Configure Network Interfaces

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.

In the Cisco Catalyst SD-WAN overlay network design, interfaces are associated with VPNs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.

At a high level, 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.

Note To maximize the efficiency of the load-balancing among Cisco Catalyst 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.

Note Ensure that any network interface configured on a device has a unique IP address.

Configure VPN

VPN

Use the VPN template for all Cisco Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

To configure VPNs using Cisco SD-WAN Manager templates, follow this general workflow:

1. Create VPN feature templates to configure VPN parameters. You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.

   For Cisco SD-WAN Manager Network Management Systems and Cisco Catalyst SD-WAN Controllers, you can configure only VPNs 0 and 512. Create templates for these VPNs only if you want to modify the default settings for the VPN. For Cisco IOS XE Catalyst SD-WAN devices, you can create templates for these two VPNs and for additional VPN feature templates to segment service-side user networks.

   - **VPN 0—Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
   - **VPN 512—Management VPN**, which carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured.
   - **VPNs 1–511**, **513–65530—Service VPNs,** for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

2. Create interface feature templates to configure the interfaces in the VPN.

Create a VPN Template

Note Cisco IOS XE Catalyst SD-WAN devices use VRFs for segmentation and network isolation. However, the following steps still apply if you are configuring segmentation for Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE Catalyst SD-WAN devices.

Note You can configure a static route through the VPN template.

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 called **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 wish to create 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. From the VPN 0 or VPN 512 drop-down list, click **Create Template**. The VPN template form appears.

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 6 To create a template for VPNs 1 through 511, and 513 through 65527:

a. Click **Service VPN**, or scroll to the **Service VPN** section.

b. Click the **Service VPN** drop-down list.

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

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 7 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Changing the Scope for a Parameter Value

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

Parameter Name	Description
Device Specific	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Create a Template Variables Spreadsheet **Note** When you are using a CSV file for configuring device-specific variables in the device attach flow, ensure to fill all the mandatory fields before uploading. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

Configure Basic VPN Parameters

To configure basic VPN parameters, choose **Basic Configuration** and then configure the following parameters. Parameters marked with an asterisk are required to configure a VPN.

Parameter Name	Description
VPN	Enter the numeric identifier of the VPN. Range for Cisco IOS XE Catalyst SD-WAN devices: 0 through 65527 Values for Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager devices: 0, 512

Parameter Name	Description
Name	Enter a name for the VPN. **Note** For Cisco IOS XE Catalyst SD-WAN devices, you can't enter a device-specific name for the VPN.
Enhance ECMP keying	Click **On** to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source, and destination IP addresses, as the ECMP hash key. ECMP keying is **Off** by default.

Note To complete the configuration of the transport VPN on a router, you must configure at least one interface in VPN 0.

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

Configure Load-Balancing Algorithm Using the CLI

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, you need CLI template to configure the **src-only** load-sharing algorithm for IPv4 and IPv6 Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN traffic. For complete details on the load-sharing algorithm CLI, see IP Commands list.

This following provides CLI configurations for selecting a Cisco Express Forwarding load-balancing algorithm for non Cisco Catalyst SD-WAN IPv4 and IPv6 traffic. You can enable ECMP keying to send the configurations for both IPv4 and IPv6.

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source [id]
 | destination [id]] |
src-only [id]}
```

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source
[id] | destination [id]] |
src-only [id]}
```

This following provides CLI configurations for enabling load balancing algorithm on an interface for Cisco Catalyst SD-WAN IPv4 and IPv6 traffic. You can enable ECMP keying to send the configurations for both IPv4 and IPv6.

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

Configure DNS and Static Hostname Mapping

To configure DNS addresses and static hostname mapping, click **DNS** and configure the following parameters:

Parameter Name	Options	Description
Primary DNS Address	Click either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN.	
New DNS Address	Click **New DNS Address** and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address.	
	Mark as Optional Row	Check the **Mark as Optional Row** check box to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.
	Hostname	Enter the hostname of the DNS server. The name can be up to 128 characters.
	List of IP Addresses	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.
To save the DNS server configuration, click **Add**.		

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

Mapping Host Names to IP Addresses

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

Configure Interfaces in the WAN Transport VPN (VPN 0)

This topic describes how to configure the general properties of WAN transport and service-side network interfaces. For information about how to configure specific interface types and properties—including cellular interfaces, DHCP, PPPoE, VRRP, and WLAN interfaces.

VPN 0 is the WAN transport VPN. This VPN handles all control plane traffic, which is carried over OMP sessions, in the overlay network. For a Cisco IOS XE Catalyst SD-WAN device device to participate in the overlay network, at least one interface must be configured in VPN 0, and at least one interface must connect to a WAN transport network, such as the Internet or an MPLS or a metro Ethernet network. This WAN transport interface is referred to as a tunnel interface. At a minimum, for this interface, you must configure an IP address, enable the interface, and set it to be a tunnel interface.

To configure a tunnel interface on a Cisco Catalyst SD-WAN Controller or a Cisco SD-WAN Manager, you create an interface in VPN 0, assign an IP address or configure the interface to receive an IP address from DHCP, and mark it as a tunnel interface. The IP address can be either an IPv4 or IPv6 address. To enable dual stack, configure both address types. You can optionally associate a color with the tunnel.

Note You can configure IPv6 addresses only on transport interfaces in VPN 0 and but not supported in VPN 512.

Tunnel interfaces on Cisco IOS XE Catalyst SD-WAN devices must have an IP address, a color, and an encapsulation type. The IP address can be either an IPv4 or IPv6 address. To enable dual stack in releases before Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure both address types.

To use dual stack with Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure all controllers with both IPv4 and IPv6 addresses. In addition, configure DNS for the Cisco Catalyst SD-WAN Validator interface to resolve IPv4 and IPv6 address types so that controllers can reach the Cisco Catalyst SD-WAN Validator through either IP address type.

Note Starting from Cisco vManage Release 20.6.1, in case of a dual-stack configuration, if an IPv4 address or the fully qualified domain name (FQDN) is not available, but an IPv6 address is available, then the IPv6 address is used to connect to the Cisco Catalyst SD-WAN Validator.

For the tunnel interface, you can configure a static IPv4 or IPv6 address, or you can configure the interface to receive its address from a DHCP server. To enable dual stack, configure both an IPv4 and an IPv6 address on the tunnel interface.

From Cisco IOS XE Catalyst SD-WAN Release 17.3.2, Cisco IOS XE Catalyst SD-WAN devices do not support dual stack on the same TLOC or interface. Only one address type can be provisioned for a TLOC or interface. Using a second address type requires a second TLOC or interface on which it can be provisioned.

On Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Controller NMSs, *interface-name* can be either **eth** *number* or **loopback** *number*. Because Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Controller NMSs participate only in the overlay network's control plane, the VPNs that you can configure on these devices are VPN 0 and VPN 512. Hence, all interfaces are present only on these VPNs.

To enable the interface, include the **no shutdown** command.

Color is a Cisco Catalyst SD-WAN software construct that identifies the transport tunnel. It can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. The colors **metro-ethernet**, **mpls**, and **private1** through **private6** are referred to as *private colors*, because they use private addresses to connect to the remote side Cisco IOS XE Catalyst SD-WAN device in a private network. You can use these colors in a public network provided that there is no NAT device between the local and remote Cisco IOS XE Catalyst SD-WAN devices.

To limit the remote TLOCs that the local TLOC can establish BFD sessions with, mark the TLOC with the **restrict** option. 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.

Note When a WAN edge device is configured with two IPv6 TLOCs, one with static default route and the other one with IPv6 address autoconfig default which is the IPv6 neighbor discovery default route, the IPv6 neighbor discovery default route is not installed in the routing table. In this case, the IPv6 TLOC with IPv6 neighbor discovery default route does not work.

For IPv6 TLOC with IPv6 neighbor discovery default route to work, you can configure the static route for TLOC with IPv6 neighbor discovery to overwrite the IPv6 neighbor discovery default route and ensure that both the static routes are installed into the routing table. You can also use the IPv6 neighbor discovery default route on all interfaces.

On a Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Controller NMS, you can configure one tunnel interface. On a Cisco IOS XE Catalyst SD-WAN device, you can configure up to eight tunnel interfaces.

On Cisco IOS XE Catalyst SD-WAN devices, you must configure the tunnel encapsulation. The encapsulation can be either IPsec or GRE. For IPsec encapsulation, the default MTU is 1442 bytes, and for GRE it is 1468 bytes, These values are a function of overhead required for BFD path MTU discovery, which is enabled by default on all TLOCs. (For more information, see Configuring Control Plane and Data Plane High Availability Parameters.) You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE Catalyst SD-WAN device, you must configure the same tunnel encapsulation type or types so that the two routers can exchange data traffic. Data transmitted out of an IPsec tunnel can be received only by an IPsec tunnel, and data sent on a GRE tunnel can be received only by a GRE tunnel. The Cisco Catalyst SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE Catalyst SD-WAN device.

A tunnel interface allows only DTLS, TLS, and, for Cisco IOS XE Catalyst SD-WAN devices, IPsec traffic to pass through the tunnel. To allow additional traffic to pass without having to create explicit policies or access lists, enable them by including one **allow-service** command for each service. You can also explicitly disallow services by including the **no allow-service** command. Note that services affect only physical interfaces. You can allow or disallow these services on a tunnel interface:

Service	Cisco Catalyst SD-WAN Controller	Cisco Catalyst SD-WAN Controller
all (Overrides any commands that allow or disallow individual services)	X	X
bgp	—	—
dhcp (for DHCPv4 and DHCPv6)	—	—
dns	—	—
https	X	—
icmp	X	X
netconf	X	—
ntp	—	—
ospf	—	—

Service	Cisco Catalyst SD-WAN Controller	Cisco Catalyst SD-WAN Controller
sshd	X	X
stun	X	X

The **allow-service stun** command pertains to allowing or disallowing a Cisco IOS XE Catalyst SD-WAN device to generate requests to a generic STUN server so that the device can determine whether it is behind a NAT and, if so, what kind of NAT it is and what the device's public IP address and public port number are. On a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT, you can also have tunnel interface to discover its public IP address and port number from the Cisco Catalyst SD-WAN Validator.

With this configuration, the Cisco IOS XE Catalyst SD-WAN device uses the Cisco Catalyst SD-WAN Validator as a STUN server, so the router can determine its public IP address and public port number. (With this configuration, the router cannot learn the type of NAT that it is behind.) No overlay network control traffic is sent and no keys are exchanged over tunnel interface configured to the the Cisco Catalyst SD-WAN Validator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it. Because no control traffic is sent over a tunnel interface that is configured to use the Cisco Catalyst SD-WAN Validator as a STUN server, you must configure at least one other tunnel interface on the Cisco IOS XE Catalyst SD-WAN device so that it can exchange control traffic with the Cisco Catalyst SD-WAN Controller and the Cisco Catalyst SD-WAN Controller NMS.

You can log the headers of all packets that are dropped because they do not match a service configured with an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

TLOC Extension

There are scenarios when Cisco IOS XE Catalyst SD-WAN devices cannot connect to a single transport directly and only one device can connect to a single transport. A switch is connected to each transport and the devices connect to each transport through the switches. To have a set-up with the switch option at a branch increases the cost of the solution and result in managing another device. TLOC extension enables a device to access the opposite WAN transport connected to the neighbouring device using a TLOC-extension interface.

TLOC Extension Over IPv6

Table 1: Feature History

Feature Name	Release Information	Description
TLOC Extension Over IPv6	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables the support of TLOC extension for IPv6. In the previous releases, TLOC extension was supported only for IPv4.

Information About TLOC Extension Over IPv6

In the earlier releases, TLOC extension was supported only over IPv4 interfaces.

This feature supports the following requirements:

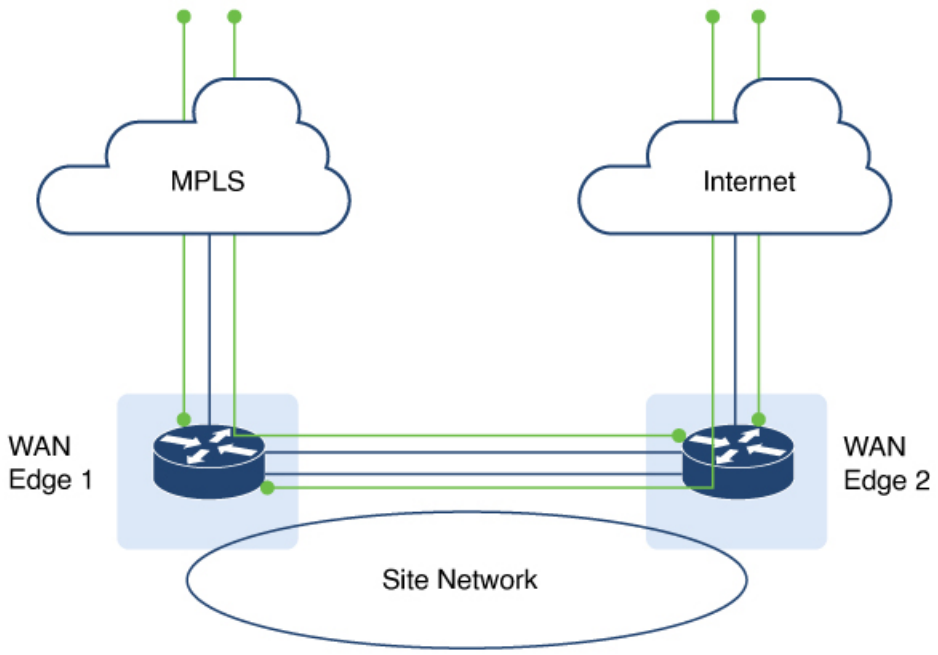
- TLOC extension over IPv6 works only if the underlay supports IPv6 addressing on both the Cisco IOS XE Catalyst SD-WAN devices connecting each other.
- Implicit IPv6 ACL on TLOC tunnel interface is supported.
- IPv6 TLOC has dual stack support. When both IPv4 and IPv6 are configured, the tunnel is built on top of either IPv4 or IPv6, based on the configuration.
- TLOC interface supports NAT66. The limitations of NAT66 also applies to the TLOC extended interface.
- The following interface types supports IPv6 TLOC extension:
  - Physical interface
  - Physical sub-interface
  - Loopback interface

Note Only the Layer 2 setup supports IPv6 TLOC extension.

- This feature is supported for both private and public color TLOC interfaces.
- This feature supports the loopback TLOC interface that is bound to either:
  - The WAN transport circuit.
  - An extended WAN interface between two Cisco IOS XE Catalyst SD-WAN devices.

Use Case for TLOC Over IPv6 Extension

Figure 1: TLOC Extension



The TLOC extension allows each Cisco IOS XE Catalyst SD-WAN device to access the opposite transport through a TLOC-extension interface on the neighboring SD-WAN device. In the diagram, SD-WAN device 1 can access the internet through the SD-WAN device 2 TLOC extension interface in addtion to the direct MPLS connection. SD-WAN device 2 can access the MPLS transport through the SD-WAN device 1 TLOC extension interface in addition to the direct internet connetion. TLOC extension over IPv6 achieves redundancy in a dual-device deployment scenario with only one circuit connection on each device.

Limitations for TLOC Extension Over IPv6

- SIG is not supported on the IPv6 TLOC extension.
- NAT64 is not supported for IPv6 TLOC extension.
- TLOC extension over IPv6 is not supported for Layer 3 connections.

When a TLOC configuration is extended to a peer interface and then to ISP, the extended control connections are still up on the peer interface, even after removing TLOC Extension configuration.

In TLOC-Extension, the extender interface is part of the Cisco Catalyst SD-WAN. However, the tunnel-interface configuration under the extender interface is optional.

Configure TLOC Extension

1. Enter global configuration mode, and configure an interface.

   ```
   Device# config-transaction
   ```

2. Enter SD-WAN configuration mode.

```
Device(config)# sdwan
```

3. In the SD-WAN configuration mode, configure an interface type such as, Gigabit Ethernet.

```
Device(config-sdwan)# interface GigabitEthernet3
```

4. Configure tunnel interface.

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
```

5. Configure encapsulation, color, allowed services for TLOC.

```
Device(config-interface-GigabitEthernet3)# tunnel-interface
Device(config-interface-GigabitEthernet3)# encapsulation ipsec
Device(config-interface-GigabitEthernet3)# color color
Device(config-interface-GigabitEthernet3)# exit
```

6. In the global configuration mode, configure an interface.

```
Device# config-transaction
Device(config)# ip route 0.0.0.0 0.0.0.0 ip-address
```

7. On device 2, the LTE WAN connection is on GigabitEthernet1 and this transport is extended to device 1 GigabitEthernet3 TLOC interface.

```
Device(config-sdwan)# tloc-extension GigabitEthernet1
```

8. Configure NAT routes on GigabitEthernet1 for data traffic to reach back to device 1 through device 2 for GigabitEthernet3 subnet.

The following example describes how TLOC extension is configured on a network interface.

```
On Device1,
Configure TLOC interface on VPN 0
sdwan
interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec
   color custom1
   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

  Configure default route via this TLOC interface with nexthop
  to L2 connected interface of the peer (ED2 Gig3).

  ip route 0.0.0.0 0.0.0.0 10.1.19.16

 On Device2,
LTE WAN connection is on Gig1 and this transport is extended to ED1 Gig3 TLOC
interface(custom1).
 sdwan
 int GigabitEthernet3
 tloc-extension GigabitEthernet1
```

```
Configure NAT routes on Gig1 or appropriate routes for data traffic to reach back to ED1
via ED2 for Gig3 subnet.
```

Verify TLOC Extension

The following is a sample output of the commands to verify if TLOC extension is configured on a network interface.

```
Device# show sdwan control connections
PEER                                          PEER
  CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                    PRIV
  PEER
PUB                                           GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                              PORT
  PUBLIC IP
PORT  ORGANIZATION            LOCAL COLOR     PROXY STATE UPTIME      ID
-----------------------------------------------------------------------------------------------------
vsmart  dtls 172.16.255.19   100        1      2001:a0:5::13
12455 2001:a0:5::13                           12455 vIPtela Inc Regression  custom1
      No    up
0:01:23:06 0
vsmart  dtls 172.16.255.20   200        1      2001:a0:c::14                          12456
2001:a0:c::14                            12456 vIPtela Inc Regression  custom1
No    up
0:01:23:06 0
```

```
Device# show sdwan bfd sessions
                                         SOURCE TLOC      REMOTE TLOC
DST PUBLIC                          DST PUBLIC         DETECT      TX
  SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
IP                                            PORT        ENCAP  MULTIPLIER  INTERVAL(msec
  UPTIME
TRANSITIONS
-----------------------------------------------------------------------------------------------------
172.16.255.14    400         up          custom1            lte             2001:a0:15::10
2001:a1:e::e                                12346       ipsec  7           1000
0:00:05:50  3
```

Configure the System Interface

For each Cisco IOS XE Catalyst SD-WAN device, you configure a system interface with the **system system-ip** command. The system interface's IP address is a persistent address that identifies the Cisco IOS XE Catalyst SD-WAN device. It is similar to a router ID on a regular router, which is the address used to identify the router from which packets originated.

Specify the system IP address as an IPv4 address in decimal four-part dotted notation. Specify just the address; the prefix length (/32) is implicit.

The system IP address can be any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, and 240.0.0.0/4 and later. Each device in the overlay network must have a unique system IP address. You cannot use this same address for another interface in VPN 0.

The system interface is placed in VPN 0, as a loopback interface named **system**. Note that this is not the same as a loopback address that you configure for an interface.

To display information about the system interface, use the **show interface** command. For example:

The system IP address is used as one of the attributes of the OMP TLOC. Each TLOC is uniquely identified by a 3-tuple comprising the system IP address, a color, and an encapsulation. To display TLOC information, use the **show omp tlocs** command.

For device management purposes, it is recommended as a best practice that you also configure the same system IP address on a loopback interface that is located in a service-side VPN that is an appropriate VPN for management purposes. You use a loopback interface because it is always reachable when the router is operational and when the overlay network is up. If you were to configure the system IP address on a physical interface, both the router and the interface would have to be up for the router to be reachable. You use a service-side VPN because it is reachable from the data center. Service-side VPNs are VPNs other than VPN 0 (the WAN transport VPN) and VPN 512 (the management VPN), and they are used to route data traffic.

Configure Control Plane High Availability

A highly available Cisco Catalyst SD-WAN network contains two or more Cisco Catalyst SD-WAN Controllers in each domain. A Cisco Catalyst SD-WAN domain can have up to eight Cisco Catalyst SD-WAN Controllers, and each Cisco IOS XE Catalyst SD-WAN device, by default, connects to two of them. You change this value on a per-tunnel basis:

Configure Other Interfaces

Configure Interfaces in the Management (VRF mgmt-intf)

On all Cisco Catalyst SD-WAN devices, VPN 512 is used for out-of-band management, by default as part of the factory-default configuration. On Cisco IOS XE Catalyst SD-WAN devices the management VPN is converted to VRF Mgmt-Intf.

Cisco XE SD-WAN devices use VRFs in place of VPNs.

```
Device# show sdwan running-config | sec vrf definition Mgmt-intf

vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
============
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 negotiation auto
exit
============
config-t
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0

vrf definition Mgmt-intf
 rd 1:512
 !
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
 exit-address-family
```

```
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 192.168.20.11 255.255.255.0
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0
!
```

To display information about the configured management interfaces, use the **show interface** command. For example:

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  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 set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 12 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     4839793 packets input, 415574814 bytes, 0 no buffer
     Received 3060073 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     82246 packets output, 41970224 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 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
```

Note VPN 512 is not advertised in the overlay. It is local to the device. If you need a management VPN that is reachable through the overlay, create a VPN with a number other than 512.

Configure Loopback Interfaces

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

One special use of loopback interfaces is to configure data traffic exchange across private WANs, such as MPLS or metro Ethernet networks. To allow a router that is behind a private network to communicate directly over the private WAN with other edge routers, you direct data traffic to a loopback interface that is configured as a tunnel interface rather than to an actual physical WAN interface.

Implicit ACL on Loopback Interfaces

Table 2: 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	This feature allows you to enable implicit ACL on loopback TLOC interfaces. 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.

Information About Implicit ACL on Loopback Interfaces

Access lists that you configure using localized data policy are called Explicit ACLs. Router tunnel interfaces also have implicit ACLs, which are also referred to as Services. Some of these are present by default on the tunnel interface, and they are in effect until you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco IOS XE Catalyst SD-WAN devices, the following services are enabled by default: DHCP, DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

You can configure and modify implicit ACLs with the **allow-service** command to allow a service. Use the **no allow-service** command to disallow a service. If both implicit ACL and explicit ACL are configured, explicit ACL takes precedence over the implicit ACL.

When Cisco IOS XE Catalyst SD-WAN device loopback interfaces are configured with a Transport Location (TLOC), implicit ACL rules are applied to the traffic destined for it. Implicit ACL on loopback interfaces are applied both in a bind mode and in an unbind mode. A bind mode is where a loopback interface is bound to a physical interface on a Cisco IOS XE Catalyst SD-WAN device to send data. In an unbind mode, a loopback interface is not bound to any physical interface.

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.

Note Use this command **implicit-acl-on-bind-intf** 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.

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, 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.

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.

Example Using Bind Mode and Unbind Mode

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.

To enable implicit ACL protection on physical interface GigabitEthernet1 for incoming VPN 0 traffic use the command **implicit-acl-on-bind-intf** .

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.

Benefits of Implicit ACL on Loopback Interfaces

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

Configure Implicit ACL on Loopback Interfaces

Similar to configuring physical WAN interfaces, you can configure implicit ACL on loopback interfaces using a feature template or using a CLI Add-on template in Cisco SD-WAN Manager.

For information about using a feature template to configure implicit ACL on loopback interfaces, see Configure VPN Ethernet Interface.

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

Configure Implicit ACL on Loopback Interfaces Using CLI

By default DNS, DHCP, ICMP and HTTPS services are permitted, and other services are denied.

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

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
```

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
```

Monitor Implicit ACL on Loopback Interfaces

Use the **show platform hardware qfp active statistics drop** command to monitor implicit ACL configuration on loopback interfaces.

Example

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
```

Configure 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.

For example:

```
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
  !
 !
```

Configure Interface Properties

Set the Interface Speed

When a Cisco IOS XE Catalyst SD-WAN device comes up, 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 speed of the interface. To display the hardware present in the router, use the **show hardware inventory** command:

To display the actual speed of each interface, use the **show interface** command. Here, interface **ge0/0**, which connects to the WAN cloud, is running at 1000 Mbps (1Gbps; it is the 1GE PIM highlighted in the output above), and interface **ge0/1**, which connects to a device at the local site, has negotiated a speed of 100 Mbps.

For non-physical interfaces, such as those for the system IP address and loopback interfaces, the interface speed is set by default to 10 Mbps.

To override the speed negotiated by the two devices on the interface, disable autonegotiation and configure the desired speed:

For Cisco Catalyst SD-WAN Controllers and Cisco SD-WAN Manager systems, the initial interface speeds are 1000 Mbps, and the operating speed is negotiated with the device at the remote end of the interface. The controller interface speed may vary depending upon the virtualization platform, the NIC used, and the drivers that are present in the software.

Set the Interface MTU

By default, all interfaces have an MTU of 1500 bytes. You can modify this on an interface:

For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a the MTU can range from 576 through 2000 bytes.

Starting from release Cisco IOS XE Catalyst SD-WAN Release 17.4.1a the MTU can range from 576 through 9216 bytes on 1 GE interfaces. This MTU range is also supported on 10 GE and 100 GE interfaces starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a.

To display an interface's MTU, use the **show interface** command.

For Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller devices, you can configure interfaces to use ICMP to perform path MTU (PMTU) discovery. When PMTU discovery is enabled, the device to 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. To explicitly configure BFD to perform PMTU discovery, use the **bfd color pmtu-discovery** configuration command. However, you can choose to instead use ICMP to perform PMTU discovery:vEdge Cloud router

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

VFR and Underlay Fragmentation

Table 3: Feature History

Feature Name	Release Information	Description
VFR and Underlay Fragmentation	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In Cisco Catalyst SD-WAN networks, the VFR (Virutal Fragmentation Reassembly) actively fragments and reassembles packets. The packets undergo fragmentation to improve transportation efficiency while passing through a VFR-enabled Cisco IOS XE Catalyst SD-WAN device. The VFR reassembles the fragmented packets to match the original incoming packet. The reassembled packet contains critical Layer 4 or Layer 7 information necessary for proper reception by the destination device. Underlay fragmentation refers to the process of breaking down a large data packet into smaller fragments at the network layer. Underlay fragmentation allows the successful transmission of packets that exceed the MTU limitations by breaking them down into manageable fragments and ensuring their reliable delivery.

Information About VFR and Underlay Fragmentation

While transmitting data across a network, due to various network constraints, the original data packets fragment into smaller fragments to facilitate seamless transmission. While the packets travel through the Cisco IOS XE Catalyst SD-WAN device, they are fragmented . VFR allows fragmented packets to be reassembled efficiently before reaching their destination.

In Cisco Catalyst SD-WAN network, data packets undergo reassembly in two modes: the default mode and the reassembly mode.

In the default mode, packets are virtually reassembled by default. Upon the delivery of the first fragment, each feature in the network receives the entire payload of the virtually reassembled packet. When the last fragment is received, the remaining features reassemble the packet. The original packet is fragmented, and the internal fragment information structure is shared. The fragments are then queued for refragmentation based on the fragment-offset sequence. The VFR mechanism reconstructs the packets using information from the fragment headers, such as fragment identifiers, sequence numbers, and offsets.

On the other hand, in the reassembly mode, the packets undergo physical reassembly, and fragment header information isn't saved. Upon receiving the last fragment, the fragments reassemble via a metapacket, and the internal fragment information structure is released.

Note

- If the packets were originally fragmented using the default mode, they undergo reassembly as if they were the original incoming packets. On the other hand, when the reassembly mode is utilized to virtually fragment the packets, they experience fragmentation based on the MTU of the egress interface before reassembly.
- Some features (such as NAT, Cisco IOS XE Firewall, IPSec) automatically enable VFR to obtain Layer 4 or Layer 7 information.
- When a particular interface enables VFR, it overrides the existing firewall or NAT's VFR mode configuration by default, ensuring interoperability with the firewall or NAT.

Information About Underlay Fragmentation

Underlay fragmentation processes large data packets that exceed the MTU (Maximum Transmission Unit) size supported by the Cisco Catalyst SD-WAN network infrastructure. Each data packet has a maximum size that can transmit over the network without being fragmented. This maximum size is defined by the MTU. The process of breaking down a large data packet into smaller fragments at the network layer is known as underlay fragmentation. The underlay fragmentation enables the transmission of packets that exceed the MTU limitations by breaking them down into smaller fragments and ensuring their successful delivery.

Prerequisites For Configuring VFR and Underlay Fragmentation

The Maximum Transmission Unit (MTU) size needs to be properly configured on the network devices. The MTU defines the maximum size of a packet that can be transmitted without fragmentation. It is essential to ensure that the MTU is set appropriately on all devices involved in the network path to avoid underlay fragmentation unless it is intentionally desired.

Restrictions For Configuring VFR and Underlay Fragmentation

- The VFR process requires all fragments within an IP datagram. If fragments within an IP datagram are sent to different devices due to load balancing, VFR may fail and fragments may be dropped.
- VFR is designed to work with any feature that requires fragment reassembly (such as Cisco Catalyst SD-WAN NAT, and IPsec). By default, NAT, Crypto-based IPSec, and NAT64 enable and disable VFR internally; that is, when these features are enabled on an interface, VFR is enabled on that interface. If more than one feature attempts to enable VFR on an interface, VFR maintains a reference count to keep track of the number of features that have enabled VFR. When the reference count is zero, VFR is automatically disabled.
- The underlay fragmentation mechanism is limited to the network layer and is specific to the underlying network infrastructure. It does not handle fragmentation and reassembly across multiple network segments or end-to-end connections.

- If any of the fragments in a series of fragmented packets are lost or arrive out of order, the reassembly process may fail. This can result in incomplete or corrupted packets.
- The VFR CLIs are unavailable under port-channel sub-interfaces.

Benefits of VFR and Underlay Fragmentation

- VFR enables the Cisco IOS XE Firewall to create appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.
- VFR is responsible for detecting and preventing various types of fragment attacks.
- VFR drops all fragments within a fragment chain if an overlap of a fragment is detected.

Use Cases For VFR and Underlay Fragmentation

Networks such as long-distance connections such as a connection between an airplane and aiport signal towers, can experience interruptions, due to the time it takes for large packets to traverse these links. When VFR is enabled, the fragments will reassemble into a complete datagram, then are fragmented within the Cisco Catalyst SD-WAN tunnel interface. With this, the first fragment will be sent out first and there is no interruption in receiving the packets.

Underlay fragmentation helps in fragmenting large packets into smaller sizes, and reconstruct the packet back into the original one. This improves the overall application performance.

Enable Boost Mode

The boost mode helps in resolving one of the identified bottlenecks related to the memory management of fragments within the data plane of the network. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the memory allocation to reassembly of fragments occured from a global chunk, necessitating a lock in period for the memory until the reassembly is complete. This leads to potential competition among multiple threads for the same global chunk and results in waiting for the same memory. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the boost mode enhances performance by utilizing CVLA, an alternative data plane memory infrastructure. Unlike the chunk mechanism, CVLA is lock-free and is an efficient memory management mechanism within Cisco IOS XE devices.

Note The boost mode is disabled by default on Cisco IOS XE Catalyst SD-WAN devices.

Enable Boost Mode Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

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

This section provides example CLI configurations to enable the boost mode.

1. Enable the boost mode:

platform *ipreass* **boost-mode**

Here is the complete configuration example to enable the boost mode:

```
platform ipreass boost-mode
```

Configure VFR Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

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

This section provides example CLI configurations to configure VFR.

Enable VFR for IPv4 packets on Inbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   interface *interface-type* *interface-number*
2. Enable VFR on the interface and specify the maximum threshold values:

   ip virtual-reassembly [**max-reassemblies** number] [**max-fragments** number] [**timeout** seconds] [**mode** modes][**drop-fragments**]

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet5
ip virtual-reassembly max-reassemblies 64 max-fragments 16 mode default timeout 5
```

Enable VFR for IPv4 packets on Outbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   interface *interface-type* *interface-number*
2. Enable VFR for outbound interface traffic on the interface and specify the maximum threshold values:

   ip virtual-reassembly-out [**max-reassemblies** number] [**max-fragments** number] [**timeout** seconds] [**mode** modes][**drop-fragments**]

Here is the complete configuration example to enable VFR for IPv4 packets:

```
interface GigabitEthernet 5
ip virtual-reassembly-out mode default max-fragments 64
```

Enable VFR for IPv6 packets on Inbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   interface *interface-type* *interface-number*
2. Enable VFR for IPv6 packets on inbound interface traffic

   ipv6 virtual-reassembly [in | out][**max-reassemblies** number] [**max-fragments** number] [**timeout** seconds] [**mode** modes][**drop-fragments**]

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
ipv6 virtual-reassembly in mode default max-fragments 25
max-reassemblies 1024
```

Enable VFR for IPv6 packets on Outbound Interface Traffic

1. Configure an interface type and enter interface configuration mode:

   interface *interface-type interface-number*
2. Enable VFR for IPv6 packets on outbound interface traffic

   ipv6 virtual-reassembly [in | out][**max-reassemblies** number] [**max-fragments** number] [**timeout** seconds] [**mode** modes][**drop-fragments**]

Here is the complete configuration example to enable VFR for IPv6 packets:

```
interface GigabitEthernet 5
ipv6 virtual-reassembly out mode default max-fragments 25
```

Configure Underlay Fragmentation Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

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

This section provides example CLI configurations to configure underlay fragmentation.

1. Enter the config-sdwan mode:

   sdwan
2. Configure an interface type and enter interface configuration mode:

   interface *interface-name interface-number*
3. Configure the tunnel interface:

   tunnel-interface
4. Skip Layer 3 fragmentation and clear overlay DF bit:

   inner-fragmentation-disable
5. Perform the encapsulation for the GRE interface of the TLOC:

   encapsulation *gre*

Note Only GRE encapsulation is supported for underlay fragmentation in Cisco IOS XE Catalyst SD-WAN Release 17.12.1a.

Here is the complete configuration example to enable underlay fragmentation:

```
sdwan
interface GigabitEthernet1
tunnel-interface
inner-fragmentation-disable
encapsulation gre
```

Verify Boost Mode

The following is a sample output from the **show platform hardware qfp active infrastructure cvla client handles** command:

```
Device# show platform hardware qfp active infrastructure cvla client handles
Handles for cpp 0:

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

Entity name: IPREASS_CVLA_0

Handle: 0xeea45000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF_AOR

Handle: 0xeea0d000

Number of allocations: 0

Memory allocated: 0


Entity name: NBAR_CVLA_ENTITY

Handle: 0xee946000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 2

Handle: 0xef929000

Number of allocations: 0

Memory allocated: 0


Entity name: FNF Chunk 1

Handle: 0xef928000

Number of allocations: 0

Memory allocated: 0
```

```
---------------------
```

Note If there is no entity for **IPREASS_CVLA_*** displayed, the boost mode is disabled. Once the boost mode is disabled, the **IPREASS_CVLA_*** disappears after 64 seconds.

Monitor VFR and Underlay Fragments Using the CLI

Monitor VFR for IPv4 packets

The following is a sample output from the **show ip virtual-reassembly** command:

```
Device# show ip virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   Virtual Fragment Reassembly (VFR) is ENABLED [out]

   Concurrent reassemblies (max-reassemblies): 16

   Fragments per reassembly (max-fragments): 32

   Reassembly timeout (timeout): 3 seconds

   Drop fragments: OFF


   Current reassembly count:0

   Current fragment count:0

   Total reassembly count:12

   Total reassembly timeout
```

The example shows if VFR for IPv4 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

Monitor VFR for IPv6 packets

The following is a sample output from the **show ipv6 virtual-reassembly** command:

```
Device# show ipv6 virtual-reassembly GigabitEthernet 5
GigabitEthernet5:

   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [out]

   IPv6 configured concurrent reassemblies (max-reassemblies): 64

   IPv6 configured fragments per reassembly (max-fragments): 16

   IPv6 configured reassembly timeout (timeout): 3 seconds

   IPv6 configured drop fragments: OFF
```

```
  IPv6 current reassembly count:0

  IPv6 current fragment count:0

  IPv6 total reassembly count:12

  IPv6 total reassembly timeout count:0
```

The example shows if VFR for IPv6 is enabled or not. **Virtual Fragment Reassembly (VFR) is ENABLED [out]** signifies that VFR is enabled. The total packets that underwent reassembly are also displayed.

Monitor Underlay Fragmentation

The following is a sample output from the **show ip traffic interface GigabitEthernet 1** command:

```
Device# show ip traffic interface GigabitEthernet 1
GigabitEthernet 1 statistics :

  Rcvd:  11048818 total, 749458331 total_bytes

         0 format errors, 0 hop count exceeded

         0 bad header, 0 no route

         0 bad destination, 0 not a router

         0 no protocol, 0 truncated

         0 forwarded

         0 fragments, 0 total reassembled

         0 reassembly timeouts, 0 reassembly failures

         0 discards, 0 delivers

  Sent:  0 total, 0 total_bytes 0 discards

         0 generated, 0 forwarded

         0 fragmented into, 0 fragments, 0 failed

  Mcast: 0 received, 0 received bytes

         0 sent, 0 sent bytes

  Bcast: 0 received, 1256 sent
```

The example shows the number of packets that were sent and received, including the total number of packets. A change from the previous number of packet tranfer indicates that underlay fragmentation is enabled.

The following is a sample output from **show sdwan ftm** *tloc-list* command:

```
Device# show sdwan ftm tloc-list

--- LOCAL  TLOC LIST ---




Id: 32775 (binosId=0xf808007f), Tenant Id: 0      LocalTLOC, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0 Inner-fragmentation
-disable: No
```

```
[TOTAL-LOCAL-TLOC:1]



--- REMOTE TLOC LIST ---



Id: 32768 (binosId=0xf808000f), Tenant Id: 0       SLAClass, num-nhops: 0   ,hash: 0, ref:
 1    SLA 0x0:0x0
 num-active-nhops: 0


Id: 32774 (binosId=0xf808006f), Tenant Id: 0       SLAClass, num-nhops: 1   ,hash: 0, ref:
 1    SLA 0x1:0x0
 [nhop1] nhop-Id: 19   , Type: IPsec     , Encap: IPSEC SLA 0x1:0x0hw_record_index:   5
198.100.1.5/12366->198.100.1.6/12346 pr
oto 0x800 hash 0x13 wan-if 3 tloc 32774 R-color mpls local-tloc 32775 L-color mpls BFD UP
tloc-capability 0 SLA 0x1:0x0 weight
1   pref 0

 num-active-nhops: 1


[TOTAL-REMOTE-TLOC:2]


--- PENDING TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-PENDING-TLOC:0]



--- UNMATCHED TLOC LIST (is_pending_updates:FALSE)---



[TOTAL-UNMATCHED-TLOC:0]


--- TENANT LOCAL  TLOC LIST ---
```

The example displays all the local TLOCs in the network.

The following is a sample output from **show platform software sdwan** *R0 next-hop overlay all* command:

```
Device# show platform software sdwan R0 next-hop overlay all

Show sdwan next-hop oce all :


OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY

Overlay: client_handle (nil), ppe addr (nil)

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_IP, ifhandle: 15, encap type: MCP_ET_NULL

  encap rewrite: 00

  mtu: 1446, fixup: 0x0, fixup_flags_2: 0x0, color: mpls, phy_oce_handle: 31, nh_overlay_h:
 0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366

    dst-ip: 198.100.1.6, dst-port: 12346

    local_system_ip: 1.1.1.1

    remote_system_ip: 2.2.2.2

    local_color: 2 [mpls], remote_color: 2 [mpls]

    wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]

    tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0

    bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5

    Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in a particular next-hop overlay.

The following is a sample output from **show platform software sdwan** *F0 next-hop overlay all* command:

```
Device# show platform software sdwan F0 next-hop overlay all

OCE ID: 0xf800013f, OCE Type: SDWAN_NH_OVERLAY

Overlay: client_handle 0x63d321350ba0, ppe addr db910710

  overlay encap: ipsec

  src-ip: 198.100.1.5, src-port: 12366

  dst-ip: 198.100.1.6, dst-port: 12346

  flags: 0x0, linktype: MCP_LINK_SDWAN, ifhandle: 15, encap type: MCP_ET_ARPA

  encap rewrite: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  mtu: 1446, fixup: 0x0, fixup_flags_2: 0x800000, color: mpls, phy_oce_handle: 31,
nh_overlay_h: 0xf800013f
    Overlay_CFG:

    encap type: ipsec

    src-ip: 198.100.1.5, src-port: 12366

    dst-ip: 198.100.1.6, dst-port: 12346

    local_system_ip: 1.1.1.1

    remote_system_ip: 2.2.2.2

    local_color: 2 [mpls], remote_color: 2 [mpls]

    wan_ifindex: 8 [GigabitEthernet2], tun_ifindex: 15 [Tunnel0]

    tun_adj_id: 0, l2_adj_id: 0x1f, tunnel_qos_dpidx: 0x0

    bfd-ld: 20005, ipsec_flow_id: 603979786, session_id: 5

    Inner-fragmentation-disable: yes
```

The example demonstrates whether the inner fragmentation is disabled or enabled in all the available overlays.

Configure TCP MSS and Clear Dont Fragment

Table 4: Feature History

Feature Name	Release Information	Description
Configure TCP MSS	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds support for TCP MSS adjustment on Cisco IOS XE Catalyst SD-WAN devices on both directions of the Cisco Catalyst SD-WAN tunnel interface.
Configure Clear Don’t Fragment Option	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides the option to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco Catalyst SD-WAN tunnel . When you clear the Don't Fragment configuration, packets larger than the interface MTU are fragmented before being sent.

TCP maximum segment size (MSS) is a parameter that specifies the largest amount of data, in bytes, that a communications device can receive in a single TCP segment, without counting the TCP header or the IP header. The MSS is specified as TCP MSS, initially in the TCP SYN packet during TCP handshake. Small MSS values reduces or eliminates IP fragmentation resulting in higher overhead.

You can configure the MSS of TCP SYN packets passing through a device. By default, the MSS is dynamically adjusted based on the interface or tunnel maximum transmission unit (MTU) such that TCP SYN packets are

never fragmented. For data sent over an interface, the MSS is calculated by adding the interface MTU, the IP header length, and the maximum TCP header length.

Limitations

- TCP MSS values can be adjusted for Cisco Catalyst SD-WAN tunnel interfaces only.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1, you can adjust the TCP MSS value for a service VPN or for Network Address Translation (NAT) Direct Internet Access (DIA) use cases. Adjusting the TCP MSS value helps prevent TCP sessions from being dropped.

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

- The option **Clear Dont Fragment** is available for Cisco Catalyst SD-WAN tunnel interfaces only.

Configure TCP MSS and Clear Dont Fragment

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

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

3. Create a new CLI add-on feature template or edit one of the following templates. You can use any of the following feature templates to configure TCP MSS and clear Dont Fragment:
   - VPN Ethernet Interface
   - VPN Interface DSL IPoE
   - VPN Interface DSL PPoA
   - VPN Interface DSL PPPoE
   - VPN Interface Multilink
   - VPN Interface T1/E1
   - Cellular Interfaces

   For information on creating a new CLI add-on feature template, see Create a CLI Add-on Feature Template.
4. Click **Tunnel**.
5. To configure TCP MSS, in **Tunnel TCP MSS**, 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

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 setting is lower than the MSS in the header. If the MSS header value is already lower than the TCP MSS, it flows 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.

6. Click the **Clear-Dont-Fragment** option to clear the Dont Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the Don't Fragment bit is cleared, packets larger than that interface's MTU are fragmented before being sent.

Note Clear-Dont-Fragment clears the Don't Fragment bit when there is fragmentation needed and the Don't Fragment bit is set. For packets that don't require fragmentation, the Don't Fragment bit is not affected.

7. Click **Save** or **Update**.

Configure TCP MSS Using CLI

Use the following command to configure TCP MSS on the CLI:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

Verify TCP MSS Configuration

The following is sample output of the **`show platform hardware qfp active feature sdwan datapath session summary`** command:

```
Device#show platform hardware qfp active feature sdwan datapath session summary
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU

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

10.1.15.25      10.1.14.14      12347    12346      IPSEC    65526    10007       1446

10.1.15.25      10.0.5.21       12347    12357      IPSEC    65526    10009       1446

10.1.15.25      10.0.5.11       12347    12347      IPSEC    65526    10008       1446

10.1.15.25      10.1.16.16      12347    12366      IPSEC    65526    10006       1446
```

Configure Clear Dont Fragment on the CLI

Use the following command to configure **Clear Dont Fragment** option using the CLI:

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment
```

Verify Dont Fragment Configuration on the CLI

The following is sample output of the **`show platform software interface rp active name Tunnel1`** command to verify if **Clear-dont-fragment** is enabled or not.

```
Device# show platform software interface rp active name Tunnel1 | include dont
IP Clear-dont-fragment: TRUE
```

The following is sample output of the **show running-config interface Tunnel1** command that displays the running configuration when **Clear-dont-fragment** is enabled.

```
Device# show running-config interface Tunnel1
Building configuration...

Current configuration : 132 bytes
!
interface Tunnel1
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end
```

Monitoring Bandwidth on a Transport Circuit

You can monitor the bandwidth usage on a transport circuit, to determine how the bandwidth usage is trending. If the bandwidth usage starts approaching a maximum value, you can configure the software to send a notification. Notifications are sent as Netconf notifications, which are sent to the Cisco SD-WAN Manager NMS, SNMP traps, and syslog messages. You might want to enable this feature for bandwidth monitoring, such as when you are doing capacity planning for a circuit or when you are gathering trending information about bandwidth utilization. You might also enable this feature to receive alerts regarding bandwidth usage, such as if you need to determine when a transport interface is becoming so saturated with traffic that a customer's traffic is impacted, or when customers have a pay-per-use plan, as might be the case with LTE transport.

To monitor interface bandwidth, you configure the maximum bandwidth for traffic received and transmitted on a transport circuit. The maximum bandwidth is typically the bandwidth that has been negotiated with the circuit provider. When bandwidth usage exceeds 85 percent of the configured value for either received or transmitted traffic, a notification, in the form of an SNMP trap, is generated. Specifically, interface traffic is sampled every 10 seconds. If the received or transmitted bandwidth exceeds 85 percent of the configured value in 85 percent of the sampled intervals in a continuous 5-minute period, an SNMP trap is generated. After the first trap is generated, sampling continues at the same frequency, but notifications are rate-limited to once per hour. A second trap is sent (and subsequent traps are sent) if the bandwidth exceeds 85 percent of the value in 85 percent of the 10-second sampling intervals over the next 1-hour period. If, after 1 hour, another trap is not sent, the notification interval reverts to 5 minutes.

You can monitor transport circuit bandwidth on Cisco IOS XE Catalyst SD-WAN devices and on Cisco SD-WAN Manager NMSs.

To generate notifications when the bandwidth of traffic received on a physical interface exceeds 85 percent of a specific bandwidth, configure the downstream bandwidth:

To generate notifications when the bandwidth of traffic transmitted on a physical interface exceeds 85 percent of a specific bandwidth, configure the upstream bandwidth:

In both configuration commands, the bandwidth can be from 1 through 2147483647 (2^{32} / 2) – 1 kbps.

To display the configured bandwidths, look at the bandwidth-downstream and bandwidth-upstream fields in the output of the **show interface detail** command. The rx-kbps and tx-kbps fields in this command shows the current bandwidth usage on the interface.

Enable DHCP Server using Cisco SD-WAN Manager

Table 5: Feature History

Feature Name	Release Information	Feature Description
DHCP Option Support	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges.

Use the DHCP-Server template for all Cisco Catalyst SD-WANs.

You enable DHCP server functionality on a Cisco Catalyst SD-WAN device interface so it can assign IP addresses to hosts in the service-side network.

To configure a Cisco Catalyst SD-WAN device to act as a DHCP server using Cisco SD-WAN Manager templates:

1. Create a DHCP-Server feature template to configure DHCP server parameters, as described in this topic.
2. Create one or more interface feature templates, as described in the VPN-Interface-Ethernet and the VPN-Interface-PPP-Ethernet help topics.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

To configure a Cisco IOS XE Catalyst SD-WAN device interface to be a DHCP helper so that it forwards broadcast DHCP requests that it receives from DHCP servers, in the DHCP Helper field of the applicable interfaces template, enter the addresses of the DHCP servers.

Navigate to the Template Screen and Name the Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then click **Create Template**.

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

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Service VPN** or scroll to the **Service VPN** section.
6. Click **Service VPN** drop-down list.
7. From **Additional VPN Templates**, click **VPN Interface**.
8. From the **Sub-Templates** drop-down list, choose **DHCP Server**.
9. From the **DHCP Server** drop-down list, click **Create Template**. The DHCP-Server template form is displayed.

This form contains fields for naming the template, and fields for defining the DHCP Server parameters.

10. In **Template Name**, enter a name for the template.

    The name can be up to 128 characters and can contain only alphanumeric characters.

11. 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.

Minimum DHCP Server Configuration

To configure DHCP server functionality, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk as required to configure DHCP servers.

Table 6:

Parameter Name	Description
Address Pool*	Enter the IPv4 prefix range, in the format *prefix/length*, for the pool of addresses in the service-side network for which the router interface acts as DHCP server.
Exclude Addresses	Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma. To specify a range of addresses, separate them with a hyphen.
Maximum Leases	Specify the number of IP addresses that can be assigned on this interface.*Range:* 0 through 4294967295
Lease Time	Specify how long a DHCP-assigned IP address is valid.*Range:* 0 through 4294967295 seconds
Offer Time	Specify how long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client.*Range:* 0 through 4294967295 secondsDefault: 600 seconds
Administrative State	Select Up to enable or Down to disable the DHCP functionality on the interface. By default, DHCP server functionality is disabled on an interface.

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

Configure Static Leases

To configure a static lease to assign a static IP address to a client device on the service-side network, click **Static Lease**, and click **Add New Static Lease** and configure the following parameters:

Table 7:

Parameter Name	Description
MAC Address	Enter the MAC address of the client to which the static IP address is being assigned.
IP Address	Enter the static IP address to assign to the client.
Hostname	Enter the hostname of the client device.

To edit a static lease, click **pencil** icon.

To remove a static lease, click **trash** icon.

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

Configure Advanced Options

To configure a advanced DHCP server options, click **Advanced** and then configure the following parameters:

Table 8:

Parameter Name	Description
Interface MTU	Specify the maximum MTU size of packets on the interface.*Range:* 68 to 65535 bytes
Domain Name	Specify the domain name that the DHCP client uses to resolve hostnames.
Default Gateway	Enter the IP address of a default gateway in the service-side network.
DNS Servers	Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses.
TFTP Servers	Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma.

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

Configure DHCP server using CLI

```
Device# config-transaction
Device(dhcp-config)# ip dhcp pool DHCP-POOL
Device(dhcp-config)# network 10.1.1.1 255.255.255.0
Device(dhcp-config)# default-router 10.1.1.2
Device(dhcp-config)# dns-server 172.16.0.1
Device(dhcp-config)# domain-name DHCP-DOMAIN
Device(dhcp-config)# exit
Device(config)ip dhcp excluded-address 10.1.1.2 10.1.1.10
Device(
```

Release Information

Introduced in Cisco SD-WAN Manager in Release 15.2.

Configuring PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) connects multiple users over an Ethernet local area network to a remote site through common customer premises equipment. PPPoE is commonly used in a broadband aggregation, such as by digital subscriber line (DSL). PPPoE provides authentication with the CHAP or PAP protocol. In the Cisco Catalyst SD-WAN overlay network, Cisco Catalyst SD-WAN devices can run the PPPoE client. The PPPoE server component is not supported.

It is recommended that you configure quality of service (QoS) and shaping rate on a PPPoE Dialer interface. Queuing based QoS policies on both Dialer interface and PPPoE-enabled physical interface at the same time, is not supported.

PPPoE-enabled physical interfaces are supported on ATM PVCs and Ethernet interfaces. A dialer interface must be used for cloning virtual access. Multiple PPPoE client sessions can be configured on an Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

The Cisco Catalyst SD-WAN implementation of PPPoE does not support the Compression Control Protocol (CCP) options, as defined in RFC 1962.

This example shows configuring PPPoE server on IPv4 interfaces:

```
!
interface Dialer100
 mtu 1492
 ip address negotiated
 encapsulation ppp
 ip tcp adjust-mss 1460
 dialer pool 100
 dialer down-with-vInterface
 ppp authentication chap callin
 ppp chap hostname cisco
 ppp chap password 7 1511021F07257A767B
 ppp ipcp route default
```

Note Follow these steps to replace a template configured with PPPoE as WAN interface with a regular interface in Dialer100:

1. Remove the IP address assigned to the dialer interface using the command:

   ```
   no ip address <ip> <mask>
   ```

2. Add a new IP address for the dialer interface.

Configure PPPoE from Cisco SD-WAN Manager Templates

To use Cisco SD-WAN Manager templates to configure PPPoE on Cisco IOS XE Catalyst SD-WAN device, you create three feature templates and one device template:

- Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface.
- Create a VPN-Interface-PPP-Ethernet feature template to configure a PPPoE-enabled interface.
- Optionally, create a VPN feature template to modify the default configuration of VPN 0.

- Create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates.

Create a VPN-Interface-PPP feature template to configure PPP parameters for the PPP virtual interface:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

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

3. Choose Cisco IOS XE Catalyst SD-WAN device Cloud or a router model.
4. Choose the **VPN-Interface-PPP** template.
5. In the template, configure the following parameters:

Table 9:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
Shutdown	Click **No** to enable the PPP virtual interface.
Interface Name	Enter the number of the PPP interface. It can be from 1 through 31.
Description (optional)	Enter a description for the PPP virtual interface.
Authentication Protocol	Select either CHAP or PAP to configure one authentication protocol, or select PAP and CHAP to configure both. For CHAP, enter the hostname and password provided by your ISP. For PAP, enter the username and password provided by your ISP. If you are configuring both PAP and CHAP, to use the same username and password for both, click Same Credentials for PAP and CHAP.
AC Name (optional)	Select the PPP tab, and in the AC Name field, enter the name of the the name of the access concentrator used by PPPoE to route connections to the Internet.
IP MTU	Click **Advanced**, and in the IP MTU field, ensure that the IP MTU is at least 8 bytes less than the MTU on the physical interface. The maximum MTU for a PPP interface is 1492 bytes. If the PPPoE server does not specify a maximum receive unit (MRU), the MTU value for the PPP interface is used as the MRU. Starting from Cisco vManage Release 20.9.1, there is 8 bytes overheads deduced based on the specified IP MTU value when configuration is pushed to the device.
Save	To save the feature template, click **Save**.

To create a VPN-Interface-PPP-Ethernet feature template to enable the PPPoE client on the physical interfaces:

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

2. Click **Feature Templates**, and click **Add Template**.

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

3. Choose Cloud or a router model.
4. Choose the **VPN-Interface-PPP-Ethernet** template.
5. In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
Shutdown	Click **No** to enable the PPPoE-enabled interface.
Interface Name	Enter the name of the physical interface in VPN 0 to associate with the PPP interface.
Description (optional)	Enter a description for the PPPoE-enabled interface.
IP Confguration	Assign an IP address to the physical interface: • To use DHCP, select Dynamic. The default administrative distance of routes learned from DHCP is 1. • To configure the IP address directly, enter of the IPv4 address of the interface.
DHCP Helper (optional)	Enter up to four IP addresses for DHCP servers in the network.
Save	To save the feature template, click **Save**.

To create a VPN feature template to configure the PPPoE-enabled interface in VPN 0, the transport VPN:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

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

3. Choose Cloud or a router model.
4. Choose the **VPN** template.
5. In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.

Parameter Field	Procedure
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
VPN Identifier	Enter VPN identifier 0.
Name	Enter aname for the VPN.
Other interface parameters	Configure the desired interface properties.
Save	To save the feature template, click **Save**.

To create a device template that incorporates the VPN-Interface-PPP, VPN-Interface-PPP-Ethernet, and VPN feature templates:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then click **Create Template**.

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

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

   Cisco SD-WAN Manager displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (*).
5. Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.
6. In **Transport & Management VPN**, under **VPN 0**, from the drop-down list of available templates, select the desired feature template. The list of available templates are the ones that you have previously created.
7. In **Additional VPN 0 Templates**, click the plus sign (+) next to **VPN Interface PPP**.
8. From **VPN-Interface-PPP** and **VPN-Interface-PPP-Ethernet** fields, select the feature templates to use.
9. To configure multiple PPPoE-enabled interfaces in VPN 0, click the plus sign (+) next to Sub-Templates.
10. To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
11. To create the device template, click **Create**.

To attach a device template to a device:

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

2. Click **Device Templates**.

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

3. Choose a template.
4. Click **…**, and click **Attach Device**.
5. Search for a device or select a device from the Available Device(s) column to the left.
6. Click the arrow pointing right to move the device to the Selected Device(s) column on the right.
7. Click **Attach**.

Configure PPPoE Over ATM

Table 10: Feature History

Feature Name	Release Information	Description
Configure PPPoE over ATM	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature provides support for configuring PPPoEoA on Cisco IOS XE Catalyst SD-WAN devices. PPPoEoA uses AAL5MUX encapsulation which delivers better efficiency compared to other encapsulation methods.

You can configure PPPoE over ATM interfaces (PPPoEoA) on Cisco IOS XE Catalyst SD-WAN devices that support ADSL. PPPoEoA uses ATM Adaptation Layer 5 Multiplexed Encapsulation (AAL5MUX) encapsulation to carry PPPoE over ATM permanent virtual circuits (PVCs), providing efficiency gain over AAL5 LLC/SNAP encapsulation.

PPPoEoA over AAL5MUX reduces Subnetwork Access Protocol (SNAP) encapsulation bandwidth usage, using multiplexed (MUX) encapsulation to reduce the number of cells needed to carry voice packets. Deploying the PPPoEoA over ATM AAL5MUX feature in a VoIP environment results in improved throughput and bandwidth usage.

Supported Platforms for PPPoE Over ATM

The following platforms support PPPoE over ATM:

- Cisco 1100 4G/6G Series Integrated Services routers.
- Cisco1100 Series Integrated Service routers.
- Cisco1109 Series Integrated Service routers.
- Cisco111x Series Integrated Service routers.
- Cisco1111x Series Integrated Service routers.

- Cisco1120 Series Integrated Service routers.
- Cisco1160 Series Integrated Service routers.

Configure PPPoE Over ATM using Cisco SD-WAN Manager

You can configure PPPoE using in Cisco SD-WAN Manager using the device CLI template.

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

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

3. From the **Create Template** drop-down list, select **CLI Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
6. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
7. Choose **Device configuration**. Using this option, you can provide IOS-XE configuration commands that appear in the output of the `show sdwan running-config` command.
8. (Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.
9. In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file. The configuration for PPPoEoA is available in the Configure PPPoE Over ATM on the CLI section.
10. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
11. Click **Add**. The new device template is displayed in the Device Template table. The **Type** column shows **CLI** to indicate that the device template was created from CLI text.

Configure PPPoE Over ATM on the CLI

This section provides example CLI configurations to configure PPoE over ATM on the CLI.

```
Device(config)# interface atm number
Device(config)# no ip address
Device(config)# interface atm number point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# encapsulation aal5mux  pppoe-client
Device(config)# pppoe-client dial-pool-number number
Device(config)# interface Dialer dialer-rotary-group-number
```

```
Device(config)# mtu bytes
Device(config)# ip address negotiated
Device(config-if)# encapsulation encapsulation-type
Device(config)# load-interval seconds
Device(config)# dialer pool number
Device(config)# dialer-group group-number
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname hostname
Device(config)# ppp chap password secret
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
```

Configuration Example for Configuring PPPoE Over ATM Interfaces

This example shows configuring PPPoE over ATM interfaces.

```
Device(config)# interface ATM0/1/0
Device(config)# no ip address
Device(config)# no atm enable-ilmi-trap
!
Device(config)# interface ATM0/1/0.10 point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# cdp enable
Device(config)# pvc 22/62
Device(config)# ubr 1045
Device(config-if)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number 120
!
!
Device(config)# interface Dialer 120
Device(config)# mtu 1492
Device(config)# ip address negotiated
Device(config)# ip nat outside
Device(config-if)# encapsulation ppp
Device(config)# load-interval 30
Device(config)# dialer pool 120
Device(config)# dialer-group 1
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname test@cisco.com
Device(config)# ppp chap password 0 cisco
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
!
```

Configuring VRRP

Note The x710 NIC must have the **t->system-> vrrp-advt-with-phymac** command configured, for VRRP to function.

The Virtual Router Redundancy Protocol (VRRP) is a LAN-side protocol that provides redundant gateway service for switches and other IP end stations. In the Cisco Catalyst SD-WAN software, you configure VRRP on an interface, and typically on a subinterface, within a VPN.

VRRP is only supported with service-side VPNs (VPN 0 and 512 reserved) and if sub-interfaces are used, then the VRRP physical interface must be configured in VPN 0.

For each VRRP interface (or subinterface), you assign an IP address and you place that interface in a VRRP group.

The group number identifies the virtual router. You can configure a maximum of 512 groups on a router. In a typical VRRP topology, two physical routers are configured to act as a single virtual router, so you configure the same group number on interfaces on both these routers.

For each virtual router ID, you must configure an IP address.

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.

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.

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:

- Track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.

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. (The default OMP hold timer interval is 60 seconds.) 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.

- Track both the OMP session and a list of remote prefixes.

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.

Configuring Dynamic Interfaces

Table 11: 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.

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

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.

Create a Dynamic Interface Mode Feature Template

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.

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

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

3. Click the **Create Template** drop-down list and choose **Feature Template**.
4. From the **Device Model** drop-down list, choose the device for which you wish to create the template.
5. In **Template Name**, enter a name for the template.

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

This field can contain any characters and spaces.

7. From **Additional Templates**, choose the **Dynamic Interface Mode** drop-down list and click **Create Template**.
8. In **Template Name**, enter a name for the template.

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

   This field can contain any characters and spaces.
10. 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.
11. Click **Save**.

Configure an Interface for Control Connections

This section describes how to configure a new VPN 0 interface for an existing control connection to operate with the bays that you configured in "Create a Dynamic Interface Mode Feature Template." It also describes how to configure an IPv4 route for the interface.

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

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

3. Click **...** of the template for which you want to configure the interface, and then choose **Edit**.
4. Click **Transport & Management VPN** and perform these actions to create interfaces for the bays:
   a. Click **VPN Interface** in the **Additional VPN 0 Template**.
   b. Choose the new **VPN Interface Ethernet** menu that displays, and then click **Create Template**.
   c. In **Template Name**, enter a name for the template.

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

      This field can contain any characters and spaces.
   e. Add control connections to the bays that you configured as described in "Create a Dynamic Interface Mode Feature Template."
5. Choose **Basic Configuration** and perform these actions:
   a. In **Interface Name**, enter a name for the interface.

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

b. Configure other options on this tab as needed.

6. From **Tunnel**, set **Tunnel Interface** to **On**.
7. Click **Save**.
8. Choose **IPv4 Route** and perform these actions to configure an IPv4 route for the VPN0 template:
   a. Click **New IPv4 Route**.
   b. In **Prefix**, enter a prefix for the IPv4 route.
   c. In **Gateway**, choose **Next Hop**.
   d. Configure items as needed in **Next Hop**, and then click **Add**.
   e. Click **Save**.
9. Click **Update**.

Associate the Dynamic Interface Mode Feature Template with a Device Template

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.

Configure VPN Ethernet Interface

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.

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.

Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, choose **Basic Configuration** and configure the following parameters:

Note Parameters marked with an asterisk are required to configure an interface.

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.
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.	

Parameter Name	IPv4 or IPv6	Options	Description
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.	

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

Create a Tunnel Interface

On Cisco IOS XE Catalyst SD-WAN devices, you can configure up to eight tunnel interfaces. This means that each Cisco IOS XE Catalyst SD-WAN device router can have up to eight TLOCs. On Cisco Catalyst SD-WAN Controllers and Cisco SD-WAN Manager, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0. The WAN interface will enable the flow of tunnel traffic to the overlay. You can add other parameters shown in the table below only after you configure the WAN interface as a tunnel interface.

To configure a tunnel interface, select **Interface Tunnel** and configure the following parameters:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
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 Catalyst SD-WAN Controller default: Disabled
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	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)
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

Associate a Carrier Name with a Tunnel Interface

To associate a carrier name or private network identifier with a tunnel interface, use the **carrier** command. *carrier-name* can be **default** and **carrier1** through **carrier8:**

```
Device(config)# interface Tunnel 0
Device(config-if)# ip unnumbered GigabitEthernet1
Device(config-if)# ipv6 unnumbered GigabitEthernet2
Device(config-if)# tunnel source GigabitEthernet1
```

```
Device(config-if)# tunnel mode sdwan
Device(config-if)# exit
Device(config)# sdwan
Device(config-sdwan)# int GigabitEthernet1
Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# carrier default
```

Create Tunnel Groups

By default, WAN Edge routers try to build tunnels with all other TLOCs in the network, regardless of color. When the restrict option is used with the color designation under the tunnel configuration, the TLOC is restricted to only building tunnels to TLOCs of the same color. For more information on the restrict option see, Configure Interfaces in the WAN Transport VPN(VPN0).

The tunnel group feature is similar to the restrict option but gives more flexibility because once a tunnel group ID is assigned under a tunnel, only TLOCs with the same tunnel group IDs can form tunnels with each other irrespective of color.

If a TLOC is associated with a tunnel group ID, it continues to form tunnels with other TLOCs in the network that are not associated with any tunnel group IDs.

Note The restrict option can still be used in conjunction with this feature. If used, then an interface with a tunnel group ID and restrict option defined on an interface will only form a tunnel with other interfaces with the same tunnel group ID and color.

Configure Tunnel Groups on Cisco IOS XE Catalyst SD-WAN devices Using CLI

To configure tunnel groups on Cisco IOS XE Catalyst SD-WAN devices:

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet2

Device(config-interface-GigabitEthernet2)# tunnel-interface
Device(config-tunnel-interface)#group Group ID
```

Limit Keepalive Traffic on a Tunnel Interface

By default, Cisco IOS XE Catalyst SD-WAN devices send a Hello packet once per second to determine whether the tunnel interface between two devices is still operational and to keep the tunnel alive. The combination of a hello interval and a hello tolerance determines how long to wait before declaring a DTLS or TLS tunnel to be down. The default hello interval is 1 second, and the default tolerance is 12 seconds. With these default values, if no Hello packet is received within 11 seconds, the tunnel is declared down at 12 seconds.

If the hello interval or the hello tolerance, or both, are different at the two ends of a DTLS or TLS tunnel, the tunnel chooses the interval and tolerance as follows:

- For a tunnel connection between two controller devices, the tunnel uses the lower hello interval and the higher tolerance interval for the connection between the two devices. (Controller devices are Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controller.) This choice is made in case one of the controllers has a slower WAN connection. The hello interval and tolerance times are chosen separately for each pair of controller devices.

- For a tunnel connection between a Cisco IOS XE Catalyst SD-WAN device and any controller device, the tunnel uses the hello interval and tolerance times configured on the router. This choice is made to minimize the amount 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 Cisco IOS XE Catalyst SD-WAN device and a controller device.

To minimize the amount of keepalive traffic on a tunnel interface, increase the Hello packet interval and tolerance on the tunnel interface:

```
Device(config-tunnel-interface)#  hello-interval milliseconds
Device(config-tunnel-interface)#  hello-tolerance 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). The hello tolerance interval must be at most one-half the OMP hold time. The default OMP hold time is 60 seconds, and you configure it with the **omp timers holdtime** command.

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.*

Apply Access Lists and QoS Parameters

Quality of service (QoS) helps determine how a service will perform. By configuring QoS, enhance the performance of an application on the WAN. To configure a shaping rate for an interface and to apply a QoS map, a rewrite rule, access lists, and policers to a interface, click **ACL/QoS**, and configure the following parameters:

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.

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

Add ARP Table Entries

The Address Resolution Protocol (ARP) helps associate a link layer address (such as the MAC address of a device) to its assigned internet layer address. Configure a static ARP address when dynamic mapping is not functional. To configure static ARP table entries on the interface, select ARP. Then click **Add New ARP** and configure the following parameters:

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

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

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

Configuring VRRP

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. **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

You can configure prefix list tracking for VRRP using device and feature templates. To configure a prefix list, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy**.
2. Click **Localized Policy**.
3. From the **Custom Options** drop-down list, click **Lists**.
4. Click **Prefix** from the left pane, and click **New Prefix List**.
5. In **Prefix List Name**, enter a name for the prefix list.
6. Choose **IPv4** as the **Internet Protocol**.
7. In **Add Prefix**, enter the prefix entries separated by commas.
8. Click **Add**.
9. Click **Next** and configure **Forwarding Classes/QoS**.
10. Click **Next** and configure **Access Control Lists**.
11. Click **Next** and in **Route Policy** pane, select a relevant route policy and click **…** , and click **Edit** to add the newly added prefix list.
12. From the **Match** pane, click **AS Path List** and in the **Address**, choose the newly added prefix list.
13. Click **Save Match and Actions**.
14. Click **Next** and enter the **Policy Name** and **Policy Description** in the **Policy Overview** screen.

15. Click **Save Policy**.

Configure a Prefix List for VRRP in the Device Template

To configure the Prefix List to the VRRP and the localized policy in the device template, do the following:

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

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

3. Select a relevant device template and click **…** and click **Edit** to edit the template details.
4. From **Policy**, select the policy with the newly added prefix list.
5. Click **Update**.
6. Click **Feature Templates**.
7. Select a relevant device template and click **…** and click **Edit** to edit the template details.
8. Click **VRRP**.
9. Select a relevant group ID and click the pen icon to associate the new prefix-list to the VRRP details.
10. Click the **Track Prefix List** drop-down list and enter the newly added prefix-list name.
11. Click **Save Changes**.
12. Click **Update** to save the changes.
13. Click **Device Templates** and select the policy with the newly added prefix list.
14. Click **…** and click **Attach Devices**.
15. From **Available Devices**, double-click the relevant device to move it to **Selected Devices**, and then click **Attach**.

Configure Advanced Properties

To configure other interface properties, select the **Advanced** tab and configure the following parameters:

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.

Parameter Name	Description
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.
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.

Parameter Name	Description
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.

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

VPN Interface Bridge

Use the VPN Interface Bridge template for all Cisco IOS XE Catalyst SD-WAN device Cloud and Cisco IOS XE Catalyst SD-WAN devices.

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.

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, as described in this article.
2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters. See the Bridge help topic.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Service VPN** or scroll to the **Service VPN** section.

6. Click the **Service VPN** drop-down list.
7. From **Additional VPN Templates**, click **VPN Interface Bridge**.
8. 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.
9. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. 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 to the left of the parameter field and select one of the following:

Table 12:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 15.3. In Release 18.2, add support for disabling ICMP redirect messages.

Create a Bridging Interface

To configure an interface to use for bridging servers, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure bridging.

Table 13:

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.

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

Apply Access Lists

Apply Access Lists

To 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 14:

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.

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

Configure VRRP

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 15:

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 twoCisco 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: 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.
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.

To save the VRRP configuration, click **Add**.

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

Add ARP Table Entries

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

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.

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

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

Configure Advanced Properties

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

Table 17:

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

Parameter Name	Description
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)
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.

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

VPN Interface DSL IPoE

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

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.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL IPoE**.
7. 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.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 18:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure IPoE Functionality

To configure basic IPoE functionality, click **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

Table 19:

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.

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

Configure the Ethernet Interface

Configuring an Ethernet interface with PPPoE allows multiple users on a LAN to be connected to a remote site. To configure an Ethernet interface on the VDSL controller, click **Ethernet** and configure the following parameters. You must configure all parameters.

Table 20:

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.

Parameter Name	Description
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.

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

Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

Table 21:

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

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 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 Catalyst 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 Catalyst 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 Catalyst 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
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
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
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 22:

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.

Parameter Name	Description
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.
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

Configure the Interface as a NAT Device

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

Table 23:

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 24:

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

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

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

Apply Access Lists

Configure ACLs to selectively indicate what traffic will enjoy the benefits of QoS. To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

Table 25:

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.

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

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 26:

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

Parameter Name	Description
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
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.

Parameter Name	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.

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

Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.4.1.

VPN Interface DSL PPPoA

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.

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, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.

5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoA**.
7. 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.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 27:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click **Device Specific**, the **Enter Key box** opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

Table 28:

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

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

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

Configure the ATM Interface

To configure an ATM interface on the VDSL controller, select **ATM** and configure the following parameters. You must configure all parameters.

Table 29:

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).

Parameter Name	Description
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.
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.

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

Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

Table 30:

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 255 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

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

Create a Tunnel Interface

On Cisco IOS XE Catalyst SD-WAN devices, you can configure up to eight tunnel interfaces. This means that each Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

Table 31:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
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 Catalyst 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 Catalyst 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 Catalyst 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
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
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 32:

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.

Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

Table 33:

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.

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

Configure Other Interface Properties

To configure other interface properties, select **Advanced** and configure the following properties:

Table 34:

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.

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

Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.3.

VPN Interface DSL PPPoE

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

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

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

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

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
6. Under **Additional VPN 0 Templates**, click **VPN Interface DSL PPPoE**.
7. From the **VPN Interface DSL PPPoE** drop-down list, click **Create Template**. The VPN Interface DSL PPPoE template form is displayed. This form contains fields for naming the template, and fields for defining PPPoE Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

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

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

Table 35:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

Note 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 36:

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.

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

Configure the Ethernet Interface on VDSL Controller

To configure an Ethernet interface on the VDSL controller, select **Ethernet** and configure the following parameters. You must configure all parameters.

Table 37: 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.

Table 38:

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.

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

Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

Table 39:

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 255 characters. • **PAP**—Enter the username and password that are provided by your ISP. *username* can be up to 255 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

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

Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

Table 40:

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

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 Catalyst 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 Catalyst 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 Catalyst 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
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.
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 41:

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.

Parameter Name	Description
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.
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.

Configure the Interface as a NAT Device

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

Table 42:

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 43:

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

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

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

Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

Table 44:

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.

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

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 45:

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.

Parameter Name	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 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.

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

Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.3.

VPN Interface Ethernet PPPoE

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

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

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

1. Create a VPN Interface Ethernet PPPoE feature template to configure Ethernet PPPoE interface parameters, as described in this section.
2. Create a VPN feature template to configure VPN parameters. See VPN help topic.

Navigate to the Template Screen and Name the Template

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

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

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

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

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

8. In **Template Name**, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 46:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template . When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco Catalyst SD-WAN device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure PPPoE Functionality

To configure basic PPPoE functionality, click **Basic Configuration** and configure the following parameters. Required parameters are indicated with an asterisk.

Table 47:

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

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

Configure the PPP Authentication Protocol

To configure the PPP Authentication Protocol, click **PPP** and configure the following parameters. Required parameters are indicated with an asterisk.

Table 48:

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 255 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

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

Create a Tunnel Interface

On IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

Table 49:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
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 Catalyst 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 Catalyst 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 Catalyst 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
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
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 50:

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. **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)
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

Configure the Interface as a NAT Device

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

Table 51:

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

Parameter Name	Description
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 52:

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

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

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

Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, click **ACL** and configure the following parameters:

Table 53:

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.

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.
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.

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

Configure Other Interface Properties

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

Table 54:

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.

Parameter Name	Description
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.

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

Release Information

Introduced in Cisco SD-WAN Manager NMS in Release 18.4.1.

Cisco VPN Interface GRE

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.

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 Catalyst SD-WAN Controller that applies to the service VPN, including a **set-service** *service-name* **local** command.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
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 **VPN Interface GRE**.

c. From the **VPN Interface GRE** drop-down list, click **Create Template**. The VPN Interface GRE template form is displayed.

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

6. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
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 to the left of the parameter field and select the paramater scope.

Configuring a Basic GRE Interface

To configure a basic GRE interface, click **Basic Configuration** and then configure the following parameters. Parameters marked with an asterisk are required to configure a GRE interface.

Table 55:

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.
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

Parameter Name	Description
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 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 to 1460 bytes *Default:* None

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

Configure Interface Access Lists

To configure access lists on a GRE interface, click **ACL** and configure the following parameters:

Table 56:

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.

Configure Tracker Interface

To configure a tracker interface to track the status of a GRE interface, select **Advanced** and configure the following parameter:

Table 57:

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

GRE-in-UDP

Table 58: Feature History

Feature Name	Release Information	Description
GRE-in-UDP	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco Catalyst SD-WAN Control Components Release 20.11.1	You can configure GRE encapsulation for UDP transport.

Information About GRE-in-UDP

Cisco Catalyst SD-WAN supports generic routing encapsulation (GRE) with UDP for IPv4 and IPv6 traffic.

With a GRE-in-UDP tunnel, a router encapsulates GRE packets, containing information such as the source and destination ports, within a UDP header. The router sends the UDP packet through the tunnel. The destination device de-encapsulates the UDP packet.

Supported Devices for GRE-in-UDP

Cisco IOS XE Catalyst SD-WAN devices.

Prerequisites for GRE-in-UDP

Configure GRE encapsulation.

Restrictions for GRE-in-UDP

Any restricitions that apply to GRE encapsulaton apply to GRE-in-UDP.

Configure GRE-in-UDP Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

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

You can configure GRE-in-UDP tunnel only through a CLI template.

1. For the desired interface, enter interface configuration mode.

```
sdwan
interface interface
```

2. Enter tunnel interface mode.

   ```
   tunnel-interface
   ```

3. Configure GRE encapsulation.

   ```
   encapsulation gre
   ```

4. Configure GRE-in-UDP as the encapsulation mode.

   ```
   gre-in-udp
   ```

Example

Here is a complete example of configuring GRE-in-UDP.

```
interface GigabitEthernet1
  tunnel-interface
   encapsulation gre
   color lte
   gre-in-udp
   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
```

VPN Interface IPsec

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 65530, except for 512.

Cisco 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.

Create VPN IPsec Interface Template

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

Step 2 Click **Feature Templates**.

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

Step 3 Click **Add Template**.

Step 4 Choose a Cisco IOS XE Catalyst SD-WAN device from the list.

Step 5 From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.

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.

Basic Configuration

To configure a basic IPsec tunnel interface select **Basic Configuration** and configure the following parameters:

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

CLI Equivalent

```
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
```

Configure Dead-Peer Detection

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, click DPD and configure the following parameters:

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

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

CLI Equivalent

```
crypto
   ikev2
      profile ikev2_profile_name
         dpd 10-3600 2-60 {on-demand | periodic}
```

Configure IKE

Table 59: 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.

To configure IKE, click **IKE** and configure the following parameters:

Note 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.

IKE Version 1 and IKE Version 2

To configure the IPsec tunnel that carries IKEv1 and IKEv2 traffic, click **IPSEC** and configure the following parameters:

Parameter Name	Options	Description
IKE Version	**1** IKEv1 **2** IKEv2	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. *Default*: IKEv1

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

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

Change the IKE Version from IKEv1 to IKEv2

To change the IKE version, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and then click **Add Template**.

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

3. Choose the device for which you are creating the template.
4. Click **Basic Configuration**.
5. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
6. Remove the ISAKMP profile from the IPsec profile.

7. Attach the IKEv2 profile with the IPsec profile.

Note Perform this step if you already have an IKEv2 profile. Otherwise, create an IKEv2 profile first.

8. Use the **shutdown** parameter with the **no** option (**no shutdown**) to start up the tunnel.

Note You must issue the **shutdown** operations in two separate operations.

Note 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.

CLI Equivalents for IKEv1

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
```

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
```

Summary Steps

1. enable
2. configure terminal
3. crypto isakmp policy *priority*
4. encryption {des | 3des | aes | aes 192 | aes 256 }

5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

CLI Equivalent 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
```

Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries Internet Key Exchange (IKE) traffic, click IPsec and configure the following parameters:

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

Note Starting 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.

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

CLI Equivalent

```
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
```

VPN Interface Multilink

Use the VPN Interface Multilink template for Cisco IOS XE Catalyst SD-WAN devices running the Cisco Catalyst SD-WAN software.

Note 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. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

To configure multilink on Cisco IOS XE Catalyst SD-WAN Device using Cisco SD-WAN Manager templates:

1. Create a VPN Interface Multilink feature template to configure multilink interface properties.
2. Optionally, create a VPN feature template to modify the default configuration of VPN 0.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. If you are configuring the multilink interface in the transport VPN (VPN 0):
   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under Additional VPN 0 Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.
6. If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0):
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. In the Service **VPN** drop-down list, enter the number of the service VPN.
   c. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.
7. 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.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Table 60:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template . When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure a Multilink Interface

To configure a multilink interface, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

Note 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 61:

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.

Parameter Name	Description
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.
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

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

Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select **PPP** and configure the following parameters:

Table 62:

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 255 characters. • **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters. • **PAP** and **CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.

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

Create a Tunnel Interface

You can configure up to eight tunnel interfaces. This means that each device can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the **Tunnel Interface** tab and configure the following parameters:

Table 63:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
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 Catalyst 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

Parameter Name	Description
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 Catalyst SD-WAN Controller that the tunnel interface is not allowed to connect to. *Range:* 0 through 100
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
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
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 64:

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.
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

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

Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select **ACL** and configure the following parameters:

Table 65:

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.

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

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 66:

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.

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

Release Information

Introduced in Cisco SD-WAN Manager in Release 18.3.

Configure VPN Interface SVI using Cisco SD-WAN Manager

Use the VPN Interface SVI template to configure SVI for Cisco IOS XE Catalyst SD-WAN devices. You configure a switch virtual interface (SVI) to configure 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.

Create VPN Interface SVI Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. In **Device Templates**, click **Create Template**.

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

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

4. From the **Device Model** drop-down, choose the type of device for which you are creating the template.
5. If you are configuring the SVI in the transport VPN (VPN 0):
   a. Click **Transport & Management VPN**, or scroll to the Transport & Management VPN section.
   b. Under Additional VPN 0 Templates, click **VPN Interface SVI**.
6. If you are configuring the SVI in a service VPN (VPNs other than VPN 0):
   a. Click **Service VPN**, or scroll to the Service VPN section.
   b. In the **Service VPN** drop-down list, enter the number of the service VPN.
   c. Under **Additional VPN Templates**, click **VPN Interface SVI**.
7. From the **VPN Interface SVI** drop-down, click **Create Template**. The VPN Interface SVI template form is displayed.

   The form contains fields for naming the template, and fields for defining VLAN Interface parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you open a feature template initially, 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 next to the parameter field.

Note To get the SVI interface up and functional, ensure that the appropriate VLAN is explicitly configured on the Switch Port Access or Trunk interface.

Configure Basic Interface Functionality

Table 67: 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.

To configure basic VLAN interface functionality in a VPN, choose **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 68:

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

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

Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, choose **ACL** and configure the following parameters:

Table 69:

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.

Parameter Name	Description
Egress Policer	Click **On** and specify the name of the policer to apply to packets being transmitted on the interface.

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

Configure VRRP

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
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.

Add ARP Table Entries

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

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.

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

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

Configure Other Interface Properties

To configure other interface properties, choose **Advanced** and configure the following properties:

Table 72:

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)

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

VPN Interface T1/E1

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.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:

Note **Note**: 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. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

   a. Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
   b. Under **Additional VPN 0 Templates**, click **VPN Interface T1/E1 Serial**.
   c. From the **VPN Interface T1/E1 Serial** drop-down list, click **Create Template**. The **VPN Interface T1/E1** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.

6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. Click the **Service VPN** drop-down list.
   c. Under **Additional VPN** templates, click **VPN Interface**.
   d. From the **VPN Interface** drop-down list, click **Create Template**. The **VPN Interface Ethernet** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.

7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. 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 to the left of the parameter field.

Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select **Basic Configuration** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 73:

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.
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

Create a Tunnel Interface

On Cisco IOS XE routers, you can configure up to eight tunnel interfaces. This means that each router can have up to eight TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select **Tunnel Interface** and configure the following parameters:

Table 74:

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

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 Catalyst 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 Catalyst 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 Catalyst 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
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
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.

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

Release Information

Introduced in Cisco vManage Release 18.2.

T1/E1 Controller

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.

Navigate to the Template Screen and Name the Template

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

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

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
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 **VPN Interface**.
   c. From the **VPN Interface** drop-down list, click **Create Template**. The **VPN Interface T1/E1** template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
   a. Click **Service VPN** or scroll to the **Service VPN** section.
   b. Click the **Service VPN** drop-down list.
   c. Under **Additional VPN** templates, click **VPN Interface**.
   d. From the **VPN Interface** drop-down list, click **Create Template**. The VPN Interface Ethernet template form is displayed. This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
7. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. 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 and select one of the following:

- Device Specific (indicated by a host icon)
- Global (indicated by a globe icon)

Configure a T1 Controller

To configure a T1 controller, click **T1** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 75:

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.
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

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

Configure an E1 Controller

To configure an E1 controller, click **E1** and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 76:

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.

Parameter Name	Description
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.
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

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

Release Information

Introduced in Cisco vManage Release 18.1.1.

Cellular Interfaces

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

A cellular network is commonly used as a backup WAN link, to provide network connectivity if all the wired WAN tunnel interfaces on the router become unavailable. You can also use a cellular network as the primary WAN link for a branch office, depending on usage patterns within the branch office and the data rates supported by the core of the service provider's cellular network.

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

Configure Cellular Interfaces Using Cisco SD-WAN Manager

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

1. Create a VPN Interface Cellular feature template to configure cellular module parameters, as described in this section.
2. Create a Cellular Profile template to configure the profiles used by the cellular modem.
3. Create a VPN feature template to configure VPN parameters.

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

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

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

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

Create VPN Interface Cellular

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

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

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

   This form contains fields for naming the template, and fields for defining the VPN Interface Cellular parameters.
8. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

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

Configure Basic Cellular Interface Functionality

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

Table 77:

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

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

Create a Tunnel Interface

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

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

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

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

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

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

Table 78:

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.

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

Configure the Cellular Interface as a NAT Device

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

Table 79:

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 80:

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

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

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

Apply Access Lists

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

Table 81: 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.

Parameter Name	Description
Ingress policer	Click **On**, and specify the name of the policer to apply to packets being received on the interface.
Egress policer	Click **On**, and specify the name of the policer to apply to packets being transmitted on the interface.

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

Add ARP Table Entries

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

Table 82:

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

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

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

Configure Other Interface Properties

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

Table 83: 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.

Parameter Name	Description
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	From the drop-down, select **Global**. Click **On** for IP directed-broadcast. Default: **Off**

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

Configure Cellular Interfaces Using CLI

The following example enables a cellular interface:

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

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

Data Profile

Table 84: Feature History

Feature Name	Release Information	Description
Ability to Configure APNs under Running Configurations for Single and Dual SIMs	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature allows you to create a data profile for a cellular device.

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

- Identification number of the data profile
- Name of the access point network of the service provider
- Authentication type used for APN access: No authentication, CHAP authentication only, PAP authentication only, or either CHAP or PAP authentication

- Username and password that are provided by the service provider for APN access authentication, if authentication is used
- Type of packet data matching that is used for APN access: IPv4 type bearer, IPv6 type bearer, or IPv4v6 type bearer
- SIM slot that contains the SIM to configure

Best Practices for Configuring Cellular Interfaces

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

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

  When the configurations are activated on the edge device with cellular interfaces, then all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a BFD connection, the circuit of last resort shuts itself down.

  Only when all the primary interfaces lose their connections to remote edges, then the circuit of last resort activates itself triggering a BFD TLOC Down alarm and a Control TLOC Down alarm on the edge device. The last resort interfaces are used as backup circuit on edge device and are activated when all other transport links BFD sessions fail. In this mode the radio interface is turned off, and no control or data connections exist over the cellular interface.

  Use the **last-resort-circuit** command to configure a cellular interface to be a circuit of last resort.

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

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

  - Increase control packet timers—To minimize control traffic on a cellular interface, you can decrease how often protocol update messages are sent on the interface. OMP sends Update packets every second, by default. You can increase this interval to a maximum of 65535 seconds (about 18 hours) by including the **omp timers advertisement-interval** configuration command. BFD sends Hello packets every second, by default. You can increase this interval to a maximum of 5 minutes (300000 milliseconds) by including the **bfd color hello-interval** configuration command. (Note that you specify the OMP Update packet interval in seconds and the BFD Hello packet interval in milliseconds.)

  - Prioritize Cisco SD-WAN Manager control traffic over a non-cellular interface: When a edge device has both cellular and non-celluar transport interfaces, by default, the edge device chooses one of the interfaces to use to exchange control traffic with the Cisco SD-WAN Manager. You can configure the edge device to never use the cellular interface to exchange traffic with the Cisco SD-WAN

Manager, or you can configure a lower preference for using the cellular interface for this traffic. You configure the preference by including the **vmanage-connection-preference** command when configuring the tunnel interface. By default, all tunnel interface have a Cisco SD-WAN Manager connection preference value of 5. The value can range from 0 through 8, where a higher value is more preferred. A tunnel with a preference value of 0 can never exchange control traffic with the Cisco SD-WAN Manager.

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