.2.3.11
   track-prefix-list vrrp-prefix-list1
  !
 !
!

vEdge2# show running-config vpn 1
vpn 1
 interface ge0/1.2
  ip address 10.2.2.4/24
  mtu      1496
  no shutdown
  vrrp 2
   ipv4 10.2.2.1
   track-prefix-list vrrp-prefix-list2
  !
 !
 interface ge0/1.3
  ip address 10.2.3.6/24
  mtu      1496
  no shutdown
  vrrp 3
   ipv4 10.2.3.11
   track-prefix-list vrrp-prefix-list2
  !
 !
!

vEdge1# show interface vpn 1

                             IF      IF
           TCP
                            ADMIN   OPER    ENCAP  PORT                              SPEED
          MSS                 RX      TX
VPN   INTERFACE   IP ADDRESS   STATUS  STATUS  TYPE   TYPE     MTU   HWADDR            MBPS
   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
------------------------------------------------------------------------------------------
1     ge0/6.2     10.2.3.3/24  Up      Up      vlan   service  1496  00:0c:29:ab:b7:94  10
   full    0       0:00:05:52  0        357
1     ge0/6.3     10.2.3.5/24  Down    Down    vlan   service  1496  00:0c:29:ab:b7:94  -
   -       0       -           0        0

vEdge1# show vrrp interfaces


 MASTER                              TRACK   PREFIX
              GROUP  VIRTUAL                                  VRRP    OMP    ADVERTISEMENT
 DOWN                                PREFIX  LIST
VPN   IF NAME  ID     IP          VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
 TIMER   LAST STATE CHANGE TIME     LIST    STATE
```

```
1    ge0/6.2  2      10.2.2.1   00:0c:29:ab:b7:94  100       master  down   1
 3       2015-05-01T20:09:37+00:00  -       -
     ge0/6.3  3      10.2.3.11  00:00:00:00:00:00  100       init    down   1
 3       0000-00-00T00:00:00+00:00  -       -
```

In the following example, Router-1 is the primary VRRP, because it has a higher priority value than Router 2:

```
Router-1# show running-config vpn 1
vpn 1
!
 interface ge0/1.15
  ip address 10.10.1.2/24
  mtu         1496
  no shutdown
  vrrp 15
   priority  110
   track-omp
   ipv4 10.20.23.1
  !
 !
!

Router-1# show vrrp vpn 1

      MASTER                              TRACK   PREFIX
               GROUP                                                VRRP    OMP    ADVERTISEMENT
  DOWN                                  PREFIX  LIST
VPN  IF NAME   ID     VIRTUAL IP     VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER
      TIMER   LAST STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
1    ge0/1.1   1      10.20.22.1     00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.5   5      10.20.22.193   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.10  10     10.20.22.225   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:55+00:00  -       -
     ge0/1.15  15     10.20.23.1     00:0c:bd:08:79:a4  110       master  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.20  20     10.20.24.1     00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.25  25     10.20.25.1     00:0c:bd:08:79:a4  110       master  up     1
      3       2016-01-13T03:10:56+00:00  -       -
     ge0/1.30  30     10.20.25.129   00:0c:bd:08:79:a4  100       backup  up     1
      3       2016-01-13T03:10:56+00:00  -       -


Router-1# show vrrp vpn 1 interfaces ge0/1.15 groups 15

                                                                                    MASTER
                        TRACK   PREFIX
GROUP                                          VRRP    OMP    ADVERTISEMENT  DOWN
                        PREFIX  LIST
ID     VIRTUAL IP   VIRTUAL MAC        PRIORITY  STATE   STATE  TIMER          TIMER   LAST
 STATE CHANGE TIME     LIST    STATE
-------------------------------------------------------------------------------------------
1      10.20.33.1  00:0c:bd:08:79:a4  110       master  up     1              3
2016-01-13T03:10:56+00:00  -       -

Router-2# show running-config vpn 1
vpn 1
!
 interface ge0/1.15
```

```
  ip address 10.10.1.3/24
  mtu         1496
  no shutdown
  vrrp 15
   track-omp
   ipv4 10.20.23.1
  !
 !
!

Router-2# show vrrp vpn 1 interfaces groups


 MASTER                              TRACK   PREFIX
          GROUP                                                  VRRP    OMP    ADVERTISEMENT
 DOWN                                PREFIX  LIST
IF NAME    ID     VIRTUAL IP     VIRTUAL MAC         PRIORITY  STATE   STATE  TIMER
 TIMER    LAST STATE CHANGE TIME     LIST    STATE
------------------------------------------------------------------------------------------
ge0/1.1    1      10.20.32.1     00:0c:bd:08:2b:a5  110       master  up     1
 3        2016-01-13T00:22:15+00:00  -       -
ge0/1.5    5      10.20.32.193   00:0c:bd:08:2b:a5  110       master  up     1
 3        2016-01-13T00:22:15+00:00  -       -
ge0/1.10   10     10.20.32.225   00:0c:bd:08:2b:a5  110       master  up     1
 3        2016-01-13T00:22:15+00:00  -       -
ge0/1.15   15     10.20.33.1     00:0c:bd:08:2b:a5  100       backup  up     1
 3        2016-01-13T03:10:56+00:00  -       -
ge0/1.20   20     10.20.34.1     00:0c:bd:08:2b:a5  110       master  up     1
 3        2016-01-13T00:22:16+00:00  -       -
ge0/1.25   25     10.20.35.1     00:0c:bd:08:2b:a5  100       backup  up     1
 3        2016-01-13T03:10:56+00:00  -       -
ge0/1.30   30     10.20.35.129   00:0c:bd:08:2b:a5  100       master  up     1
 3        2016-01-13T00:22:16+00:00  -       -

Router-2# show vrrp vpn 100 interfaces groups 15


MASTER                              TRACK   PREFIX
          GROUP                                                  VRRP    OMP    ADVERTISEMENT
DOWN                                PREFIX  LIST
IF NAME    ID     VIRTUAL IP    VIRTUAL MAC         PRIORITY  STATE   STATE  TIMER
TIMER    LAST STATE CHANGE TIME     LIST    STATE
------------------------------------------------------------------------------------------
ge0/0.15   15     10.20.33.1    00:0c:bd:08:2b:a5  100       backup  up     1              3
        2016-01-13T03:10:56+00:00  -       -
```

Cisco SD-WAN supports configuring multiple VRRP groups on an interface. A use case for configuring this is where primary and secondary IP addresses have been assigned to a single interface. On one interface, you can configure:

- One primary IP address
- Up to four secondary IP addresses

To support each of these IP addresses, you can configure up to 5 VRRP groups (each with a unique group ID) on an interface, subinterface, or integrated routing and bridging (IRB) interface that supports VRRP groups.

The following is an example of configuring 5 VRRP groups on 1 interface.

```
vpn 2
 interface ge0/4.2
  ip address 10.0.1.10/24
```

```
  ip secondary-address 10.0.2.10/24
  ip secondary-address 10.0.3.10/24
  ip secondary-address 10.0.4.10/24
  mtu 1496
  no shutdown
  vrrp 1
   priority 101
    ipv4 10.0.1.1
!
  vrrp 2
   ipv4 10.0.1.2
!
  vrrp 3
   priority 101
    ipv4 10.0.2.1
!
  vrrp 4
   ipv4 10.0.3.1
!
  vrrp 5
   ipv4 10.0.4.1
  !
 !
!
```

VRRP tracking use cases

The VRRP state is determined based on the tunnel link status. If the tunnel or interface is down on the primary VRRP, then the traffic is directed to the secondary VRRP. The secondary VRRP router in the LAN segment becomes primary VRRP to provide gateway for the service-side traffic.

Zscaler Tunnel Use Case 1—Primary VRRP, Single Internet Provider

The primary and secondary Zscaler tunnels are connected through a single internet provider to the primary VRRP. The primary and secondary VRRP routers are connected using TLOC extension. In this scenario, the VRRP state transitions occurs if the primary and secondary tunnels go down on the primary VRRP. The predetermined priority value decrements when the tracking object is down, which triggers the VRRP state transition. To avoid asymmetric routing, VRRP notifies this change to the Overlay through OMP.

Zscaler Tunnel Use Case 2—VRRP Routers in TLOC Extension, Dual Internet Providers

The primary and secondary VRRP routers are configured in TLOC extension high availability mode. The primary and secondary Zscaler tunnels are directly connected with primary and secondary VRRP routers, respectively, using dual internet providers. In this scenario too, the VRRP state transition occurs if the primary and secondary tunnels go down on the primary VRRP. The predetermined priority value decrements when the tracking object is down, which triggers the VRRP state transition. VRRP notifies this change to the overlay through OMP.

TLOC Preference

Transport Locators (TLOCs) connect an OMP route to a physical location. A TLOC is directly reachable using an entry in the routing table of the physical network, or represented by a prefix beyond a NAT device.

In Cisco IOS XE Catalyst SD-WAN devices, the TLOC change increase preference value increases based on the configured value. You can configure the TLOC change increase preference value on both the active and the backup nodes.

Restrictions for VRRP interface tracking

- Use VRRP only with service-side VPNs.
- Configure VRRP physical interfaces with VPN 0 when you use subinterfaces.
- Enable VRRP tracking only on a physical uplink interface or a logical tunnel interface (IPSEC, GRE, or both).
- Do not use IP prefix as an object for the VRRP Tracking feature.
- Apply the same tracker to multiple VRRP groups or VPNs.
- Do not track multiple VRRP interfaces using the same track object.
- Group a maximum of 16 track objects under a list track object.
- Do not configure **tloc-change** or **increase-preference** on more than one VRRP group.

Configure VRRP tracking using CLI templates

You can configure VRRP tracking using the CLI add-on feature templates and CLI device templates. For more information, see CLI Templates.

- VRRP object tracking using CLI
- SIG container tracking

VRRP object tracking using CLI

Procedure

Use the following configuration to add an interface to a track list using the Cisco SD-WAN Manager device CLI template:

```
Device(config)# track <object-id1> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track < object-id2> interface <interface-type-number> [line-protocol]
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit
Device(config)# interface GigabitEthernet2


Device(config-if)# vrf forwarding <vrf-number>
```

```
Device(config-if)# ipv4 address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)# exit
```

Example:

Interface Object Tracking Using CLI

```
config-transaction
  track 100 interface Tunnel123 line-protocol
   exit
 track 200 interface GigabitEthernet5 line-protocol
  exit
track 400 list boolean and
  object 100
  object 200
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 400 decrement 10
  tloc-change increase-preference 333
  exit
```

SIG container tracking

Procedure

Use the following example to configure a track list and tracking for SIG containers using the Cisco SD-WAN Manager device CLI template.

```
Device(config)# track <object-id1> service global

Device(config-tracker)# exit
Device(config)# track <object-id2> service global
Device(config-tracker)# exit
Device(config)# track <group-object-id> list boolean [and | Or]
Device(config-tracker)# object <object-id1>
Device(config-tracker)# object <object-id2>
Device(config-tracker)# exit

Device(config)# interface GigabitEthernet2

Device(config-if)# vrf forwarding <vrf-number>

Device(config-if)# ip address <ip-address> <subnet-mask>
Device(config-if)# negotiation auto
Device(config-if)# vrrp <vrrp-number> address-family ipv4
Device(config-if-vrrp)# address <ipv4-address> [primary | secondary]
Device(config-if-vrrp)# track <object-id> [decrement <dec-value> | shutdown]
```

```
Device(config-if-vrrp)# tloc-change increase-preference <value>
Device(config-if-vrrp)#exit
```

Example:

SIG Object Tracking Using CLI

```
config-transaction
  track 1 service global
  exit
  exit
  track 2 service global
track 3 list boolean and
  object 1
  object 2
  exit

interface GigabitEthernet2
 vrf forwarding 1
 ip address 10.10.1.1 255.255.255.0
 negotiation auto
vrrp 1 address-family ipv4
  address 10.10.1.10 primary
  track 3 decrement 10
  tloc-change increase-preference 333
  exit
```

Configure VRRP tracking

1. Configure an object tracker using a feature template.
2. Configure VRRP for a VPN Interface template and associate the object tracker with the template.

Configure an object tracker using a feature template

Use the **Cisco System** template to configure an object tracker.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **ConfigurationTemplates**.

Step 2 Click **Feature Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Navigate to the **Cisco System** template for the device.

Step 4 Click **Tracker** and choose **New Object Tracker** to configure the tracker parameters.

Table 138: Tracker Parameters

Field	Description
Tracker Type	Choose **Interface** or **SIG** or **Route** to configure the object tracker.
Object ID	Enter the object ID number.
Interface	Choose global or device-specific tracker interface name.
Route IP	Enter the IP route prefix to track the state of an IP route.
Route IP Mask	Enter the prefix mask.
VPN	Enter the VPN number.

Step 5 Click **Add**.

Step 6 Optionally, to create a tracker group, click **Tracker**, and click **Tracker Groups** > **New Object Tracker Groups** to configure the tracker parameters.

Note
Ensure that you have created two trackers to create a track group.

Table 139: Object Tracker Group Parameters

Field	Description
Group Tracker ID	Enter the name of the tracker group.
Tracker ID	Enter the name of the object tracker that you want to group.
Criteria	Choose **AND** or **OR** explicitly. **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 route is active. If you choose **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the route is active.

Note
Provide information in all the mandatory fields before you save the template.

Step 7 Click **Add**.

Step 8 Click **Save**.

Configure VRRP for a VPN interface template and associate interface object tracker

To configure VRRP for a **Cisco VPN** template, do the following:

Procedure

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

Step 2 Click **Feature Templates**.

Note
In Cisco SD-WAN Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

Step 3 Navigate to the **Cisco VPN Interface Ethernet** template for the device.

Note
For information about creating a new **Cisco VPN Interface Ethernet** template, see *Configure VPN Ethernet Interface*.

Step 4 Click **VRRP** and choose **IPv4**.

Step 5 Click **New VRRP** to create a new VRRP or edit the existing VRRP and configure the following parameters:

Parameter Name	Description
TLOC Preference Change	(Optional) Choose **On** or **Off** to set whether the TLOC preference can be changed or not.
TLOC Preference Change Value	(Optional) Enter the TLOC preference change. Range: 1 to 4294967295.

Step 6 Click the **Add Tracking Object** link, and in the **Tracking Object** dialog box that is displayed, click **Add Tracking Object**.

Step 7 In the **Tracker ID** field, enter the Interface Object ID or Object Group Tracker ID.

Step 8 From the **Action** drop-down list, choose **Decrement** and enter the **Decrement Value** as 1. Cisco vEdge Devices support decrement value of 1.

Or

Choose **Shutdown**

Step 9 Click **Add** to save the VRRP details, then click **Save** to save the configuration.

Monitor VRRP configuration

To view information about VRRP configuration:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

For Cisco SD-WAN Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Choose a device from the list of devices.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose **VRRP Information**.

Note
You can view the status of the VRRP configuration in **Track State**.

Verify VRRP tracking

View the summary of the VRRP configuration

The following is a sample output for the **show vrrp** command:

```
Device# show vrrp
GigabitEthernet2 - Group 1 - Address-Family IPv4
State is MASTER
State duration 37 mins 52.978 secs
Virtual IP address is 10.10.1.10
Virtual MAC address is 0000.5E00.0101
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
State change reason is VRRP_TRACK_UP
Tloc preference configured, value 333
Track object 400 state UP decrement 10
Master Router is 10.10.1.1 (local), priority is 100
Master Advertisement interval is 1000 msec (expires in 607 msec)
Master Down interval is unknown
FLAGS: 1/1
```

View the summary of tracked objects

The following is a sample output for the **show track brief** command:

```
Device# show track brief
Track Type      Instance           Parameter     State      Last Change
100   interface Tunnel123 l        line-protocol Up         00:12:48
200   interface GigabitEthernet5   line-protocol Up         00:49:57
400   list                         boolean       Up         00:12:47
```

View the state of the tracked list

The following is a sample output for the **show track list** command:

```
Device# show track list
Track 400
  List boolean and
  Boolean AND is Up
    6 changes, last change 00:12:58
    object 100 Up
    object 200 Up
  Tracked by:
    VRRPv3 GigabitEthernet2 IPv4 group 1
```

View a brief summary state of the tracked list

The following is a sample output for the **show track list brief** command:

```
Track  Type        Instance        Parameter        State  Last Change
         400    list                          boolean          Up    00:13:02
```