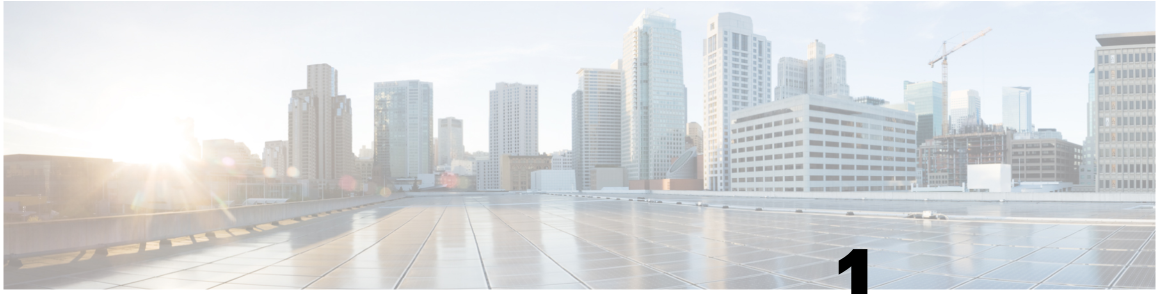
Bridging, Routing, Segmentation, and QoS Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12

First Published: 2019-04-25

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

CONTENTS



CHAPTER 1

What's New for Cisco SD-WAN

This chapter describes what's new in Cisco SD-WAN for each release.

What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r

This section applies to Cisco IOS XE SD-WAN devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: What's New for Cisco IOS XE SD-WAN Devices

Feature	**Description**
Getting Started	
API Cross-Site Request Forgery Prevention	This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can put requests on an allowed list so that they do not require protection if needed. See Cross-Site Request Forgery Prevention.
Systems and Interfaces	
IPv6 Support for NAT64 Devices	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices. See IPv6 Support for NAT64 Devices.
Secure Shell Authentication Using RSA Keys	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server. See SSH Authentication using vManage on Cisco XE SD-WAN Devices. See Configure SSH Authentication.

Feature	Description
DHCP option support	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. See Configure DHCP.
Communication with an UCS-E Server	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template. See Create a UCS-E Template.
Bridging, Routing, Segmentation, and QoS	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. See QoS on Subinterface.
Policies	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See Configure and Monitor Packet Duplication. See Configure and Monitor Packet Duplication.
Control Traffic Flow Using Class of Service Values	This feature lets you control the flow of traffic into and out of a Cisco device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. See Configure Localized Data Policy for IPv4 Using Cisco vManage.
Integration with Cisco ACI	The Cisco SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI. See Integration with Cisco ACI.
Encryption of Lawful Intercept Messages	This feature encrypts lawful intercept messages between a Cisco IOS XE SD-WAN device and a media device using static tunnel information. See Encryption of Lawful Intercept Messages.
Security	
High-Speed Logging for Zone-Based Firewalls	This feature allows a firewall to log records with minimum impact to packet processing. See Firewall High-Speed Logging.
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See *Apply Policy to a Zone Pair* in Use the Policy Configuration Wizard.
Secure Communication Using Pairwise IPsec Keys	This feature allows you to create and install private pairwise IPsec session keys for secure communication between IPsec devices and its peers. See IPSec Pairwise Keys Overview.
Network Optimization and High Availability	

Feature	Description
TCP Optimization	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput. See TCP Optimization: Cisco XE SD-WAN Routers.
Share VNF Devices Across Service Chains	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. See Share VNF Devices Across Service Chains.
Monitor Service Chain Health	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. See Monitor Service Chain Health.
Manage PNF Devices in Service Chains	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. See Manage PNF Devices in Service Chains.
Devices	
Cisco 1101 Series Integrated Services Routers	Cisco SD-WAN capability can now be enabled on Cisco 1101 Series Integrated Services Routers.
Commands	
Loopback interface support for WAN (IPsec)	This feature allows you to configure a loopback transport interface on a Cisco IOS XE SD-WAN device for troubleshooting and diagnostic purposes. See the bind command.

CHAPTER 2

Bridging

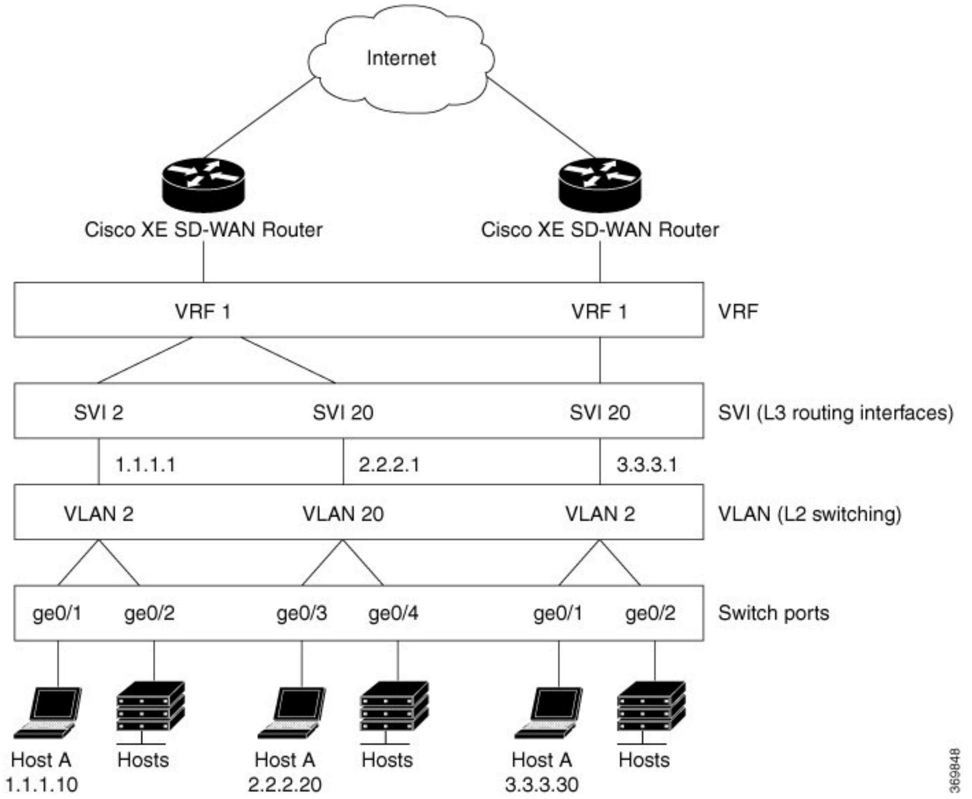
A Cisco IOS XE SD-WAN device can act as a transparent bridge, switching traffic between LANs that are part of a Virtual Local Area Network (VLAN) at the site of local router. To implement bridging, each VLAN acts as a separate broadcast domain, and each has its own Ethernet switching table (or MAC table) to use for switching traffic within the broadcast domain. Multiple VLANs can coexist in a single Cisco IOS XE SD-WAN device.

To allow hosts associated with different VLANs to communicate with each other, Cisco IOS XE SD-WAN devices support Switch Virtual Interface (SVI). SVIs provide Layer 3 routing services to allow traffic exchange between various VLANs. Each VLAN can have a single SVI.

Components of Bridging

The following figure illustrates the components of bridging in Cisco SD-WAN for Cisco IOS XE SD-WAN devices.

Figure 1: Components of Bridging



VLANs

What is a VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs provide the means to divide LAN into smaller broadcast domains. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any device port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a device supporting fallback bridging. In a device stack, VLANs can be formed with ports across the stack. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the device is assigned manually on an interface-by-interface basis. When you assign device interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership. Traffic between VLANs must be routed. The device can route traffic between VLANs by using device virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

Ports that connect to WAN segments are associated with VLANs. In the Cisco SD-WAN overlay network, these ports are the physical Gigabit Ethernet interfaces on Cisco IOS XE SD-WAN devices. Specifically, they are the base interfaces, for example, Gi0/1/0.

There is a one-to-one association between an SVI and a VLAN. An SVI can be associated only with one VLAN, and the other way around.

Native VLANs

Native VLAN is used primarily on trunk ports. VLAN provides backwards compatibility for devices that do not support VLAN tagging. For example, native VLAN allows trunk ports to accept all traffic regardless of what devices are connected to the port. Without native VLAN, the trunk ports would accept traffic only from devices that support VLAN tagging.

SVI

VLANS divide a LAN into smaller broadcast domains. Each VLAN is a separate broadcast domain, and switching within that domain directs traffic to destinations within the VLAN. The result is that hosts within a single bridge domain can communicate among themselves, but cannot communicate with hosts in other VLANs.

The only way for the traffic to cross Layer 2 VLAN boundaries to allow communication between VLANs is through Layer 3 routing. Switch Virtual Interfaces (SVI) on Cisco IOS XE SD-WAN devices is designed to provide basic Layer 3 functions for the Layer 2 switch ports that belong to a specific VLAN. SVI is a logical interface that inherits all the properties of a regular interface, but is not associated with a port or with a physical interface.

The switch ports on Cisco IOS XE SD-WAN devices do not natively support Layer 3 addresses. They must be assigned to an SVI and use a VLAN interface to enable Layer 3 features.

To configure IP routing, you need to assign IP addresses to Layer 3 network interfaces, in this case SVI. This enables communication with the hosts on those interfaces that use IP. IP routing is disabled by default, and no IP addresses are assigned to Switch Virtual Interfaces (SVIs).

VRF

Virtual Routing and Forwarding (VRF) associates a VRF instance with an SVI to map VLANs to different logical or physical VPN WAN connections. VRF allows a single physical router to have multiple route tables to enable multiple routing instances. In a single network component, multiple VRF resources create the isolation between virtual networks.

VLAN and Switchport Support

Cisco 1000 Series Integrated Services Routers and Cisco 4000 Series Integrated Services Routers with NIM-ES modules support switchports and VLANs.

Supported Switch Modules

The following switch modules are supported.

- NIM-ES2-4: Single-wide NIM form factor

- NIM-ES2-8: Single-wide NIM form factor
- NIM-ES2-8-P: Single-wide NIM form factor

Restrictions for Cisco IOS XE SD-WAN Devices

- Configuring MAC aging time per VLAN is not supported. You can only configure global MAC aging time.
- Setting a maximum limit for MAC addresses per VLAN is not supported.
- Configuring a single static MAC address on multiple switch ports is not supported.
- Packet statistics is not supported on VLANs.
- Bridge Domain Interface (BDI) is not supported on the Cisco ASR 1000.

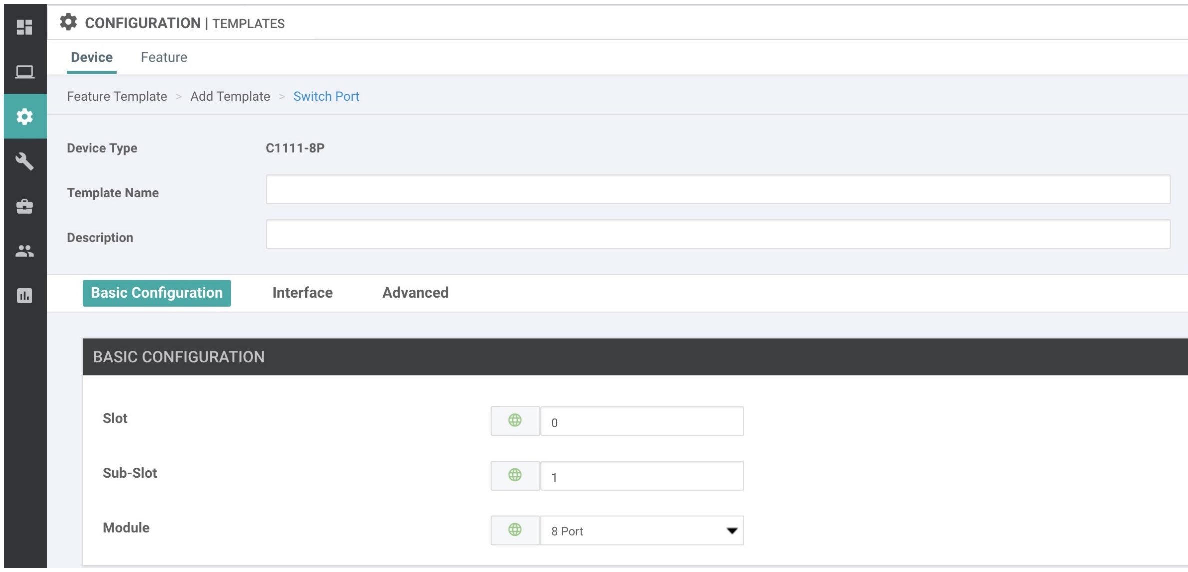
Configure Bridging Using Cisco vManage

Use the Switch Port template to configure bridging for Cisco SD-WAN.

To have a Cisco IOS XE SD-WAN device act as a bridge, configure VLANs on the router. A router can have up to 16 VLANS.

Configure Switchports

1. In Cisco vManage, choose **Configuration** > **Templates**.
2. In the Device tab, click **Create Template**.
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. Click the **Additional Templates** tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. Click the plus sign (+) next to Switch Port.
7. In the Switch Port drop-down, choose the port number.
8. If the switch port you want to choose does not exist, from the lower Switch Port drop-down, click **Create Template**. The Switch Port template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining switch port parameters.


CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > Switch Port
Basic Configuration
Interface
Advanced
BASIC CONFIGURATION

Device Type C1111-8P

Template Name

Description

Slot 0

Sub-Slot 1

Module 8 Port

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

10. In the Template Description field, 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 2:

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 Cisco SD-WAN device to a device template. 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 Basic Switch Port Parameters

To configure basic switch port parameters, select the Basic Configuration tab and configure the following parameters:

Table 3:

Parameter Name	Description
Slot	Enter the number of the slot in which the Layer 2 switch port module is installed.
Sub-Slot	Enter the number of the sub-slot.
Module	Select the switch port module type. You can choose from 4, 8, or 22 ports.

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

Associate Interfaces with the Switch Port

To associate an interface with the switch port, click the Interface tab and click **Add New Interface**.

The Wlan-GigabitEthernet0/1/8 interface applies only to C1111-8PW and C1111-8PLTExxW routers. When you configure this interface, select either **C1111-8PW** or **C1111-8PLTExxW** when you create a switch port, and select **8 port** from the Module drop-down list. In addition, from the New Interface drop-down menu, make sure to choose **Wlan-GigabitEthernet0/1/8**.

Table 4:

Parameter Name	Description
Interface Name	Enter the name of the interface to associate with the bridging domain, in the format **Gi** *slot*/*sub-slot*/*port*.
Shutdown	Click No to enable the interface. By default, an interface is disabled.
Switch Port	Select the switch port mode: • Access—Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN. • VLAN Name—Enter a description for the VLAN. • VLAN ID—Enter the VLAN number, which can be a value from 1 through 4094. • Trunk—Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLANs. • Allowed VLANs—Enter the numbers of the VLANs for which the trunk can carry traffic.a description for the VLAN. • Native VLAN ID—Enter the number of the VLAN allowed to carry untagged traffic.

Click **Save**.

To use the switch port for routing, associate it with an SVI.

Configure Other Interface Properties

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

Note For Cisco IOS XE SD-WAN devices, you cannot configure MAC age-out time and static MAC address per interface. You can only configure them globally.

Table 5:

Parameter Name	Description
Age-Out Time	Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out.*Range:* 0, 10 through 1000000 seconds*Default:* 300 seconds
Static MAC Address	Click **Add Static MAC Address** to map a MAC address to a switch port. In the MAC Static Address field that appears, enter the following: • MAC Address—Enter the static MAC address to map to the switch port interface. • Switch Port Interface Name—Enter the name of the switch port interface. • VLAN ID—Enter the number of the VLAN for the switch port. Click **Add** to save the static MAC address mapping.

Click **Save**.

Configure VPN Interface SVI using vManage

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

To configure DSL interfaces on Cisco routers using Cisco vManage templates, create a VPN Interface SVI feature template to configure VLAN interface parameters.

Create VPN Interface SVI Template

1. In Cisco vManage, choose **Configuration** > **Templates**.
2. In the **Device** tab, click **Create Template**.
3. From the **Create Template** drop-down, select **From Feature Template**.
4. From the **Device Model** drop-down, select 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 the **Transport & Management VPN** tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
    b. Under Additional VPN 0 Templates located to the right of the screen, click **VPN Interface SVI**.

6. If you are configuring the SVI in a service VPN (VPNs other than VPN 0):

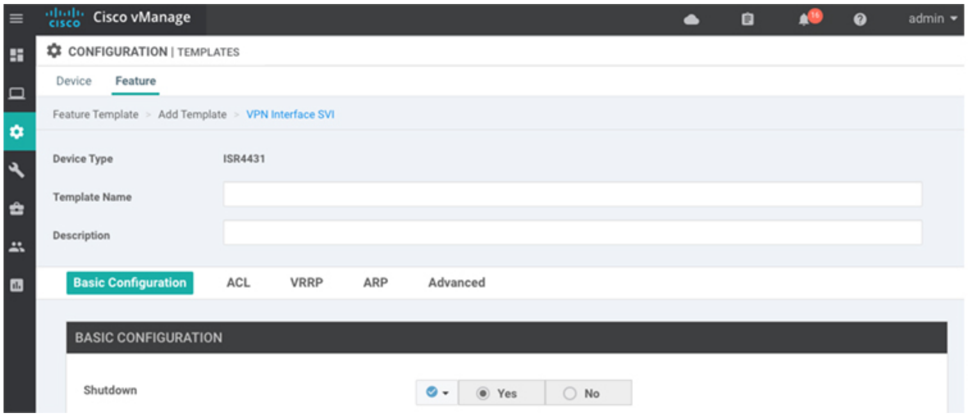
   a. Click the **Service VPN** tab located directly beneath the **Description** field, or scroll to the Service VPN section.

   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 SVI**.

7. From the **VPN Interface SVI** drop-down, click **Create Template**. The VPN Interface SVI template form is displayed.

   The top of the form contains fields for naming the template, and the bottom contains fields for defining VLAN Interface parameters.



Device Type ISR4431

Template Name

Description

Shutdown ● Yes ○ No

520036

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

9. In the **Template Description** field, 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 to the left of the parameter field.

Configure Basic Interface Functionality

Table 6: Feature History

Feature Name	Release Information	Description
Support for Configuring Secondary IP Address	Cisco IOS XE 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, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 7:

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, select the **ACL** tab and configure the following parameters:

Table 8:

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

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, select the **VRRP** tab. Then click **Add New VRRP** and configure the following parameters:

Table 9:

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 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

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 Cisco IOS XE SD-WAN device is the primary virtual router. if a Cisco IOS XE 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 one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the Cisco IOS XE 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 SD-WAN device and the peer running VRRP.

Add ARP Table Entries

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

Table 10:

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, select the Advanced tab and configure the following properties:

Table 11:

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets passing through the Cisco IOS XE 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**.

Configure Bridging Using CLI for Cisco IOS XE SD-WAN Devices

To configure bridging on Cisco IOS XE SD-WAN devices, you must create VLANs to enable L2 switching, and SVIs to enable routing traffic between various VLANs. Follow these steps to configure Bridging on Cisco IOS XE SD-WAN devices.

Configure VLANs

VLANs enable L2 switching by creating separate broadcast domains.

1. Create a VLAN.

```
vlan 10
name atm
commit
```

2. Configure a trunk interface. A trunk interface allows a switch port to carry traffic from multiple VLANs.

```
interface GigabitEthernet0/2/0
switchport mode trunk
switchport trunk allowed vlan10-20
commit
```

3. Configure native VLAN for trunk interface.

```
interface GigabitEthernet0/2/0
switchport trunk native vlan100
commit
```

4. Configure access interface.

```
interface GigabitEthernet0/2/0
switchport mode access
switchport access vlan20
commit
```

5. [Optional] Modify MAC aging time.

```
mac address-table aging-time60
commit
```

Note: Cisco IOS XE SD-WAN devices do not support modifying MAC aging-time for individual VLANs. Only global configuration on MAC aging-time is supported.

6. [Optional] Configure static MAC address.

```
mac address-table static0001.1111.1111
vlan 100 interface Gigabitethernet0/1/0
commit
```

Configuration Example

The following example shows how to attach an access mode switchport to a VLAN name.

```
config-transaction
  vlan 10
   name test
   commit
   exit
   !
 interface GigabitEthernet0/1/2
  switchport mode access
  switchport access vlan name test
  commit
```

Configure SVI

After you create VLANs to enable L2 switching between hosts, you must configure Switch Virtual Interfaces (SVI) to be able to route traffic between various VLANs.

Create an SVI interface to associate it with the VLAN you created in the Create VLAN topic.

```
interface vlan10
ip address192.0.2.1 255.255.255.0
commit
```

Run the **show ip interface brief** command to verify the creation of SVI.

```
Device# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/1/1   unassigned      YES NVRAM  up                    up

GigabitEthernet0/2/0   unassigned      YES unset  up                    up

GigabitEthernet0/2/1   unassigned      YES unset  up                    up

GigabitEthernet0       10.10.10.1      YES other  up                    up

Vlan1                  unassigned      YES unset  up                    up

Vlan10                 192.0.2.1       YES other  up                    up
```

CHAPTER 3

Unicast Overlay Routing

The overlay network is controlled by the Cisco SD-WAN Overlay Management Protocol (OMP), which is at the heart of Cisco SD-WAN overlay routing. This solution allows the building of scalable, dynamic, on-demand, and secure VPNs. The Cisco SD-WAN solution uses a centralized controller for easy orchestration, with full policy control that includes granular access control and a scalable secure data plane between all edge nodes.

The Cisco SD-WAN solution allows edge nodes to communicate directly over any type of transport network, whether public WAN, internet, metro Ethernet, MPLS, or anything else.

Supported Protocols

This section explains the protocols supported for unicast routing.

OMP Routing Protocol

The Cisco SD-WAN Overlay Management Protocol (OMP) is the protocol responsible for establishing and maintaining the Cisco SD-WAN control plane. It provides the following services:

- Orchestration of overlay network communication, including connectivity among network sites, service chaining, and VPN or VRF topologies
- Distribution of service-level routing information and related location mappings
- Distribution of data plane security parameters
- Central control and distribution of routing policy

OMP is the control protocol that is used to exchange routing, policy, and management information between Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices in the overlay network. These devices automatically initiate OMP peering sessions between themselves, and the two IP end points of the OMP session are the system IP addresses of the two devices.

OMP is an all-encompassing information management and distribution protocol that enables the overlay network by separating services from transport. Services provided in a typical VRF setting are usually located within a VRF domain, and they are protected so that they are not visible outside the VRF. In such a traditional architecture, it is a challenge to extend VRF domains and service connectivity.

OMP addresses these scalability challenges by providing an efficient way to manage service traffic based on the location of logical transport end points. This method extends the data plane and control plane separation concept from within routers to across the network. OMP distributes control plane information along with related policies. A central Cisco vSmart Controller makes all decisions related to routing and access policies for the overlay routing domain. OMP is then used to propagate routing, security, services, and policies that are used by edge devices for data plane connectivity and transport.

OMP Route Advertisements

On Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs. These routes are called OMP routes or vRoutes to distinguish them from standard IP routes. The routes advertised are actually a tuple consisting of the route and the TLOC associated with that route. It is through OMP routes that the Cisco vSmart Controllers learn the topology of the overlay network and the services available in the network.

OMP interacts with traditional routing at local sites in the overlay network. It imports information from traditional routing protocols, such as OSPF and BGP, and this routing information provides reachability within the local site. The importing of routing information from traditional routing protocols is subject to user-defined policies.

Because OMP operates in an overlay networking environment, the notion of routing peers is different from a traditional network environment. From a logical point of view, the overlay environment consists of a centralized controller and a number of edge devices. Each edge device advertises its imported routes to the centralized controller and based on policy decisions, this controller distributes the overlay routing information to other edge devices in the network. Edge devices never advertise routing information to each other, either using OMP or any other method. The OMP peering sessions between the centralized controller and the edge devices are used exclusively to exchange control plane traffic; they are never, in any situation, used for data traffic.

Registered edge devices automatically collect routes from directly connected networks as well as static routes and routes learned from IGP protocols. The edge devices can also be configured to collect routes learned from BGP.

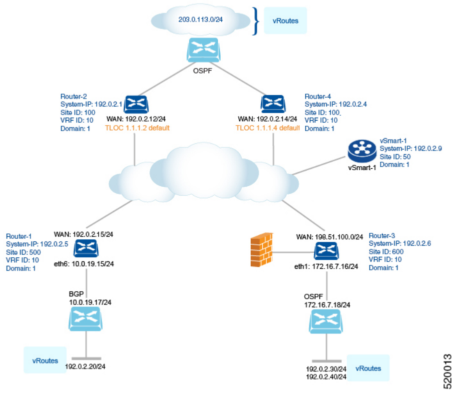
Route map AS path and community configuration, for example, AS path prepend, are not supported when route-maps are configured for protocol redistribution. The AS path for redistributed OMP routes can be configured and applied by using a route map on the BGP neighbor outbound policy.

OMP performs path selection, loop avoidance, and policy implementation on each local device to decide which routes are installed in the local routing table of any edge device.

OMP advertises the following types of routes:

- OMP routes (also called vRoutes)—Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.
- Transport locations (TLOCs)—Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.

The following figure illustrates the two types of OMP routes.



OMP Routes

Each device at a branch or local site advertises OMP routes to the Cisco vSmart Controllers in its domain. These routes contain routing information that the device has learned from its site-local network.

A Cisco SD-WAN device can advertise one of the following types of site-local routes:

- Connected (also known as direct)
- Static
- BGP
- EIGRP
- LISP
- OSPF (inter-area, intra-area, and external)

OMP routes advertise the following attributes:

- TLOC—Transport location identifier of the next hop for the vRoute. It is similar to the BGP NEXT_HOP attribute. A TLOC consists of three components:
  - System IP address of the OMP speaker that originates the OMP route
  - Color to identify the link type
  - Encapsulation type on the transport tunnel
- Origin—Source of the route, such as BGP, OSPF, connected, and static, and the metric associated with the original route.
- Originator—OMP identifier of the originator of the route, which is the IP address from which the route was learned.
- Preference—Degree of preference for an OMP route. A higher preference value is more preferred.
- Site ID—Identifier of a site within the Cisco SD-WAN overlay network domain to which the OMP route belongs.

- Tag—Optional, transitive path attribute that an OMP speaker can use to control the routing information it accepts, prefers, or redistributes.
- VRF—VRF or network segment to which the OMP route belongs.

You configure some of the OMP route attribute values, including the system IP, color, encapsulation type, carrier, preference, service, site ID, and VRF. You can modify some of the OMP route attributes by provisioning control policy on the Cisco vSmart Controller.

TLOC Routes

TLOC routes identify transport locations. These are locations in the overlay network that connect to physical transport, such as the point at which a WAN interface connects to a carrier. A TLOC is denoted by a 3-tuple that consists of the system IP address of the OMP speaker, a color, and an encapsulation type. OMP advertises each TLOC separately.

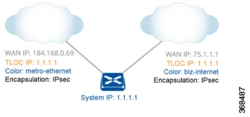
TLOC routes advertise the following attributes:

- TLOC private address—Private IP address of the interface associated with the TLOC.
- TLOC public address—NAT-translated address of the TLOC.
- Carrier—An identifier of the carrier type, which is generally used to indicate whether the transport is public or private.
- Color—Identifies the link type.
- Encapsulation type—Tunnel encapsulation type.
- Preference—Degree of preference that is used to differentiate between TLOCs that advertise the same OMP route.
- Site ID—Identifier of a site within the Cisco SD-WAN overlay network domain to which the TLOC belongs.
- Tag—Optional, transitive path attribute that an OMP speaker can use to control the flow of routing information toward a TLOC. When an OMP route is advertised along with its TLOC, both or either can be distributed with a community TAG, to be used to decide how send traffic to or receive traffic from a group of TLOCs.
- Weight—Value that is used to discriminate among multiple entry points if an OMP route is reachable through two or more TLOCs.

The IP address used in the TLOC is the fixed system address of the device itself. The reason for not using an IP address or an interface IP address to denote a TLOC is that IP addresses can move or change; for example, they can be assigned by DHCP, or interface cards can be swapped. Using the system IP address to identify a TLOC ensures that a transport end point can always be identified regardless of IP addressing.

The link color represents the type of WAN interfaces on a device. The Cisco SD-WAN solution offers predefined colors, which are assigned in the configuration of the devices. The color can be one of default, 3g, biz-internet, blue, bronze, custom1, custom2, custom3, gold, green, lte, metro-ethernet, mpls, private1, private2, public-internet, red, and silver.

The encapsulation is that used on the tunnel interface. It can be either IPsec or GRE.



The diagram to the right shows a device that has two WAN connections and hence two TLOCs. The system IP address of the router is 1.1.1.1. The TLOC on the left is uniquely identified by the system IP address 1.1.1.1, the color metro-ethernet, and the encapsulation IPsec, and it maps to the physical WAN interface with the IP address 184.168.0.69. The TLOC on the right is uniquely identified by the system IP address 1.1.1.1, the color biz-internet, and the encapsulation IPsec, and it maps to the WAN IP address 75.1.1.1.

You configure some of the TLOC attributes, including the system IP address, color, and encapsulation, and you can modify some of them by provisioning control policy on the Cisco vSmart Controller. See *Centralized Control Policy*.

OMP Route Redistribution

OMP automatically redistributes the following types of routes that it learns either locally or from its routing peers:

- Connected
- Static
- OSPF intra-area routes
- OSPF inter-area routes

To avoid routing loops and less than optimal routing, redistribution of following types of routes requires explicit configuration:

- BGP
- OSPF external routes

To avoid propagating excessive routing information from the edge to the access portion of the network, the routes that devices receive via OMP are not automatically redistributed into the other routing protocols running on the routers. If you want to redistribute the routes received via OMP, you must enable this redistribution locally on each device.

OMP sets the origin and sub-origin type in each OMP route to indicate the route's origin (see the table below). When selecting routes, the Cisco vSmart Controllerand the router take the origin type and subtype into consideration.

Table 12:

OMP Route Origin Type	**OMP Route Origin Subtype**
BGP	External Internal
Connected	—
OSPF	External-1 External-2 Intra-area Inter-area and NSSA-External-1, NSSA-External-2
Static	—

OMP Route Origin Type	OMP Route Origin Subtype
EIGRP	• EIGRP Summary • EIGRP Internal • EIGRP External
LISP	—

OMP also carries the metric of the original route. A metric of 0 indicates a connected route.

Administrative Distance

Administrative distance is the measure used to select the best path when there are two or more different routes to the same destination from multiple routing protocols. When the Cisco vSmart Controller or the router is selecting the OMP route to a destination, it prefers the one with the lower or lowest administrative distance value.

The following table lists the default administrative distances used by the Cisco SD-WAN devices:

Table 13:

Protocol	Administrative Distance
Connected	0
Static	1
NAT (NAT and static routes cannot coexist in the same VPN; NAT overwrites static routes)	1
Learned from DHCP	1
GRE	5
EBGP	20
OSPF	110
IBGP	200
OMP	250
EIGRP	Internal: 90, External: 170

OMP Best-Path Algorithm and Loop Avoidance

Cisco SD-WAN devices advertise their local routes to the Cisco vSmart Controller using OMP. Depending on the network topology, some routes might be advertised from multiple devices. Cisco SD-WAN devices use the following algorithm to choose the best route:

1. Select an ACTIVE route. An ACTIVE route is preferred over a STALE route. An active route is a route from a peer with which an OMP session is UP. A stale route is a route from a peer with which an OMP session is in Graceful Restart mode.
2. Check whether the OMP route is valid. If not, ignore it.
3. If the OMP route is valid and if it has been learned from the same Cisco SD-WAN device, select the OMP route with the lower administrative distance.
4. If the administrative distances are equal, select the OMP route with the higher OMP route preference value.
5. If the TLOC preference values are equal, compare the origin type, and select one in the following order (select the first match): Connected Static EBGP OSFP intra-area OSPF inter-area OSPF external EIGRP internal EIGRP external IBGP Unknown
6. If the origin type is the same, select the OMP route that has the lower origin metric.
7. If the router IDs are equal, a Cisco IOS XE SD-WAN device selects the OMP route with the lower private IP address. If a Cisco vSmart Controller receives the same prefix from two different sites and if all attributes are equal, it chooses both of them.

Here are some examples of choosing the best route:

- A Cisco vSmart Controller receives an OMP route to 10.10.10.0/24 via OMP from a Cisco vEdge device Cisco IOS XE SD-WAN device with an origin code of OSPF, and it also receives the same route from another Cisco vSmart Controller, also with an origin code of OSPF. If all other things are equal, the best-path algorithm chooses the route that came from the Cisco IOS XE SD-WAN device.
- A Cisco vSmart Controller learns the same OMP route, 10.10.10.0/24, from two Cisco IOS XE SD-WAN devicesin the same site. If all other parameters are the same, both routes are chosen and advertised to other OMP peers. By default, up to four equal-cost routes are selected and advertised.

A Cisco IOS XE SD-WAN device installs an OMP route in its forwarding table (FIB) only if the TLOC to which it points is active. For a TLOC to be active, an active BFD session must be associated with that TLOC. BFD sessions are established by each device which creates a separate BFD session with each of the remote TLOCs. If a BFD session becomes inactive, the Cisco vSmart Controller removes from the forwarding table all the OMP routes that point to that TLOC.

OMP Graceful Restart

Graceful restart for OMP allows the data plane in the Cisco SD-WAN overlay network to continue functioning if the control plane stops functioning or becomes unavailable. With graceful restart, if the vSmart controller in the network goes down, or if multiple vSmart controllers go down simultaneously, Cisco IOS XE SD-WAN devices and Cisco vEdge devices can continue forwarding data traffic. They do this using the last known good information that they received from the vSmart controller. When a vSmart controller is again available, its DTLS connection to the device is re-established, and the device then receives updated, current network information from the vSmart controller.

When OMP graceful restart is enabled, Cisco IOS XE SD-WAN devices and Cisco vEdge devicesand a vSmart controller (that is, two OMP peers) cache the OMP information that they learn from their peer. This information includes OMP routes, TLOC routes, service routes, IPsec SA parameters, and centralized data policies. When one of the OMP peers is no longer available, the other peer uses the cached information to continue operating in the network. So, for example, when a device no longer detects the presence of the OMP connection to a vSmart controller, the device continues forwarding data traffic using the cached OMP information. The device also periodically checks whether the vSmart controller has again become available. When it does come back up and the device re-establishes a connection to it, the device flushes its local cache and considers only the new OMP information from the vSmart controller to be valid and reliable. This same scenario occurs when a vSmart controller no longer detects the presence of Cisco IOS XE SD-WAN devices and Cisco vEdge devices.

BGP and OSPF Routing Protocols

The Cisco SD-WAN overlay network supports BGP and OSPF unicast routing protocols. These protocols can be configured on Cisco IOS XE SD-WAN devices in any VRF except for transport and management VRFs to provide reachability to networks at their local sites. Cisco IOS XE SD-WAN device can redistribute route information learned from BGP and OSPF into OMP so that OMP can better choose paths within the overlay network.

When the local site connects to a Layer 3 VPN MPLS WAN cloud, the devices act as an MPLS CE device and establishes a BGP peering session to connect to the PE router in the L3VPN MPLS cloud.

When the devices at a local site do not connect directly to the WAN cloud but are one or more hops from the WAN and connect indirectly through a non-Cisco SD-WAN device, standard routing must be enabled on the devices’ DTLS connections so that they can reach the WAN cloud. Either OSPF or BGP can be the routing protocol.

In both these types of topologies, the BGP or OSPF sessions run over a DTLS connection created on the loopback interface in VRF 0, which is the transport VRF that is responsible for carrying control traffic in the overlay network. The Cisco vBond Orchestrator learns about this DTLS connection via the loopback interface and conveys this information to the Cisco vSmart Controller so that it can track the TLOC-related information. In VRF 0, you also configure the physical interface that connects the Cisco IOS XE SD-WAN device to its neighbor—either the PE router in the MPLS case or the hub or next-hop router in the local site—but you do not establish a DTLS tunnel connection on that physical interface.

BGP Community Propagation

Table 14: Feature History

Feature Name	Release Information	Description
BGP Community Propagation	Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables propagation of BGP communities between routing protocols during route redistribution. One one node, the OMP redistributes routes from BGP and on the other node, the OMP redistributes node into BGP. The BGP AS Path is propagated over OMP so that it can be preserved between Cisco SD-WAN nodes. The BGP community propagation helps in propagating BGP communities between Cisco SD-WAN sites, across VPNs using OMP redistribution.

Starting from Cisco IOS XE Release 17.3.1a, the community propagation feature is supported. Without this option, no BGP communities are sent to the BGP neighbor, even if they are attached. With this feature, the Cisco IOS XE SD-WAN device can start propagating the communities attached to the BGP entries to the neighbor. The BGP overlay is migrated to a Cisco-SDWAN overlay where BGP route attributes are propagated between Cisco SD-WAN sites across VPNs.

EIGRP

Cisco EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol. It is an open-standard Interior Gateway Protocol (IGP). EIGRP is an enhancement to the original Interior Gateway Routing Protocol (IGRP developed) by Cisco. EIGRP does not fully update if there are no changes in the network. This reduces the flooding activities in other IGPs. It also can use both equal cost and unequal cost paths, which is unique among IGPs.

EIGRP is supported only on Cisco IOS XE SD-WAN devices.

See Introduction to EIGRP for more information in EIGRP.

Note If your EIGRP network includes Cisco vEdge devices, you may need additional software. Refer to Cisco IOS XE SD-WAN Release 16.11.x and Cisco SD-WAN Release 19.1.x release notes for configuration information.

Benefits of EIGRP

- Increased network width from 15 to 100 hops
- Fast convergence
- Incremental updates, minimizing bandwidth
- Protocol-independent neighbor discovery
- Easy scaling

Limitations and Restrictions

- EIGRP is not supported on the transport side network on Cisco IOS XE SD-WAN devices.
- EIGRP route match is not supported in vSmart centralized control policy.

Configure Unicast Overlay Routing

This topic describes how to provision unicast overlay routing.

Transport-Side Routing

To enable communication between Cisco SD-WAN devices, you configure OSPF or BGP on a loopback interface in VPN 0. The loopback interface is a virtual transport interface that is the terminus of the DTLS and IPsec tunnel connections required for Cisco IOS XE SD-WAN devices and Cisco vEdge devices to participate in the overlay network.

To configure transport-side BGP using vManage, see the *Configure BGP using vManage* . To configure transport-side BGP using CLI, see the *Configure BGP Using CLI* topic.

Configure BGP Using vManage Templates

The Border Gateway Protocl (BGP) can be used for service-side routing to provide reachability to networks at the local site, and it can be used for transport-side routing to enable communication between Cisco SD-WAN devices when a device is not directly connected to the WAN cloud. Create separate BGP templates for the two BGP routing types.

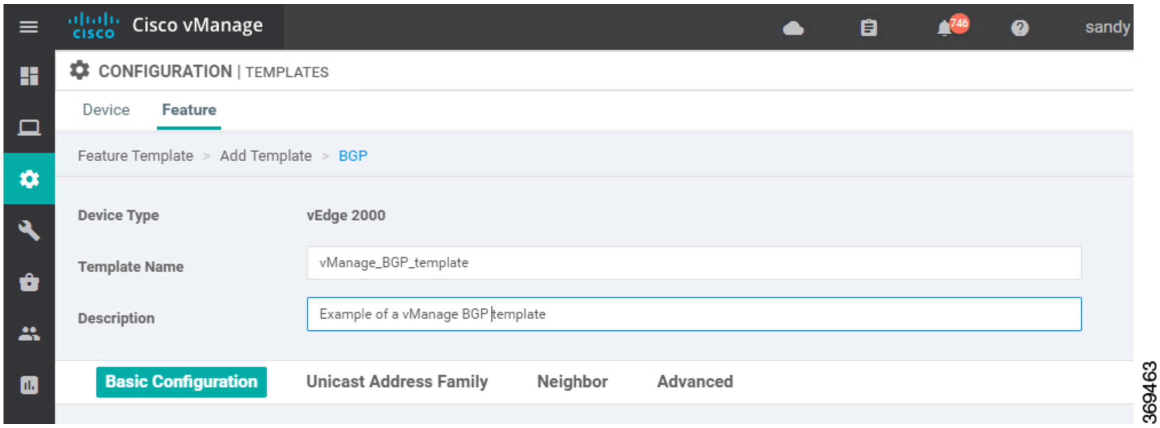
Note Cisco IOS XE SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE SD-WAN devices through Cisco vManage. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

To configure the BGP routing protocol using Cisco vManage templates:

1. Create a BGP feature template to configure BGP parameters.
2. Create a VPN feature template to configure VPN parameters for either service-side BGP routing (in any VPN other than VPN 0 or VPN 512) or transport-side BGP routing (in VPN 0).

Create a BGP Template

1. In vManage, go to **Configuration** > **Templates**.
2. In the Device tab, click **Create Template**.
3. From the Create Template drop-down, select **From Feature Template**.
4. From the Device Model drop-down, 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 the **Transport & Management VPN** tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   b. Under **Additional VPN 0 Templates**, located to the right of the screen, click **BGP**.
   c. From the BGP drop-down, click **Create Template**. The BGP template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP parameters.
6. To create a template for VPNs **1** through **511**, and **513** through **65530**:
   a. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the Service VPN section.
   b. Click the **Service VPN** drop-down.
   c. Under **Additional VPN Templates**, located to the right of the screen, click **BGP**.
   d. From the BGP drop-down, click **Create Template**. The BGP template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP parameters.



Device Type: vEdge 2000

Template Name: vManage_BGP_template

Description: Example of a vManage BGP template

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

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

Configure Basic BGP Parameters

To configure Border Gateway Protocol (BGP), select the **Basic Configuration** tab and configure the following parameters. Parameters marked with an asterisk are required to configure BGP.

Parameter Name	Description
Shutdown*	Click **No** to enable BGP on the interface.
AS number*	Enter the local AS number.
Router ID	Enter the BGP router ID in decimal four-part dotted notation.
Propagate AS Path	Click **On** to carry BGP AS path information into OMP.
Internal Routes Distance	Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another. Range: 0 through 255 Default: 0
Local Routes Distance	Specify the BGP route administrative distance for routes within the local AS. By default, a route received locally from BGP is preferred over a route received from OMP. Range: 0 through 255 Default: 0
External Routes Distance	Specify the BGP route administrative distance for routes learned from other sites in the overlay network. Range: 0 through 255 Default: 0

For service-side BGP, you might want to configure Overlay Management Protocol (OMP) to advertise to the Cisco vSmart Controller any BGP routes that the device learns. By default, Cisco SD-WAN devices advertise to OMP both the connected routes on the device and the static routes that are configured on the device, but it does not advertise BGP external routes learned by the device. You configure this route advertisement in the OMP template for devices or Cisco SD-WAN software.

For transport-side BGP, you must also configure a physical interface and a loopback interface in VPN 0. In addition, you should create a policy for BGP to advertise the loopback interface address to its neighbors, and apply the policy in the BGP instance or to a specific neighbor.

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

Configure Unicast Address Family

To configure global BGP address family information, select the **IPv4 Unicast Address Family** tab and configure the following parameters:

Tab/Parameter	Option	Sub-Option	Description
IPv4 / IPv6	Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.		
Maximum Paths	Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing. Range: 0 to 32		
Mark as Optional Row	Check **Mark as Optional Row** 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.		

Tab/Parameter	Option	Sub-Option	Description
Redistribute	Click **Redistribute** > **New Redistribute**.		
	Mark as Optional Row	Check **Mark as Optional Row** 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.	
	Protocol	Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are:	
		static	Redistribute static routes into BGP.
		connected	Redistribute connected routes into BGP.
		ospf	Redistribute Open Shortest Path First routes into BGP.
		omp	Redistribute Overlay Management Protocol routes into BGP.
		nat	Redistribute Network Address Translation routes into BGP.
		natpool-outside	Redistribute outside NAT routes into BGP.
		At a minimum, select the following: • For service-side BGP routing, select **OMP**. By default, OMP routes are not redistributed into BGP. • For transport-side BGP routing, select **Connected**, and then under **Route Policy**, specify a route policy that has BGP advertise the loopback interface address to its neighbors.	
	Route Policy	Enter the name of the route policy to apply to redistributed routes.	
	Click **Add** to save the redistribution information.		
Network	Click **Network** > **New Network**.		
	Mark as Optional Row	Check **Mark as Optional Row** 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.	
	Network Prefix	Enter a network prefix, in the format *prefix/length* to be advertised by BGP.	
	Click **Add** to save the network prefix.		

Tab/Parameter	Option	Sub-Option	Description
Aggregate Address	Click **Aggregate Address** > **New Aggregate Address**.		
	Mark as Optional Row	Check **Mark as Optional Row** to mark this configuration as device-specific. To include this configuration for a device, enter the variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.	
	Aggregate Prefix **IPv6 Aggregate Prefix**	Enter the prefix of the addresses to aggregate for all BGP sessions in the format *prefix/length*.	
	AS Set Path	Click **On** to generate the set path information for aggregated prefixes.	
	Summary Only	Click **On** to filter out specific routes from the BGP updates.	
	Click **Add** to save the aggregate address.		

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

Configure BGP Neighbors

To configure a neighbor, click **Neighbor** > **New Neighbor**, and configure the following parameters:

Note For BGP to function, you must configure at least one neighbor.

Parameter Name	Options	Sub-Options	Description
IPv4 / IPv6	Click **IPv4** to configure IPv4 neighbors. Click **IPv6** to configure IPv6 neighbors.		
Address/IPv6 Address	Specify the IP address of the BGP neighbor.		
Description	Enter a description of the BGP neighbor.		
Remote AS	Enter the AS number of the remote BGP peer.		

Parameter Name	Options	Sub-Options	Description
Address Family	Click **On** and select the address family. Enter the address family information. The software supports only the BGP IPv4 unicast address family.		
	Address Family	Select the address family. The software supports only the BGP IPv4 unicast address family.	
	Maximum Number of Prefixes	Specify the maximum number of prefixes that can be received from the neighbor. Range: 1 through 4294967295 Default: 0	
		Threshold	Specify the threshold at which to generate a warning message or restart the BGP connection. The threshold is a percentage of the maximum number of prefixes. You can specify either a restart interval or a warning only.
		Restart Interval	Specify the duration to wait for restarting the BGP connection.*Range:* 1 through 65535 minutes
		Warning Only	Click **On** to display a warning message without restarting the BGP connection.
		Route Policy In	Click **On** and specify the name of a route policy that will have the prefixes from the neighbour.
		Route Policy Out	Click **On** and specify the name of a route policy that will have the prefixes sent to the neighbour.
Shutdown	Click **On** to enable the connection to the BGP neighbor.		

Configure MPLS Interface

Table 15: Feature History

Feature Name	Release Information	Description
MPLS-BGP Support on the Service Side	Cisco IOS XE Release 17.2.1r	This features allows you to enable support on Multiprotocol Label Switching (MPLS). Multiple Service VPNs use inter autonomous system (AS) BGP labelled path to forward the traffic, which in turn helps scaling the service side VPNs with less control plane signaling. Label distribution for a given VPN routing and forwarding (VRF) instance on a given device can be handled by Border Gateway Protocol (BGP).

Cisco IOS XE SD-WAN devices support Multiprotocol Label Switching (MPLS) to enable multiple protocol environment. MPLS offers extremely scalable, protocol agnostic, data-carrying mechanism that transfers data packets with assigned labels across the network through virtual links. Extensions of the BGP protocol can be used to manage an MPLS path. The Cisco IOS XE SD-WAN devices also have the capability of BGP MPLS VPN Option B.

The multiple service VPNs use inter autonomous system (AS) BGP labelled path to forward the traffic, that in turn helps scale the service side VPNs with less control plane signaling. MPLS interface is supported only in global VRF.

To configure MPLS interface,

- Click **MPLS Interface**.
- Enter the interface name in the **Interface Name** field.
- You can click on **+** to add more interfaces and save the configuration.

Configure Label Range

The Cisco vManage automatically programs the label space for BGP MPLS. The labels are allocated per VPN. To view the configuration, use the command, **show sdwan running-config**.

Sample configuration:

```
Device# show sdwan running-config
Device# mpls label range 100000 1048575 static 16 999
Device# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
Device# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf
```

Configure Route Targets

You can configure route targets on the Cisco IOS XE SD-WAN devices. Route targets configuration is supported only on eBGP and IPv4 peer devices. All the supported protocols can be redistributed to BGP.

To configure route targets, click **Route Targets** tab and configure the following parameters:

Tab/Parameter	Option	Sub-Option	Description
IPv4 / IPv6	Click **IPv4** to configure route target for IPv4 interfaces. Click **IPv6** to configure route target for IPv6 interfaces.		
Add VPN	Click **Add VPN** to add VPNs.		
VPN ID for IPv4	Specify the VPN ID for IPv4 interface.		
Import	Imports routing information from the target VPN extended community.		
Export	Exports routing information to the target VPN extended community.		

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

Initially, the devices have default route targets, then you can add additional entries as required.

Configure Advanced Neighbor Parameter

To configure advanced parameters for the neighbor, click **Neighbor** > **Advanced Options**.

Parameter Name	Description
Next-Hop Self	Click **On** to configure the router to be the next hop for routes advertised to the BGP neighbor.
Send Community	Click **On** to send the local router's BGP community attribute to the BGP neighbor.
Send Extended Community	Click **On** to send the local router's BGP extended community attribute to the BGP neighbor.
Negotiate Capability	Click **On** to allow the BGP session to learn about the BGP extensions that are supported by the neighbor.
Source Interface Address	Enter the IP address of a specific interface of the neighbor that BGP is to use for the TCP connection to the neighbor.
Source Interface Name	Enter the name of a specific interface of the neighbor that BGP is to use for the TCP connection to the neighbor, in the format **ge** *port*/*slot*.
EBGP Multihop	Set the time to live (TTL) for BGP connections to external peers. Range: 0 to 255 Default: 1
Password	Enter a password to use to generate an MD5 message digest. Configuring the password enables MD5 authentication on the TCP connection with the BGP peer. The password is case-sensitive and can be up to 25 characters long. It can contain any alphanumeric characters, including spaces. The first character cannot be a number.
Keepalive Time	Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered available. Specify the keepalive time for the neighbor to override the global keepalive time. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)
Hold Time	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. Specify the hold time for the neighbor to override the global hold time. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive timer)
Connection Retry Time	Specify the number of seconds between retries to establish a connection to a configured BGP neighbor peer that has gone down. Range: 0 through 65535 seconds Default: 30 seconds

Parameter Name	Description
Advertisement Interval	For the BGP neighbor, set the minimum route advertisement interval (MRAI) between when BGP routing update packets are sent to that neighbor. Range: 0 through 600 seconds Default: 5 seconds for IBGP route advertisements; 30 seconds for EBGP route advertisements

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

Change the Scope of 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 to the left of the parameter field 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. 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.

Configure Advanced BGP Parameters

To configure advanced parameters for BGP, click the **Advanced** tab and configure the following parameters:

Parameter Name	Description
Hold Time	Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local device then terminates the BGP session to that peer. This hold time is the global hold time. Range: 0 through 65535 seconds Default: 180 seconds (three times the keepalive timer)

Parameter Name	Description
Keepalive	Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local device is still active and should be considered available. This keepalive time is the global keepalive time. Range: 0 through 65535 seconds Default: 60 seconds (one-third the hold-time value)
Compare MED	Click **On** to compare the device IDs among BGP paths to determine the active path.
Deterministic MED	Click **On** to compare multiple exit discriminators (MEDs) from all routes received from the same AS, regardless of when the route was received.
Missing MED as Worst	Click **On** to consider a path as the worst path if the path is missing a MED attribute.
Compare Router ID	Click **On** to always compare MEDs regardless of whether the peer ASs of the compared routes are the same.
Multipath Relax	Click **On** to have the BGP best-path process select from routes in different in ASs. By default, when you are using BGP multipath, the BGP best path process selects from routes in the same AS to load-balance across multiple paths.

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

Configure BGP Using CLI

This is an example of a BGP configuration on a Cisco IOS XE SD-WAN device.

```
router bgp 100
 bgp log-neighbor-changes
 distance bgp 20 200 20
 !
 address-family ipv4 vrf 100
  bgp router-id 10.0.0.0
  redistribute omp
  neighbor 10.0.0.1 remote-as 200
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community both
  neighbor 10.0.0.1 route-map OMP_BGP-POLICY in
  neighbor 10.0.0.1 maximum-prefix 2147483647 100


route-map OMP_BGP-POLICY permit 1
 match ip address prefix-list OMP-BGP-TEST-PREFIX-LIST
 set omp-tag 10000
route-map OMP_BGP-POLICY permit 65535


ip prefix-list OMP-BGP-TEST-PREFIX-LIST seq 5 permit 10.0.0.0/8
```

Verify BGP Redistribute Route in OMP

```
Device#show sdwan omp routes 10.0.0.0/8
---------------------------------------------------
omp route entries for vpn 100 route 10.0.0.0/8
---------------------------------------------------
```

```
               RECEIVED FROM:
peer            172.16.0.0
path-id         470777
label           1002
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       10.0.0.1
     type             installed
     tloc             172.16.0.1, mpls, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          1
     preference       not set
     tag              10000   <=====
     origin-proto     eBGP
     as-path          not set
     unknown-attr-len not set
```

The following example shows the propagation of BGP community on Cisco IOS XE SD-WAN devices:

```
vm5#show sdwan omp routes 192.168.0.0/16 detail
---------------------------------------------------
omp route entries for vpn 1 route
192.168.0.0/16---------------------------------------------------
            RECEIVED FROM:
peer         10.0.0.0
path-id         70
label           1007
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       192.168.0.0
     type             installed
     tloc             192.168.0.1, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          500
     preference       not set
     tag              not set
     origin-proto     iBGP
     origin-metric    0
     as-path          not set
     community        100:1 100:2 100:3
     unknown-attr-len not set
            ADVERTISED TO:
peer    192.168.0.1
```

This topic describes how to configure BGP for service-side and transport-side for unicast overlay routing

Configure Service-Side Routing

To set up routing on the Cisco vEdge device, you provision one VPN or multiple VPNs if segmentation is required. Within each VPN, you configure the interfaces that participate in that VPN and the routing protocols that operate in that VPN.

1. Configure a VPN.

```
vEdge(config)# vpn vpn-id
```

vpn-id can be any service-side VPN, which is a VPN other than VPN 0 and VPN 512. VPN 0 is the transport VPN and carries only control traffic, and VPN 512 is the management VPN.

2. Configure BGP to run in the VPN:
   1. Configure the local AS number:

      ```
      vEdge(config-vpn)# router bgp local-as-number
      ```

      You can specify the AS number in 2-byte ASDOT notation (1 through 65535) or in 4-byte ASDOT notation (1.0 through 65535.65535).

   2. Configure the BGP peer, specifying its address and AS number (the remote AS number), and enable the connection to the peer:

      ```
      vEdge(config-bgp)# neighbor address remote-as remote-as-number
      vEdge(config-bgp)# no shutdown
      ```

3. Configure a system IP address for the Cisco vEdge device:

   ```
   vEdge(config)# system system-ipaddress
   ```

Example of BGP Configuration on a SD-WAN IOS XE Router

```
Device# show running-config system
system
  system-ip 10.1.2.3
!
Device# show running-config vpn 1
router bgp 2
bgp log-neighbor-changes
timers bgp 1 111
neighbor 10.20.25.16 remote-as 1

!
address-family ipv4 unicast
neighbor 10.20.25.16 activate
exit-address-family
!
address-family vpnv4 unicast
neighbor 10.20.25.16 activate
neighbor 10.20.25.16 send-community extended
exit-address-family
!
address-family vpnv6 unicast
neighbor 10.20.25.16 activate
neighbor 10.20.25.16 send-community extended
exit-address-family
!
address-family ipv4 unicast vrf 1
redistribute connected
redistribute static
exit-address-family
!
address-family ipv6 unicast vrf 1
redistribute connected
redistribute omp

exit-address-family
!
address-family ipv4 unicast vrf 2
```

```
redistribute connected

exit-address-family
```

Example of configuring route targets:

```
vrf config

vrf definition 1
rd 1:1

!
address-family ipv4

route-target export 200:1

route-target import 100:1

exit-address-family
!
address-family ipv6
route-target export 101:1
route-target import 201:1
exit-address-family
```

Redistribute BGP Routes and AS Path Information

By default, routes from other routing protocols are not redistributed into BGP. It can be useful for BGP to learn OMP routes, because OMP learns routes to destinations throughout the overlay network. BGP on the Cisco SD-WAN devices, then advertises the OMP routes to all the BGP routers in the service-side of the network.

```
config-transaction
 router bgp 2
  address-family ipv4 unicast
   redistribute omp route-map route_map
```

To redistribute OMP routes into BGP so that these routes are advertised to all BGP routers in the service side of the network, configure redistribution in any VRF except transport VRF or Mgmt VRF:

For Cisco IOS XE SD-WAN device, under router BGP configuration, **redistribute omp route-map** set/match is used instead of **redistribute omp metric 0** setting as the **redistribute omp metric** is disabled in all the branches.

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 vrf 100
Device(config-router-af)# redistribute omp [route-map policy-name]
```

```
config-transaction
 router bgp 100
  address-family ipv4 vrf 100
   redistribute omp route_map route_map
```

You can also redistribute routes learned from other protocols such as OSPF, rip into BGP, and apply policy as shown in the example above:

You can control redistribution of routes on a per-neighbor basis:

```
config-transaction
 router bgp 100
```

```
  address-family ipv4
   neighbor 10.0.100.1 route-map route_map (in | out)
```

You can configure the Cisco IOS XE SD-WAN device to advertise BGP routes that it has learned, through OMP, from the Cisco vSmart Controller. Doing so allows the Cisco vSmart Controller to advertise these routes to other Cisco IOS XE SD-WAN devices in the overlay network. You can advertise BGP routes either globally or for a specific VRF:

```
config-transaction
 sdwan
  omp
   address-family ipv4 vrf 100
    advertise bgp
    exit
```

Configure OSPF Using vManage Templates

Use the OSPF template for all Cisco SD-WAN devices.

Note Cisco XE SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE SD-WAN devices through Cisco vManage. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

To configure OSPF on a device using Cisco vManage templates:

1. Create an OSPF feature template to configure OSPF parameters. OSPF can be used for transport-side routing to enable communication between the Cisco SD-WAN devices when the router is not directly connected to the WAN cloud.
2. Create a VPN feature template to configure VPN parameters for transport-side OSPF routing (in VPN 0). See the VPN help topic for more information.

Create an OSPF Template

1. In vManage NMS, select **Configuration** > **Templates**.
2. In the Device tab, click **Create Template**.
3. From the Create Template drop-down, select **From Feature Template**.
4. From the Device Model drop-down, select the type of device for which you are creating the template. To create a template for VPN 0 or VPN 512:
   a. Click the **Transport & Management VPN** tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   b. Under Additional VPN 0 Templates, located to the right of the screen, click **OSPF**.
   c. From the OSPF drop-down, click **Create Template**. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.

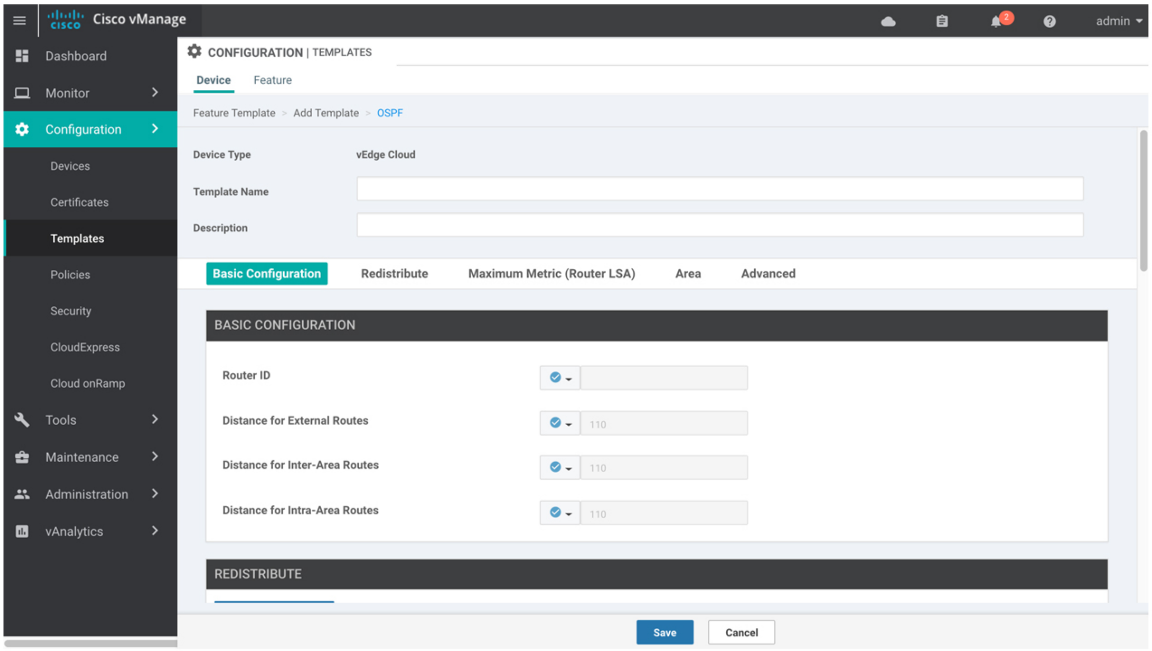
5. To create a template for VPNs 1 through 511, and 513 through 65530:

   a. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the Service VPN section.

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

   c. Under Additional VPN Templates, located to the right of the screen, click **OSPF**.

   d. From the OSPF drop-down, click **Create Template**. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.



Device Type vEdge Cloud

Template Name

Description

Router ID

Distance for External Routes 110

Distance for Inter-Area Routes 110

Distance for Intra-Area Routes 110

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

7. In the Template Description field, 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 16:

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 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 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 Basic OSPF

To configure basic OSPF, select the **Basic Configuration** tab and then configure the following parameters. All these parameters are optional. For OSPF to function, you must configure area 0, as described below.

Table 17:

Parameter Name	Description
Router ID	Enter the OSPF router ID in decimal four-part dotted notation. This is the IP address associated with the router for OSPF adjacencies.
Distance for External Routes	Specify the OSPF route administration distance for routes learned from other domains. *Range:* 0 through 255*Default:* 110
Distance for Inter-Area Routes	Specify the OSPF route administration distance for routes coming from one area into another. *Range:* 0 through 255*Default:* 110
Distance for intra-Area routes	Specify the OSPF route administration distance for routes within an area. *Range:* 0 through 255*Default:* 110

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

Redistribute Routes into OSPF

To redistribute routes learned from other protocols into OSPF on Cisco SD-WAN devices, select **Redistribute** > **Add New Redistribute** and configure the following parameters:

Table 18:

Parameter Name	Description
Protocol	Select the protocol from which to redistribute routes into OSPF. Select from BGP, Connected, NAT, OMP, and Static.
Route Policy	Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.

To add another OSPF route redistribution policy, click the plus sign (+).

To remove an OSPF route redistribution policy from the template configuration, click **the trash icon** to the right of the entry.

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

Configure OSPF To Advertise a Maximum Metric

To configure OSPF to advertise a maximum metric so that other devices do not prefer the Cisco IOS XE SD-WAN device as an intermediate hop in their Shortest Path First (SPF) calculation, select **Maximum Metric (Router LSA)** > **Add New Router LSA** and configure the following parameters:

Table 19:

Parameter Name	Description
Type	Select a type: • Administrative—Force the maximum metric to take effect immediately through operator intervention. • On-Startup—Advertise the maximum metric for the specified time.
Advertisement Time	If you selected On-Startup, specify the number of seconds to advertise the maximum metric after the router starts up. *Range:* 0, 5 through 86400 seconds*Default:* 0 seconds (the maximum metric is advertised immediately when the router starts up)

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

Configure OSPF Areas

To configure an OSPF area within a VPN on a Cisco SD-WAN device, select **Area** > **Add New Area**. For OSPF to function, you must configure area 0.

Table 20:

Parameter Name	Description
Area Number	Enter the number of the OSPF area. *Range:* 32-bit number
Set the Area Type	Select the type of OSPF area, Stub or NSSA.
No Summary	Select **On** to not inject OSPF summary routes into the area.
Translate	If you configured the area type as NSSA, select when to allow Cisco SD-WAN devices that are ABRs (area border routers) to translate Type 7 LSAs to Type 5 LSAs: • Always—Router always acts as the translator for Type 7 LSAs. That is no other router, even if it is an ABR, can be the translator. If two ABRs are configured to always be the translator, only one of them actually ends up doing the translation. • Candidate—Router offers translation services, but does not insist on being the translator. • Never—Translate no Type 7 LSAs.

To save the new area, click **Add**.

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

Configure Interfaces in an OSPF Area

To configure the properties of an interface in an OSPF area, select **Area** > **Add New Area** > **Add Interface**. In the Add Interface popup, configure the following parameters:

Table 21:

Parameter Name	Description
Interface Name	Enter the name of the interface, in the format **ge** *slot*/*port* or **loopback** *number*.
Hello Interval	Specify how often the router sends OSPF hello packets. *Range:* 1 through 65535 seconds*Default:* 10 seconds
Dead Interval	Specify how often the Cisco IOS XE SD-WAN device must receive an OSPF hello packet from its neighbor. If no packet is received, the Cisco IOS XE SD-WAN deviceassumes that the neighbor is down. *Range:* 1 through 65535 seconds*Default:* 40 seconds (4 times the default hello interval)
LSA Retransmission Interval	Specify how often the OSPF protocol retransmits LSAs to its neighbors. *Range:* 1 through 65535 seconds*Default:* 5 seconds

Parameter Name	Description
Interface Cost	Specify the cost of the OSPF interface. *Range:* 1 through 65535

To configure advanced options for an interface in an OSPF area, in the Add Interface popup, click **Advanced Options** and configure the following parameters:

Table 22:

Parameter Name	Description
Designated Router Priority	Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR.*Range:* 0 through 255*Default:* 1
OSPF Network Type	Select the OSPF network type to which the interface is to connect: • Broadcast network—WAN or similar network. • Point-to-point network—Interface connects to a single remote OSPF router. *Default:* Broadcast
Passive Interface	Select **On** or **Off** to specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol.*Default:* Off
Authentication	Specify the authentication and authentication key on the interface to allow OSPF to exchange routing update information securely.
• Authentication Type	Select the authentication type: • Simple authentication—Password is sent in clear text. • Message-digest authentication—MD5 algorithm generates the password.
• Authentication Key	Enter the authentication key. Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. The key can be 1 to 32 characters.
Message Digest	Specify the key ID and authentication key if you are using message digest (MD5).
• Message Digest Key ID	Enter the key ID for message digest (MD5 authentication). It can be 1 to 32 characters.
• Message Digest Key	Enter the MD5 authentication key in clear text or as an AES-encrypted key. It can be from 1 to 255 characters.

To save the interface configuration, click **Save**.

To save the new area, click **Add**.

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

Configure an Interface Range for Summary LSAs

To configure the properties of an interface in an OSPF area, select **Area** > **Add New Area** > **Add Range**. In the Area Range popup, click **Add Area Range**, and configure the following parameters:

Table 23:

Parameter Name	Description
Address	Enter the IP address and subnet mask, in the format *prefix/length* for the IP addresses to be consolidated and advertised.
Cost	Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination.*Range:* 0 through 16777215
No Advertise	Select **On** to not advertise the Type 3 summary LSAs or Off to advertise them.

To save the area range, click **Save**.

To save the new area, click **Add**.

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

Configure Other OSPF Properties

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

Table 24:

Parameter Name	Description
Reference Bandwidth	Specify the reference bandwidth for the OSPF auto-cost calculation for the interface. *Range:* 1 through 4294967 Mbps*Default:* 100 Mbps
RFC 1538 Compatible	By default, the OSPF calculation is done per RFC 1583. Select **Off** to calculate the cost of summary routes based on RFC 2328.
Originate	Click **On** to generate a default external route into an OSPF routing domain: • Always—Select On to always advertise the default route in an OSPF routing domain. • Default metric—Set the metric used to generate the default route.*Range:* 0 through 16777214*Default:* 10 • Metric type—Select to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.
SPF Calculation Delay	Specify the amount of time between when the first change to a topology is received until performing the SPF calculation. *Range*: 0 through 600000 milliseconds (60 seconds)*Default*: 200 milliseconds

Parameter Name	Description
Initial Hold Time	Specify the amount of time between consecutive SPF calculations. *Range*: 0 through 600000 milliseconds (60 seconds)*Default*: 1000 milliseconds
Maximum Hold Time	Specify the longest time between consecutive SPF calculations. *Range*: 0 through 600000*Default*: 10000 milliseconds (60 seconds)
Policy Name	Enter the name of a localized control policy to apply to routes coming from OSPF neighbors.

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

Configure OSPF Using CLI

This topic describes how to configure basic service-side OSPF for Unicast overlay routing.

Configure Basic Service-Side OSPF

To set up routing on the Cisco IOS XE SD-WAN device, you provision VRFs if segmentation is required. Within each VRF, you configure the interfaces that participate in that VRF and the routing protocols that operate in that VRF.

Here is an example of configuring service-side OSPF on a Cisco IOS XE SD-WAN device.

```
config-transaction
 router ospf 1 vrf1
  auto-cost reference-bandwidth 100
  max-metric router-lsa
  timers throttle spf 200 1000 10000
  router-id 172.16.255.15
  default-information originate
  distance ospf external 110
  distance ospf inter-area110
  distance ospf intra-area110
  distredistribute connected subnets route-map route_map
  exit
 interface GigabitEthernet0/0/1
  no shutdown
  arp timeout 1200
  vrf forwarding 1
  ip address 10.1.100.14 255.255.255.0
  ip redirects
  ip mtu 1500
  ip ospf 1 area 23
  ip ospf network broadcast
  mtu 1500
  negotiation auto
  exit
```

Configure OMP Using vManage Templates

Use the OMP template to configure OMP parameters for all Cisco IOS XE SD-WAN devices, and for Cisco vSmart Controllers.

OMP is enabled by default on all Cisco IOS XE SD-WAN devices, Cisco vManage NMSs, and Cisco vSmart Controllers, so there is no need to explicitly enable OMP. OMP must be operational for the Cisco SD-WAN overlay network to function. If you disable it, you disable the overlay network.

Note

- Route advertisements in OMP are done either by applying the configuration at the global level or at the specific VRF level. See the Configure OMP Advertisements section in this topic.
- Cisco XE SD-WAN devices use VRFs in place of VPNs. However, the following steps still apply to configure Cisco IOS XE SD-WAN devicesthrough Cisco vManage. When you complete the configuration, the system automatically maps the VPN configurations to VRF configurations.

Create OMP Template

1. In Cisco vManage, select **Configuration** > **Templates**.
2. In the Device tab, click **Create Template**.
3. From the Create Template drop-down, select **From Feature Template**.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for OMP, select the Factory_Default_OMP_Template and click **Create Template**. The OMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OMP parameters. You may need to click a tab or the plus sign (+) to display additional fields.
6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the Template Description field, 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 25:

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 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 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 Basic OMP Options

To configure basic OMP options, select the **Basic Configuration** tab and configure the following parameters. All parameters are optional.

Table 26:

Parameter Name	Description
Graceful Restart for OMP	Ensure that Yes is selected to enable graceful restart. By default, graceful restart for OMP is enabled.
Overlay AS Number (on vEdge routers only)	Specify a BGP AS number that OMOP advertises to the router's BGP neighbors.
Graceful Restart Timer	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart.*Range:* 0 through 604800 seconds (168 hours, or 7 days)*Default:* 43200 seconds (12 hours)
Number of Paths Advertised per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. Cisco vEdge devices advertise routes to Cisco vSmart Controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE SD-WAN device can have up to four TLOCs, and by default advertises each route-TLOC tuple to the Cisco vSmart Controller. If a local site has two sCisco IOS XE SD-WAN device, a Cisco vSmart Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised.*Range:* 1 through 16*Default:* 4

Parameter Name	Description
ECMP Limit (on vEdge routers only)	Specify the maximum number of OMP paths received from the Cisco vSmart Controller that can be installed in the Cisco IOS XE SD-WAN device'slocal route table. By default, a Cisco IOS XE SD-WAN device installs a maximum of four unique OMP paths into its route table.*Range:* 1 through 32*Default:* 4
Send Backup Paths (on vSmart Controllers only)	Click **On** to have OMP advertise backup routes to Cisco IOS XE SD-WAN devices. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.
Shutdown	Ensure that **No** is selected to enable to Cisco SD-WAN overlay network. Click **Yes** to disable OMP and disable the Cisco SD-WAN overlay network. OMP is enabled by default.
Discard rejected (on vSmart controllers only)	Click **Yes** to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes are not discarded.

To save the feature template, click Save.

Configure OMP Timers

To configure OMP timers, select the **Timers** tab and configure the following parameters:

Table 27:

Parameter Name	Description
Advertisement Interval	Specify the time between OMP Update packets. *Range:* 0 through 65535 seconds*Default:* 1 second
Hold Time	Specify how long to wait before closing the OMP connection to a peer. If the peer does not receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed.*Range:* 0 through 65535 seconds*Default:* 60 seconds
EOR Timer	Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table.*Range:* 1 through 3600 seconds (1 hour)*Default:* 300 seconds (5 minutes)

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

Configure OMP Advertisements

Note Route advertisements in OMP are done either by applying the configuration at the global level or at the specific VRF level.

To advertise routes learned locally by the Cisco IOS XE SD-WAN device to OMP, select the **Advertise** tab and configure the following parameters:

Table 28:

Parameter Name	Description
Advertise	Click **On** or **Off** to enable or disable the Cisco IOS XE SD-WAN device advertising to OMP the routes that it learns locally: • BGP—Click **On** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP. • Connected—Click **Off** to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP. • OSPF—Click **On** and click **On** again in the External field that appears to advertise external OSPF routes to OMP. OSPF inter-area and intra-area routes are always advertised to OMP. By default, external OSPF routes are not advertised to OMP. • Static—Click **Off** to disable advertising static routes to OMP. By default static routes are advertised to OMP. To configure per-VPN route advertisements to OMP, use the VPN feature template .

Click **Save**.

Configure OMP Using CLI

By default, OMP is enabled on all Cisco IOS XE SD-WAN devices and vSmart controllers. OMP must be operational for the Cisco SD-WAN overlay network to function. If you disable it, you disable the overlay network.

OMP support in Cisco SD-WAN includes the following:

- IPv6 service routes
- IPv4 and IPv6 protocols, which are both turned on by default
- OMP route advertisements to BGP, EIGRP, OSPF, connected routes, static routes, and so on

Configure OMP Graceful Restart

OMP graceful restart is enabled by default on vSmart controllers and Cisco SD-WAN devices. OMP graceful restart has a timer that tells the OMP peer how long to retain the cached advertised routes. When this timer expires, the cached routes are considered to be no longer valid, and the OMP peer flushes them from its route table.

The default timer is 43,200 seconds (12 hours), and the timer range is 1 through 604,800 seconds (7 days). To modify the default timer value:

```
Device# config-transaction
Device(config)# sdwan
Device(config-omp)# timers graceful-restart-timer seconds
```

To disable OMP graceful restart:

```
Device(config-omp)# no graceful-restart
```

The graceful restart timer is set up independently on each OMP peer; that is, it is set up separately on each Cisco IOS XE SD-WAN device and vSmart controller. To illustrate what this means, let's consider a vSmart controller that uses a graceful restart time of 300 seconds, or 5 minutes, and a Cisco IOS XE SD-WAN device that is configured with a timer of 600 seconds (10 minutes). Here, the vSmart controller retains the OMP routes learned from that device for 10 minutes—the graceful restart timer value that is configured on the device and that the device has sent to the vSmart controller during the setup of the OMP session. The Cisco IOS XE SD-WAN device retains the routes it learns from the vSmart controller for 5 minutes, which is the default graceful restart time value that is used on the vSmart controller and that the controller sent to the device, also during the setup of the OMP session.

While a vSmart controller is down and a Cisco IOS XE SD-WAN device is using cached OMP information, if you reboot the device, it loses its cached information and hence will not be able to forward data traffic until it is able to establish a control plane connection to the vSmart controller.

Advertise Routes to OMP

Table 29: Feature History

Feature Name	Release Information	Description
OMP Route Aggregation	Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1	This feature is an enhancement where OMP route aggregation is performed only for the routes that are configured for route redistribution to avoid black hole routing. This enhancement is applicable for OSPF, Connected, Static, BGP and other protocols only if the redestribution is requested.

By default, a Cisco IOS XE SD-WAN device advertises connected routes, static routes, OSPF inter-area, intra-area routes, BGP and EIGRP protocols to OMP for the Cisco vSmart controller, that is responsible for the device's domain.

To have the device advertise these routes to OMP, and hence to the Cisco vSmart controller responsible for the device's domain, use the **advertise** command.

Note Configuration of route advertisements in OMP can be done either by applying the configuration at the global level or at the specific VRF level.

To enable protocol route advertisements for OMP protocol for all VRFs, add the configuration at the global level.

```
Device(config)# sdwan
Device(config-sdwan)# omp
Device(config-omp)# address-family ipv4
Device(config-ipv4)# advertise bgp
```

To enable protocol route advertisements for a few VRFs, remove the global-level configuration using **no advertise bgp** command and add a per-VRF-level configuration:

```
Device(config)# sdwan
Device(config-sdwan)# omp
Device(config-omp)# address-family ipv4
Device(config-ipv4)# no advertise bgp
Device(config-ipv4)# address-family ipv4 vrf 2
Device(config-vrf-2)# advertise bgp
Device(config-vrf-2)# address-family ipv4 vrf 4
Device(config-vrf-4)# advertise bgp
Device(config-vrf-4)# commit
```

Note To disable certain protocol route advertisements for all or for a few VRFs, ensure that the configuration is present at neither the global level nor the VRF level.

To configure the routes that the device advertises to OMP for all VRFs configured on the device:

```
config-transaction
 sdwan
  omp
   address-family ipv4
    advertise ospf external
    advertise bgp
    advertise eigrp
    advertise connected
    advertise static
    exit
  address-family ipv6
   advertise ospf external
   advertise bgp
   advertise eigrp
   advertise connected
   advertise static
   exit
```

For OSPF, the route type can be **external**.

The **bgp**, **connected**, **ospf**, and **static** options advertise all learned or configured routes of that type to OMP. To advertise a specific route instead of advertising all routes for a protocol, use the **network** option, and specify the prefix of the route to advertise.

To configure the routes that the device advertises to OMP for a specific VRF on the device:

```
config-transaction
 sdwan
  omp
   address-family ipv4 vrf 1
    advertise aggregate prefix 10.0.0.0/8
    advertise ospf external
    advertise bgp
    advertise eigrp
    advertise connected
    advertise static
    exit
  address-family ipv6 vrf 1
   advertise aggregate 2001:DB8::/32
   advertise ospf external
   advertise bgp
   advertise eigrp
   advertise connected
   advertise static
   exit
```

For individual VRFs, routes from the specified prefix can be aggregated after advertising them into OMP using **advertise** *protocol* config command. By default, the aggregated prefixes and all individual prefixes are advertised. To advertise only the aggregated prefix, include the **aggregate-only** option as shown below.

```
config-transaction
 sdwan
  omp
   address-family ipv4 vrf 1
    advertise aggregate 10.0.0.0/8 aggregate-only
    exit
```

Note Route advertisements in OMP are done either by applying configuration at the global level or to specific VRFs. The specific VRF configuration does not override global-VRF configuration in OMP.

When BGP advertises routes into OMP, it advertises each prefix's metric. BGP can also advertise the prefix's AS path.

```
config-transaction
 router bgp 200
 address-family ipv4 vrf 11
  neighbor 1.1.1.0 remote-as 200
  propagate-aspath
  exit
```

When you configure BGP to propagate AS path information, the device sends AS path information to devices that are behind the Cisco IOS XE SD-WAN devices (in the service-side network) that are running BGP, and it receives AS path information from these routers. If you are redistributing BGP routes into OMP, the AS path information is included in the advertised BGP routes. If you configure BGP AS path propagation on some but not all devices in the overlay network, the devices on which it is not configured receive the AS path information but they do not forward it to the BGP routers in their local service-side network. Propagating AS path information can help to avoid BGP routing loops.

In networks that have both overlay and underlay connectivity—for example, when devices are interconnected by both a Cisco SD-WAN overlay network and an MPLS underlay network—you can assign as AS number to OMP itself. For devices running BGP, this overlay AS number is included in the AS path of BGP route updates. To configure the overlay AS:

```
config-transaction
 sdwan
  omp
   overlay-as 55
   exit
```

You can specify the AS number in 2-byte ASDOT notation (1 through 65535) or in 4-byte ASDOT notation (1.0 through 65535.65535). As a best practice, it is recommended that the overlay AS number be a unique AS number within both the overlay and the underlay networks. That use, select an AS number that is not used elsewhere in the network.

If you configure the same overlay AS number on multiple devices in the overlay network, all these devices are considered to be part of the same AS, and as a result, they do not forward any routes that contain the overlay AS number. This mechanism is an additional technique for preventing BGP routing loops in the network.

Configure the Number of Advertised Routes

A Cisco IOS XE SD-WAN device can have up to six WAN interfaces, and each WAN interface has a different TLOC. (A WAN interface is any interface in VPN 0 (or transport VRF) that is configured as a tunnel interface. Both physical and loopback interfaces can be configured to be tunnel interfaces.) The device advertises each route–TLOC tuple to the Cisco vSmart Controller.

The Cisco vSmart Controller redistributes the routes it learns from Cisco IOS XE SD-WAN devices, advertising each route–TLOC tuple. If, for example, a local site has two devices, a Cisco vSmart Controller could potentially learn eight route–TLOC tuples for the same route.

By default, Cisco IOS XE SD-WAN devices and Cisco vSmart Controllers advertises up to four equal-cost route–TLOC tuples for the same route. You can configure them to advertise from 1 to 16 route–TLOC tuples for the same route:

```
Device(config-omp)# send-path-limit 14
```

If the limit is lower than the number of route–TLOC tuples, the Cisco IOS XE SD-WAN device or Cisco vSmart Controller advertises the best routes.

Configure the Number of Installed OMP Paths

Cisco IOS XE SD-WAN devices install OMP paths that they received from the Cisco vSmart Controller into their local route table. By default, a Cisco IOS XE SD-WAN devices installs a maximum of four unique OMP paths into its route table. You can modify this number:

```
vEdge(config-omp)# ecmp-limit 2
```

The maximum number of OMP paths installed can range from 1 through 16.

Configure the OMP Hold Time

The OMP hold time determines how long to wait before closing the OMP connection to a peer. If the peer does not receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. The default OMP hold time is 60 seconds but it can be configured to up to 65,535 seconds. To modify the OMP hold time interval:

```
Device(config-omp)# timers holdtime 75
```

The hold time can be in the range 0 through 65535 seconds.

The keepalive timer is one-third the hold time and is not configurable.

If the local device and the peer have different hold time intervals, the higher value is used.

If you set the hold time to 0, the keepalive and hold timers on the local device and the peer are set to 0.

The hold time must be at least two times the hello tolerance interval set on the WAN tunnel interface in transport VRF. To configure the hello tolerance interface, use the hello-tolerance command.

Configure the OMP Update Advertisement Interval

By default, OMP sends Update packets once per second. To modify this interval:

```
Device(config-omp)# timers advertisement-interval 5000
```

The interval can be in the range 0 through 65535 seconds.

Configure the End-of-RIB Timer

After an OMP session goes down and then comes back up, an end-of-RIB (EOR) marker is sent after 300 seconds (5 minutes). After this maker is sent, any routes that were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. To modify the EOR timer:

```
Device(config-omp)# timers eor-timer 300
```

The time can be in the range 1 through 3600 seconds (1 hour).

Mapping Multiple BGP Communities to OMP Tags

Table 30: Feature History

Feature Name	Release Information	Description
Mapping Multiple BGP Communities to OMP Tags	Cisco IOS XE Release 17.2.1r	This features allows you to display information about OMP routes on Cisco vSmart Controller and Cisco IOS XE SD-WAN devices. OMP routes carry information that the device learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes.

For more information on the **show sdwan omp routes** command, refer show sdwan omp routes.

Configure EIGRP Using Cisco vManage

To configure EIGRP routing protocol using Cisco vManage templates follow these steps:

1. Create an EIGRP feature template to configure EIGRP parameters.
2. Create a VPN feature template to configure VPN parameters for service-side routing (any VPN other than VPN 0 or VPN 512).
3. Create a device template and apply the templates to the correct devices.

Create an EIGRP Template

1. From the Cisco vManage, navigate to **Configuration** > **Templates**.
2. Click **Feature**.
3. Click **Add Template** and select a device from the list.
4. From the Other Templates section, choose **EIGRP** and enter a name and a description for the template.

Basic Configuration

Click the **Basic Configuration** tab to configure the local autonomous system (AS) number for the template.

Parameter Name	Description
Autonomous System ID *	Enter the local AS number. • **Range**: 1-65,535 • **Default**: None

Configure IP4 Unicast Address Family

To redistribute routes from one protocol (routing domain) into a EIGRP routing domain, click **New Redistribute** and enter the following parameter values:

Table 31: Redistribution Parameters

Parameter Name	Value	Description
Mark as Optional Row	Click **Optional** 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.	
Protocol *	Select the protocols from which to redistribute routes into EIGRP, for all EIGRP sessions.	
	bgp	Redistribute Border Gateway Protocol (BGP) routes into EIGRP.
	connected	Redistribute connected routes into EIGRP.
	nat-route	Redistribute network address translation (NAT) routes into EIGRP.
	omp	Redistribute Overlay Management Protocol (OMP) routes into EIGRP.
	ospf	Redistribute Open Shortest Path First (OSPF) routes into EIGRP. **Note** You can set metric values for redistribution using the CLI add-on feature template from Cisco IOS XE SD-WAN Release 16.12.1b and later. Use the following command: `redistribute ospf 1 metric 1000000 1 1 1 1500` For more information, see CLI Add-on Feature Templates.
	static	Redistribute static routes into EIGRP.
Route Policy *	Enter the name of the route policy to apply to redistributed routes.	
Click **Add** to save the redistribution information.		

To advertise a prefix into the EIGRP routing domain, click the Network tab, and then click **New Network** and enter the following parameter values:

Table 32: Configure Network

Parameter Name	Description
Mark as Optional Row	Click **Optional** 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. See Create a Template Variables Spreadsheet.
Network Prefix *	Enter the network prefix you want EIGRP to advertise in the format of *prefix/mask*.
Click **Add** to save the network prefix.	

Configure Advanced Parameters

To configure advanced parameters for EIGRP, click the **Advanced** tab and configure the following parameter values:

Table 33: Advanced Parameters

Parameter Name	Description
Hold Time (seconds)	Set the interval after which EIGRP considers a neighbor to be down. The local router then terminates the EIGRP session to that peer. This acts as the global hold time. • **Range**: 0 through 65,535 • **Default**: 15 seconds
Hello Interval (seconds)	Set the interval at which the router sends EIGRP hello packets. • **Range**: 0 through 65,535 • **Default**: 5 seconds
Route Policy Name	Enter the name of an EIGRP route policy.

Configure Route Authentication Parameters

The IP Enhanced IGRP Route Authentication feature supports MD5 or HMAC-sha-256 authentication of routing updates from the EIGRP routing protocol. To configure authentication for EIGRP routes:

1. Click the **Authentication** tab.
2. Click **Authentication** to open the Authentication Type field.
3. Select **global** parameter scope.
4. From the drop-down list, select **md5** or **hmac-sha-256**.

Parameter	Option	Description
MD5	**MD5 Key ID**	Enter an MD5 key ID to compute an MD5 hash over the contents of the EIGRP packet using that value.
	MD5 Authentication Key	Enter an MD5 authentication key to use an encoded MD5 checksum in the transmitted packet.
	Authentication Key	A 256-byte unique piece of information that is used to compute the HMAC and is known both by the sender and the receiver of the message.
Click **Add** to save the authentication parameters.		

Note To use a preferred route map, specify both an MD5 key (ID or auth key) and a route map.

Configure Interface Parameters

To configure interface parameters for EIGRP routes, click **Interface**, and enter the following parameter values:

Table 34: Interface Parameters

Parameter Name	Description
Mark as Optional Row	Click **Optional** 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.
Interface name	Enter the interface name(s) on which EIGRP should run.
Shutdown	**No** (the default) enables the interface to run EIGRP. **Yes** disables the interface.
Click **Add** to save the interfaces.	

Configure EIGRP Using CLI

Configure EIGRP on Cisco IOS XE SD-WAN Devices

The following example shows the how to configure EIGRP on Cisco IOS XE SD-WAN devices through CLI.

```
config-transaction
router eigrp vpn
 !
 address-family ipv4 unicast vrf 1 autonomous-system 100
  !
  topology base
   table-map foo filter
   redistribute omp
  exit-af-topology
  network 10.1.44.0 0.0.0.255
 exit-address-family
 !
 address-family ipv6 unicast vrf 1 autonomous-system 200
  !
  topology base
   table-map bar
   redistribute omp
  exit-af-topology
 exit-address-family
!
```

Example: Advertise EIGRP Routes to OMP

```
config-transaction
sdwan
 omp
  no shutdown
  graceful-restart
  address-family ipv4 vrf 1
   advertise eigrp
  !
  address-family ipv6 vrf 1
   advertise eigrp
  !
  address-family ipv4
   advertise connected
   advertise static
  !
 !
```

Verify EIGRP Configuration Using CLI

Configuration on Cisco IOS XE SD-WAN Devices

The outputs of the following show commands show the EIGRP configuration on Cisco IOS XE SD-WAN devices.

View IPv4 EIGRP routes on Cisco IOS XE SD-WAN devices.

```
Device# show ip route vrf 1
m        22.22.22.22 [251/0] via 11.11.11.12, 00:28:00
      55.0.0.0/32 is subnetted, 1 subnets
D EX     55.55.55.55 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
      66.0.0.0/32 is subnetted, 1 subnets
B        66.66.66.66 [20/0] via 192.168.1.3, 00:33:57
      192.168.1.0/32 is subnetted, 3 subnets
D EX     192.168.1.3 [170/1] via 10.1.44.2, 00:33:58, GigabitEthernet3.2
m        192.168.1.33 [251/0] via 11.11.11.14 (3), 00:28:01
```

View IPv6 EIGRP routes on Cisco IOS XE SD-WAN devices.

```
Device# show ipv6 route vrf 1
C   300:4::/64 [0/0]
     via GigabitEthernet3.2, directly connected
L   300:4::1/128 [0/0]
     via GigabitEthernet3.2, receive
D   2000:1:3::1/128 [90/1]
     via FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
L   FF00::/8 [0/0]
     via Null0, receive
cEdge4-Naiming#show ipv6 route vrf 1 2000:1:3::1/128
```

```
Routing entry for 2000:1:3::1/128
  Known via "eigrp 200", distance 90, metric 1
  OMP Tag 888, type internal
  Redistributing via omp
  Route count is 1/1, share count 0
  Routing paths:
    FE80::20C:29FF:FEF5:C767, GigabitEthernet3.2
      From FE80::20C:29FF:FEF5:C767
      Last updated 00:22:06 ago
```

View OMP routes in EIGRP on Cisco IOS XE SD-WAN devices.

```
Device# show eigrp address-family ipv4 vrf 1 topology 44.4.4.0/24
EIGRP-IPv4 VR(vpn) Topology Entry for AS(100)/ID(192.168.1.44)
           Topology(base) TID(0) VRF(1)
EIGRP-IPv4(100): Topology base(0) entry for 44.4.4.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1
  Descriptor Blocks:
  192.168.1.5, from Redistributed, Send flag is 0x0
      Composite metric is (1/0), route is External
      Vector metric:
        Minimum bandwidth is 0 Kbit
        Total delay is 0 picoseconds
        Reliability is 0/255
        Load is 0/255
        Minimum MTU is 0
        Hop count is 0
        Originating router is 192.168.1.44
      External data:
        AS number of route is 0
        External protocol is OMP-Agent, external metric is 4294967294
        Administrator tag is 0 (0x00000000)
```

CHAPTER 4

Segmentation

Network segmentation has existed for over a decade and has been implemented in multiple forms and shapes. At its most rudimentary level, segmentation provides traffic isolation. The most common forms of network segmentation are virtual LANs, or VLANs, for Layer 2 solutions, and virtual routing and forwarding, or VRF, for Layer 3 solutions.

There are many use cases for segmentation:

Use Cases for Segmentation

- An enterprise wants to keep different lines of business separate (for example, for security or audit reasons).
- The IT department wants to keep authenticated users separate from guest users.
- A retail store wants to separate video surveillance traffic from transactional traffic.
- An enterprise wants to give business partners selective access only to some portions of the network.
- A service or business needs to enforce regulatory compliance, such as compliance with HIPAA, the U.S. Health Insurance Portability and Accountability Act, or with the Payment Card Industry (PCI) security standards.
- A service provider wants to provide VPN services to its medium-sized enterprises.

Limitations of Segmentation

One inherent limitation of segmentation is its scope. Segmentation solutions either are complex or are limited to a single device or pair of devices connected via an interface. As an example, Layer 3 segmentation provides the following:

1. Ability to group prefixes into a unique route table (RIB or FIB).
2. Ability to associate an interface with a route table so that traffic traversing the interface is routed based on prefixes in that route table.

This is a useful functionality, but its scope is limited to a single device. To extend the functionality throughout the network, the segmentation information needs to be carried to the relevant points in the network.

How to Enable Network-Wide Segmentation

There are two approaches to providing this network-wide segmentation:

- Define the grouping policy at every device and on every link in the network (basically, you perform Steps 1 and 2 above on every device).
- Define the grouping policy at the edges of the segment, and then carry the segmentation information in the packets for intermediate nodes to handle.

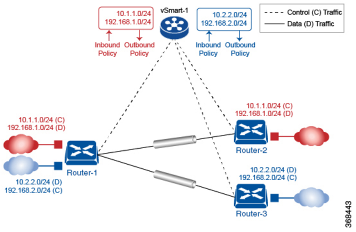
The first approach is useful if every device is an entry or exit point for the segment, which is generally not the case in medium and large networks. The second approach is much more scalable and keeps the transport network free of segments and complexity.

Segmentation in Cisco SD-WAN

In the Cisco SD-WAN overlay network, VRFs divide the network into different segments.

Cisco SD-WAN employs the more prevalent and scalable model of creating segments. Essentially, segmentation is done at the edges of a router, and the segmentation information is carried in the packets in the form of an identifier.

The figure shows the propagation of routing information inside a VRF.



In this figure:

- Router-1 subscribes to two VRFs, red and blue.
  - The red VRF caters to the prefix 10.1.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
  - The blue VRF caters to the prefix 10.2.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-2 subscribes to the red VRF.
  - This VRF caters to the prefix 192.168.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-3 subscribes to the blue VRF.
  - This VRF caters to the prefix 192.168.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).

Because each router has an OMP connection over a TLS tunnel to a vSmart controller, it propagates its routing information to the vSmart controller. On the vSmart controller, the network administrator can enforce policies to drop routes, to change TLOCs (which are overlay next hops) for traffic engineering or service chaining). The network administrator can apply these policies as inbound and outbound policies on the vSmart controller.

All prefixes belonging to a single VRF are kept in a separate route table. This provides the Layer 3 isolation required for the various segments in the network. So, Router-1 has two VRF route tables, and Router-2 and Router-3 each have one route table. In addition, the vSmart controller maintains the VRF context of each prefix.

Separate route tables provide isolation on a single node. So now the question is how to propagate the routing information across the network.

In the Cisco SD-WAN solution, this is done using VRF identifiers, as shown in the figure below. A VRF ID carried in the packet identifies each VRF on a link. When you configure a VRF on a Router, the VRF has a label associated with it. The Router sends the label, along with the VRF ID, to the vSmart controller. The vSmart controller propagates this Router-to- VRF-ID mapping information to the other Routers in the domain. The remote Routers then use this label to send traffic to the appropriate VRF. The local Routers, on receiving the data with the VRF ID label, use the label to demultiplex the data traffic. This is similar to how MPLS labels are used. This design is based on standard RFCs and is compliant with regulatory procedures (such as PCI and HIPAA).

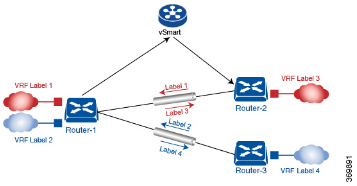


Figure 2:

It is important to point out that the transport network that connects the routers is completely unaware of the VRFs. Only the routers know about VRFs; the rest of the network follows standard IP routing.

VRFs Used in Cisco SD-WAN Segmentation

The Cisco SD-WAN solution involves the use of VRFs to separate traffic.

Global VRF

The global VRF is used for transport. To enforce the inherent separation between services (such as prefixes that belong to the enterprise) and transport (the network that connects the routers), all the transport interfaces (that is, all the TLOCs) are kept in the global VRF. This ensures that the transport network cannot reach the service network by default. Multiple transport interfaces can belong to the same VRF, and packets can be forwarded to and from transport interfaces.

A global VRF contains all interfaces for a device except for the management interface, and all the interfaces are disabled. For the control plane to establish itself so that the overlay network can function, you must configure tunnel interfaces in a global VRF.For each interface in a global VRF, you must set an IP address, and you create a tunnel connection that sets the color and encapsulation for the WAN transport connection. (The encapsulation is used for the transmission of data traffic.) These three parameters—IP address, color, and encapsulation—define a TLOC (transport location) on the router. The OMP session running on each tunnel sends the TLOC to the vSmart controllers so that they can learn the overlay network topology.

Dual Stack Support on Transport VPNs

In the global VRF, Cisco IOS XE SD-WAN devices and vSmart controllers support dual stack. To enable dual stack, configure an IPv4 address and an IPv6 address on the tunnel interface. The router learns from the vSmart controller whether a destination supports IPv4 or IPv6 addresses. When forwarding traffic, the router chooses either the IPv4 or the IPv6 TLOC based on the destination address. But IPv4 is always preferred when configured.

Management VRF

Mgmt-Intf is the management VRF on Cisco IOS XE SD-WAN devices. It is configured and enabled by feault. It carries out-of-band network management traffic among the devices in the overlay network. You can modify this configuration if desired.

Configure VRF Using Cisco vManage Templates

In vManage, use a CLI template to configure VRFs for a device. For each VRF, configure a subinterface and link the subinterface to the VRF. Configure up to 300 VRFs.

When you push a CLI template to a device, Cisco vManage overwrites any existing configuration on the device and loads the configuration defined in the CLI template. Consequently, the template cannot only provide the new content being configured, such as VRFs. The CLI template must include all configuration details required by the device. To display the relevant configuration details on a device, you can use the **show sdwan running-config** command.

For details about creating and applying CLI templates, and for an example of configuring VRFs, see the CLI Templates for Cisco XE SD-WAN Routers chapter of the Systems and Interfaces Configuration Guide.

Supported devices: Cisco ASR1001-HX, ASR1002-HX

Configure VPNs Using vManage Templates

Create a VPN Template

Note Cisco IOS XE 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 SD-WAN devices through Cisco vManage. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE SD-WAN devices.

Step 1 In Cisco vManage, choose **Configuration** > **Templates**.

Step 2 In the Device tab, click **Create Template**.

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

Step 4 From the **Device Model** drop-down, select 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 the **Transport & Management** VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

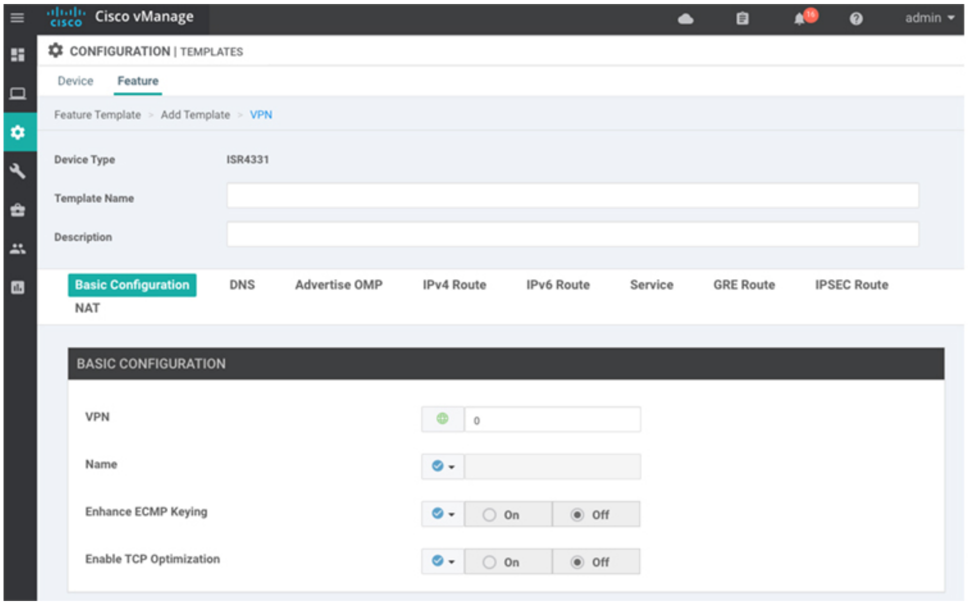
b. From the VPN 0 or VPN 512 drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.

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

a. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the Service VPN section.

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

c. From the VPN drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.



Device Type ISR4331

Template Name

Description

VPN 0

Name

Enhance ECMP Keying ○ On ● Off

Enable TCP Optimization ○ On ● Off

520025

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

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

Configure Basic VPN Parameters

To configure basic VPN parameters, choose the Basic Configuration tab 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 SD-WAN devices: 0 through 65527 Values for Cisco vSmart Controller and Cisco vManage devices: 0, 512

Parameter Name	Description
Name	Enter a name for the VPN. **Note** For Cisco IOS XE SD-WAN devices, you cannot enter a device-specific name for the VPN.

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 Basic Interface Functionality

To configure basic interface functionality in a VPN, choose the **Basic Configuration** tab 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 SD-WAN devices, you must: • Spell out the interface names completely (for example, GigabitEthernet0/0/0). • Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.		
Description	Enter a description for the interface.		
IPv4 / IPv6	Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.		
Dynamic	Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.		
	Both	**DHCP Distance**	Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.
	IPv6	**DHCP Rapid Commit**	Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments. Click **On** to enable DHCP rapid commit Click **Off** to continue using the regular commit process.

Parameter Name	IPv4 or IPv6	Options	Description
Static	Click **Static** to enter an IP address that doesn't change.		
	IPv4	**IPv4 Address**	Enter a static IPv4 address.
	IPv6	**IPv6 Address**	Enter a static IPv6 address.
Secondary IP Address	**IPv4**	Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.	
IPv6 Address	**IPv6**	Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.	
DHCP Helper	**Both**	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers.	
Block Non-Source IP	**Yes** / **No**	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic.	

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

Create a Tunnel Interface

On Cisco IOS XE SD-WAN devices, you can configure up to four tunnel interfaces. This means that each Cisco IOS XE SD-WAN device router can have up to four TLOCs. On Cisco vSmart Controllers and Cisco vManage, 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 the **Interface Tunnel** tab 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 vManage NMS and Cisco vSmart Controller default: Disabled
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

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

Configure DNS and Static Hostname Mapping

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

Parameter Name	Options	Description
Primary DNS Address	Select 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 **Mark as Optional Row** 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 Segmentation Using CLI

Configure VRFs Using CLI

To segment user networks and user data traffic locally at each site and to interconnect user sites across the overlay network, you create VRFs on Cisco IOS XE SD-WAN devices. To enable the flow of data traffic, you associate interfaces with each VRF, assigning an IP address to each interface. These interfaces connect to local-site networks, not to WAN transport clouds. For each of these VRFs, you can set other interface-specific properties, and you can configure features specific for the user segment, such as BGP and OSPF routing, VRRP, QoS, traffic shaping, and policing.

On Cisco IOS XE SD-WAN devices, a global VRF is used for transport. All Cisco IOS XE SD-WAN devices have Mgmt-intf as the default management VRF.

To configure VRFs on Cisco IOS XE SD-WAN devices, follow these steps.

Note

- Use the **config-transaction** command to open CLI configuration mode. The config terminal command is not supported on Cisco IOS XE SD-WAN devices.
- The VRF ID can be any number between 1 through 511 and 513 through 65535. The numbers 0 and 512 are reserved for Cisco vManage and Cisco vSmart controller.

1. Configure service VRFs.

```
config-transaction
 vrf definition 10
  rd 1:10
  address-family ipv4
   exit-address-family
   exit
 address-family ipv6
  exit-address-family
  exit
exit
```

2. Configure the tunnel interface to be used for overlay connectivity. Each tunnel interface binds to a single WAN interface. For example, if the router interface is Gig0/0/2, the tunnel interface number is 2.

```
config-transaction
 interface Tunnel 2
  no shutdown
  ip unnumbered GigabitEthernet1
  tunnel source GigabitEthernet1
  tunnel mode sdwan
  exit
```

3. If the router is not connected to a DHCP server, configure the IP address of the WAN interface.

```
 interface GigabitEthernet 1
 no shutdown
 ip address dhcp
```

4. Configure tunnel parameters.

```
config-transaction
 sdwan
  interface GigabitEthernet 2
   tunnel-interface
    encapsulation ipsec
    color lte
    end
```

Note If an IP address is manually configured on the router, configure a default route as shown below. The IP address below indicates a next-hop IP address.

```
config-transaction
 ip route 0.0.0.0 0.0.0.0 192.0.2.25
```

5. Enable OMP to advertise VRF segment vroutes.

```
sdwan
omp
 no shutdown
 graceful-restart
 no as-dot-notation
 timers
 holdtime 15
 graceful-restart-timer 120
 exit
address-family ipv4
 advertise ospf external
 advertise connected
 advertise static
 exit
address-family ipv6
 advertise ospf external
 advertise connected
 advertise static
 exit
address-family ipv4 vrf 1
 advertise bgp
 exit
exit
```

6. Configure the service VRF interface.

```
config-transaction
 interface GigabitEthernet 2
  no shutdown
  vrf forwarding 10
  ip address 192.0.2.2 255.255.255.0
  exit
```

Verify Configuration

Run the **show ip vrf brief** command to view information about the VRF interface.

```
Device# sh ip vrf brief
  Name                              Default RD            Interfaces
  10                                1:10                  Gi4
  11                                1:11                  Gi3
  30                                1:30
  65528                             <not set>             Lo65528
```

Segmentation (VRFs) Configuration Examples

Some straightforward examples of creating and configuring VRFs to help you understand the configuration procedure for segmenting networks.

Configuration on the vSmart Controller

On the vSmart controller, you configure general system parameters and the two VPNs—VPN 0 for WAN transport and VPN 512 for network management—as you did for the Cisco IOS XE SD-WAN device. Also, you generally create a centralized control policy that controls how the VPN traffic is propagated through the rest of the network. In this particular example, we create a central policy, shown below, to drop unwanted prefixes from propagating through the rest of the network. You can use a single vSmart policy to enforce policies throughout the network.

Here are the steps for creating the control policy on the vSmart controller:

1. Create a list of sites IDs for the sites where you want to drop unwanted prefixes:

   ```
   vSmart(config)# policy lists site-list 20-30 site-id 20
   vSmart(config-site-list-20-30)# site-id 30
   ```

2. Create a prefix list for the prefixes that you do not want to propagate:

   ```
   vSmart(config)# policy lists prefix-list drop-list ip-prefix 10.200.1.0/24
   ```

3. Create the control policy:

   ```
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 match route
   prefix-list drop-list
   vSmart(config-match)# top
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 action reject
   vSmart(config-action)# top
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 default-action
   accept
   vSmart(config-default-action)# top
   ```

4. Apply the policy to prefixes inbound to the vSmart controller:

   ```
   vSmart(config)# apply-policy site-list 20-30 control-policy drop-unwanted-routes in
   ```

Here is the full policy configuration on the vSmart controller:

```
apply-policy
 site-list 20-30
  control-policy drop-unwanted-routes in
 !
!
policy
 lists
  site-list 20-30
   site-id 20
   site-id 30
  !
  prefix-list drop-list
   ip-prefix 10.200.1.0/24
  !
 !
 control-policy drop-unwanted-routes
  sequence 10
   match route
    prefix-list drop-list
   !
   action reject
   !
  !
  default-action accept
 !
!
```

Segmentation CLI Reference

CLI commands for monitoring segmentation (VRFs).

- show dhcp
- show ipv6 dhcp
- show ip vrf brief
- show igmp commands
- show ip igmp groups
- show pim commands

CHAPTER 5

Forwarding and QoS

Forwarding is the transmitting of data packets from one router to another.

Quality of Service (QoS) is synonymous with class of service (CoS). You can enable QoS with localized data policies, which control the flow of data traffic into and out of the interfaces of Cisco vEdge devices and Cisco IOS XE SD-WAN devices.

Cisco SD-WAN Forwarding and QoS Overview

Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote router.

Once the control plane connections of the Cisco SD-WAN overlay network are up and running, data traffic flows automatically over the IPsec connections between the routers. Because data traffic never goes to or through the centralized vSmart controller, forwarding only occurs between the Cisco IOS XE SD-WAN devices as they send and receive data traffic.

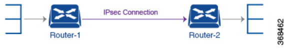
While the routing protocols running in the control plane provide a router the best route to reach the network that is on the service side of a remote router, there will be situations where it is beneficial to select more specific routes. Using forwarding, there are ways you can affect the flow of data traffic. Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote router.

To modify the default data packet forwarding flow, you create and apply a centralized data policy or a localized data policy. With a centralized data policy, you can manage the paths along which traffic is routed through the network, and you can permit or block traffic based on the address, port, and DSCP fields in the packet's IP header. With a localized data policy, you can control the flow of data traffic into and out of the interfaces of a router, enabling features such as quality of service (QoS).

Traffic Behavior With and Without QoS

Default Behavior without Data Policy

When no centralized data policy is configured on the vSmart controller, all data traffic is transmitted from the local service-side network to the local router, and then to the remote router and the remote service-side network, with no alterations in its path. When no access lists are configured on the local router to implement QoS or mirroring, the data traffic is transmitted to its destination with no alterations to its flow properties.

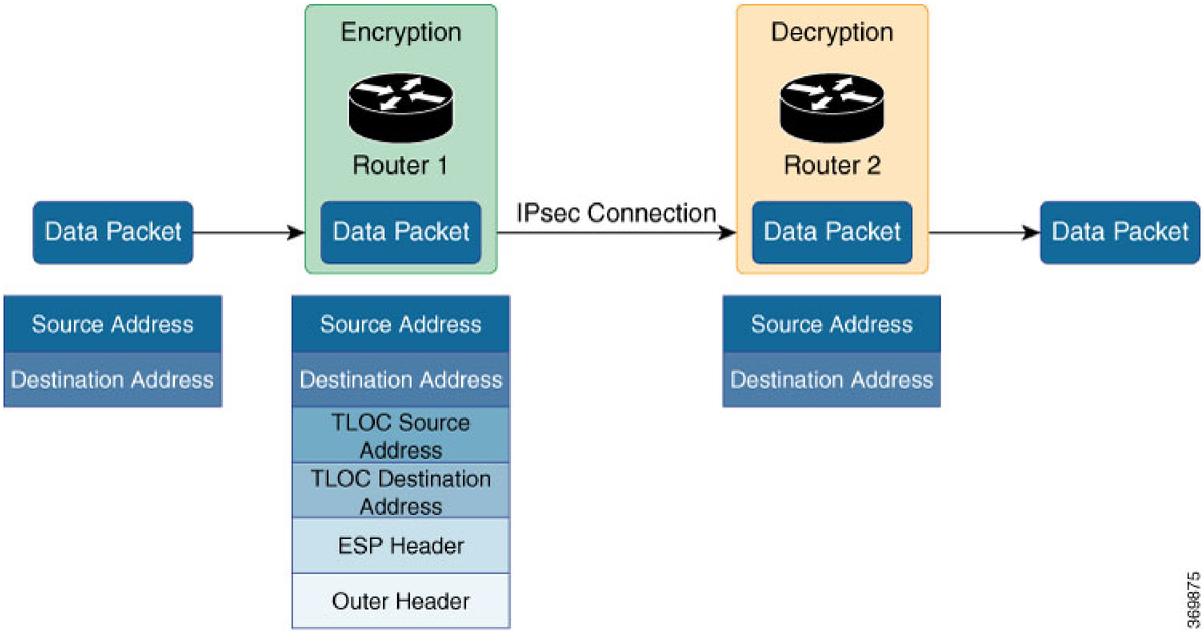


Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured:

- A data packet arriving from the local service-side network and destined for the remote service-side network comes to the router-1. The packet has a source IP address and a destination IP address.
- The router looks up the outbound SA in its VPN route table, and the packet is encrypted with SA and gets the local TLOC. (The router previously received its SA from the vSmart controller. There is one SA per TLOC. More specifically, each TLOC has two SAs, an outbound SA for encryption and an inbound SA for decryption.)
- ESP adds an IPsec tunnel header to the packet.
- An outer header is added to the packet. At this point, the packet header has these contents: TLOC source address, TLOC destination address, ESP header, destination IP address, and source IP address.
- The router checks the local route table to determine which interface the packet should use to reach its destination.
- The data packet is sent out on the specified interface, onto the network, to its destination. At this point, the packet is being transported within an IPsec connection.
- When the packet is received by the router on the remote service-side network, the TLOC source address and TLOC destination address header fields are removed, and the inbound SA is used to decrypt the packet.
- The remote router looks up the destination IP address in its VPN route table to determine the interface to use to reach to the service-side destination.

The figure below details this process.

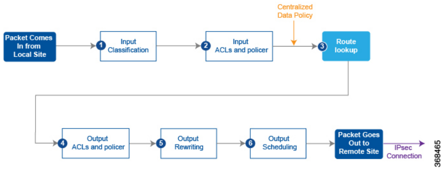
Figure 3: Data Packet Transmission without Policy



Behavior Changes with QoS Data Policy

When you want to modify the default packet forwarding flow, you design and provision QoS policy. To activate the policy, you apply it to specific interfaces in the overlay network in either the inbound or the outbound direction. The direction is with respect to the routers in the network. You can have policies for packets coming in on an interface or for packets going out of an interface.

The figure below illustrates the QoS policies that you can apply to a data packet as it is transmitted from one branch to another. The policies marked Input are applied on the inbound interface of the router, and the policies marked Output are applied on the outbound interface of the router, before the packets are transmitted out the IPSec tunnel.



The table below describes each of the above steps.

Step	Description	Command
1	Define class map to classify packets, by importance, into appropriate forwarding classes. Reference the class map in an access list.	**class-map**
2	Define policer to specify the rate at which traffic is sent on the interface. Reference the policer in an access list. Apply the access list on an inbound interface.	**policer**
3	The router checks the local route table to determine which interface the packet should use to reach its destination.	N/A

Step	Description	Command
4	Define policer and reference the policer in an access list. Apply the access list on an outbound interface.	**policer**
5	Define QoS map to define the priority of data packets. Apply the QoS map on the outbound interface.	**policy-map**
6	Define rewrite-rule to overwrite the DSCP field of the outer IP header. Apply the rewrite-rule on the outbound interface.	**rewrite-rule**

How QoS Works

The QoS feature on the Cisco IOS XE SD-WAN devices and Cisco vEdge devices works by examining packets entering at the edge of the network. With localized data policy, also called access lists, you can provision QoS to classify incoming data packets into multiple forwarding classes based on importance, spread the classes across different interface queues, and schedule the transmission rate level for each queue. Access lists can be applied either in the outbound direction on the interface (as the data packet travels from the local service-side network into the IPsec tunnel toward the remote service-side network) or in the inbound direction (as data packets are exiting from the IPsec tunnel and being received by the local router.

To provision QoS, you must configure each router in the network. Generally, each router on the local service-side network examines the QoS settings of the packets that enter it, determines which class of packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

Classify Data Packets

You can classify incoming traffic by associating each packet with a forwarding class. Forwarding classes group data packets for transmission to their destination. Based on the forwarding class, you assign packets to output queues. The routers service the output queues according to the associated forwarding, scheduling, and rewriting policies you configure.

Schedule Data Packets

You can configure a QoS map for each output queue to specify the bandwidth. This enables you to determine how to prioritize data packets for transmission to the destination. Depending on the priority of the traffic, you can assign packets higher or lower bandwidth, buffer levels, and drop profiles. Based on the conditions defined in the QoS map, packets are forwarded to the next hop.

On Cisco vEdge devices and Cisco IOS XE SD-WAN devices, each interface has eight queues, which are numbered 0 to 7. Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ. Queues 1 to 7 are available for data traffic, and the default scheduling for these seven queues is weighted round-robin (WRR). For these queues, you can define the weighting according to the needs of your network. When QoS is not configured for data traffic, queue 2 is the default queue.

Rewrite Data Packets

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network. Rewrite rules allow you to map traffic to code points when the traffic exits the system. Rewrite rules use the forwarding class information and packet loss priority (PLP) used internally by the Cisco IOS XE SD-WAN devices and Cisco vEdge devices to establish the DSCP value on outbound packets. You can then configure algorithms such as RED/WRED to set the probability that packets will be dropped based on their DSCP value.

Police Data Packets

You can configure policers to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels.

Shaping Rate

You can configure shaping to control the maximum rate of traffic sent. You can configure the aggregate traffic rate on an interface to be less than the line rate so that the interface transmits less traffic than it is capable of transmitting. You can apply shaping to outbound interface traffic.

Limitations for Forwarding on Cisco IOS XE SD-WAN Devices

The following features are not supported on Cisco IOS XE SD-WAN devices

- Mirroring is not supported.
- Delaying buffer size is not supported.
- Specifying packet loss priority (PLP) is not supported.
- Policers cannot be applied on interfaces.
- Decreased priority dropping is not supported.

QoS vManage

Forwarding and QoS Configuration Examples

This section shows examples of how you can use access lists to configure quality of service (QoS), classifying data packets and prioritizing the transmission properties for different classes. Note that QoS is synonymous with class of service (CoS).

This example shows how to configure class of service (CoS) to classify data packets and control how traffic flows out of and into the interfaces on Cisco IOS XE SD-WAN devices on the interface queues. To configure a QoS policy:

1. Map each forwarding class to an output queue.
2. Configure the QoS scheduler for each forwarding class.
3. Define an access list to specify match conditions for packet transmission and apply it to a specific interface.

4. Apply the queue map and the rewrite rule to the egress interface.

The sections below show examples of each of these steps.

Map Each Forwarding Class to Output Queue

This example shows a data policy that classifies incoming traffic by mapping each forwarding class to an output queue.

```
policy
class-map
  class Queue0 queue 0
  class ef queue 0
  class Queue1 queue 1
  class Queue2 queue 2
  class be queue 2
  class Queue3 queue 3
  class af1 queue 3
  class Queue4 queue 4
  class af2 queue 4
  class Queue5 queue 5
  class af3 queue 5
!
```

Configure QoS Scheduler for Each Forwarding Class

This example illustrates how to configure the QoS scheduler for each queue to define the importance of data packets.

```
class-map match-any Queue0
match qos-group 0
!
class-map match-any Queue1
match qos-group 1
!
class-map match-any Queue2
match qos-group 2
!
class-map match-any Queue3
match qos-group 3
!
class-map match-any Queue4
match qos-group 4
!
class-map match-any Queue5
match qos-group 5
!

policy-map test
class Queue0
  priority percent 20
!
class Queue1
  random-detect
  bandwidth percent 20
!
class class-default
  bandwidth percent 20
!
class Queue3
```

```
  bandwidth percent 15
!
class Queue4
  random-detect
  bandwidth percent 15
!
class Queue5
  bandwidth percent 10
!
!
```

Create Access Lists to Classify Data Packets

Define Access Lists

Define an access list to specify match conditions for packet transmission.

```
policy
access-list acl1
  sequence 1
   match
    dscp 46 48
   !
   action accept
    class ef
   !
  !
  sequence 11
   match
    dscp 34
   !
   action accept
    class af3
   !
  !
  sequence 21
   match
    dscp 24
   !
   action accept
    class af2
   !
  !
  sequence 31
   match
    dscp 18
   !
   action accept
    class af1
   !
  !
  sequence 41
   match
    dscp 0 10
   !
   action accept
    class be
    log
   !
  !
  default-action accept
!
```

Apply Access Lists

Apply Access List to a Specific Interface

This example illustrates how to apply the previously access list defined on the input of a service interface. Here "access-list acl1" is applied on the input of interface Gi0/0/1.

```
sdwan
interface GigabitEthernet0/0/1
  access-list acl1 in
!
 !
!
```

Configure and Apply Rewrite Rule

Configure Rewrite Rule

This example shows how to configure the rewrite rule to overwrite the DSCP field of the outer IP header. Here the rewrite rule "transport" overwrites the DSCP value for forwarding classes based on the drop profile. Since all classes are configured with RED drop, they can have one of two profiles: high drop or low drop. The rewrite rule is applied only on the egress interface, so on the way out, packets classified as "af1" and a Packet Loss Priority (PLP) level of low are marked with a DSCP value of 3 in the IP header field, while "af1" packets with a PLP level of high are marked with 4. Similarly, "af2" packets with a PLP level of low are marked with a DSCP value of 5, while "af2" packets with a PLP level of high are marked with 6, and so on.

Apply the Queue Map and Rewrite Rule to the Egress Interface

```
policy
rewrite-rule transport
  class af1 low layer-2-cos 1
  class af2 low dscp 16 layer-2-cos 2
  class af3 low dscp 24 layer-2-cos 3
  class be low dscp 0
  class ef low dscp 46 layer-2-cos 5
!
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule transport
exit
```

Verify Configuration of QoS Policy Map

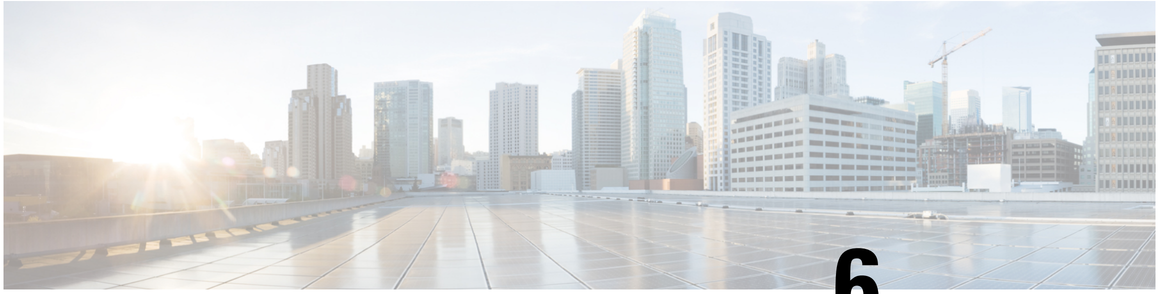
```
Device#show policy-map interface GigabitEthernet0/0/2
 GigabitEthernet0/0/2

  Service-policy output: shape_GigabitEthernet0/0/2

    Class-map: class-default (match-any)
      33823 packets, 6855717 bytes
      5 minute offered rate 31000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 33823/6855717
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000

      Service-policy : test

        queue stats for all priority classes:
          Queueing
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 33802/6853827

        Class-map: Queue0 (match-any)
          33802 packets, 6853827 bytes
          5 minute offered rate 31000 bps, drop rate 0000 bps
          Match: qos-group 0
          Priority: 20% (20000 kbps), burst bytes 500000, b/w exceed drops: 0


        Class-map: Queue1 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 1
          Queueing
          queue limit 83 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts output/bytes output) 0/0
          bandwidth 20% (20000 kbps)
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0 packets
            class       Transmitted         Random drop      Tail drop          Minimum
     Maximum     Mark
                    pkts/bytes            pkts/bytes       pkts/bytes          thresh
    thresh     prob

            0               0/0               0/0              0/0                 20
       41  1/10
            1               0/0               0/0              0/0                 22
       41  1/10
            2               0/0               0/0              0/0                 25
       41  1/10
            3               0/0               0/0              0/0                 27
       41  1/10
            4               0/0               0/0              0/0                 30
       41  1/10
            5               0/0               0/0              0/0                 32
       41  1/10
            6               0/0               0/0              0/0                 35
       41  1/10
            7               0/0               0/0              0/0                 37
       41  1/10

        Class-map: Queue3 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 3
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 15% (15000 kbps)

        Class-map: Queue4 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 4
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 15% (15000 kbps)
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0 packets
            class       Transmitted         Random drop      Tail drop          Minimum
     Maximum     Mark
                    pkts/bytes            pkts/bytes       pkts/bytes          thresh
    thresh     prob

            0               0/0               0/0              0/0                   16
       32  1/10
            1               0/0               0/0              0/0                   18
       32  1/10
            2               0/0               0/0              0/0                   20
       32  1/10
            3               0/0               0/0              0/0                   22
       32  1/10
            4               0/0               0/0              0/0                   24
       32  1/10
            5               0/0               0/0              0/0                   26
       32  1/10
            6               0/0               0/0              0/0                   28
       32  1/10
            7               0/0               0/0              0/0                   30
       32  1/10

        Class-map: Queue5 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 5
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 10% (10000 kbps)

        Class-map: class-default (match-any)
          21 packets, 1890 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
          Queueing
          queue limit 83 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 21/1890
          bandwidth 20% (20000 kbps)
```

Reference: Forwarding and QoS CLI Commands

Monitoring Commands

Use the following commands to monitor forwarding and QoS on a Cisco IOS XE SD-WAN device:

```
show sdwan policy access-list-associations
show sdwan policy access-list-counters
show sdwan policy access-list-names
show sdwan policy access-list-policers
show sdwan policy data-policy-filter
show sdwan policy rewrite-associations
show policy-map interface GigabitEthernet0/0/2
```



CHAPTER 6

QoS on Subinterface

Table 35: Feature History

Feature Name	Release Information	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces.	

A physical interface may be treated as multiple interfaces by configuring one or more logical interfaces called subinterfaces. One use case is separating the traffic of different VLANs by using a separate subinterface for each VLAN.

Quality of Service (QoS) policies may be applied to individual subinterfaces. Configure QoS as usual, specifying the interface and subinterface using the *interface.subinterface* notation. For example, for GigabitEthernet interface 4, subinterface 100:

GigabitEthernet4.100

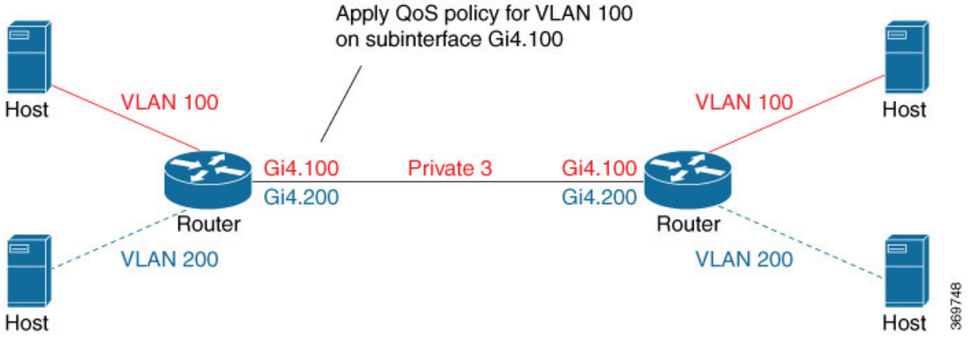
Limitations

- Do not configure a QoS policy on both a main interface and one of its subinterfaces. The exception is a class-default shape policy on the main interface.
- A QoS policy that is applied to a subinterface must have shaping defined. This configured with the shape command. Example:

```
policy-map shape_GigabitEthernet4.100
    class class-default
        service-policy xyz_QoS-model
        shape average 100000000
```

Configuration Example: QoS on Subinterface

This example applies a QoS policy to subinterface GigabitEthernet4.100 (shown in red in the figure below). This subinterface handles traffic for VLAN 100. The QoS policy affects only subinterface GigabitEthernet4.100, and not subinterface GigabitEthernet4.200, which is on the same physical interface.



Configuration by CLI

```
class-map match-any DATA
     match qos-group 1
class-map match-any Queue0
     match qos-group 0
class-map match-any Queue1
     match qos-group 1
class-map match-any Queue2
     match qos-group 2
class-map match-any Queue7
     match qos-group 7
class-map match-any WEB
     match qos-group 7

policy-map xyz_QoS-model
     class Queue0
          priority percent 37
     class Queue1
          bandwidth percent 33
      class Queue7
            random-detect
           bandwidth percent 10
      class class-default
            random-detect
           bandwidth percent 20
policy-map shape_GigabitEthernet4.100
     class class-default
           service-policy xyz_QoS-model
           shape average 100000000
 !

interface GigabitEthernet4.100
 no shutdown
 encapsulation dot1Q 100
 ip address 173.10.0.2 255.255.255.0
 ip mtu 1496
 service-policy output shape_GigabitEthernet4.100
exit
```

```
exit
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet4.100
 tunnel source GigabitEthernet4.100
 tunnel mode sdwan
exit

sdwan
 interface GigabitEthernet4.100
  tunnel-interface
   encapsulation ipsec
   color private3 restrict
   max-control-connections 0

policy
 class-map
  class Queue0 queue 0
  class VOICE queue 0
  class DATA queue 1
  class Queue1 queue 1
  class Queue2 queue 2
  class Queue7 queue 7
  class WEB queue 7
 !
```

Configuration by vManage

To apply a QoS policy to a subinterface using vManage, the procedure is similar to that used for configuring policies on a main interface. Add a subinterface feature template to the device template for the target device. This enables loading the QoS policy onto the subinterface.

Preparation

- **Configure a QoS Policy**

  Configuration > Policies > Localized Policy > Custom Options > Forwarding Class/QoS

- **Apply a QoS Policy to a Subinterface**

  Apply a QoS policy and define shaping.

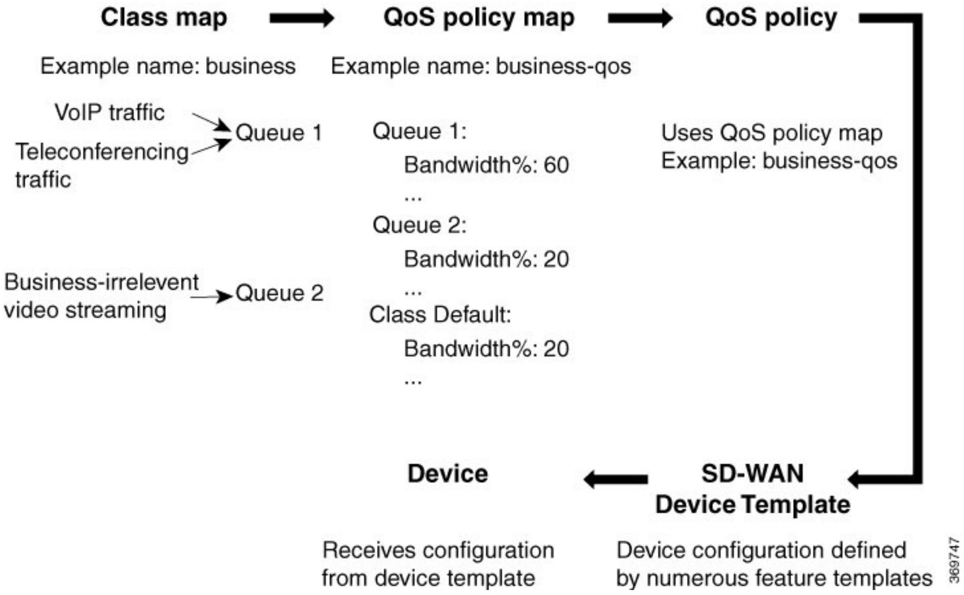
  1. Configuration > Feature > feature-name > ACL/QoS
  2. Configure the following fields:
     - Shaping Rate (Kbps)
     - QoS Map

Procedure

This procedure applies a QoS policy to a subinterface.

Prerequisite: One or more class maps have been defined. These assign classes of traffic (for example, VoIP traffic) to specific queues.

Figure 4: Overview of Workflow for Applying a QoS Policy



1. Create a QoS policy map.
   a. Configuration > Policies
   b. Click **Localized Policy** at the top.
   c. Click the **Add Policy** button to create a new policy map.
   d. Click **Next**.
   e. Click the **Add QoS Map** button and select **Create New** from the dropdown menu.
   f. (This step relies on class maps that have been defined. The class maps assign classes of traffic to specific queues. The queues then represent those classes of traffic. This step uses the queues to control how the traffic will be handled.)

      In the Add Queue dialog box, select queues that represent the types of traffic relevant to the QoS objectives. Configure parameters such as Bandwidth% and Buffer% for the queues. For example, to configure bandwidth for audio traffic, select a queue that represents audio traffic and configure the bandwidth parameter. Click the **Save Queue** button.
   g. Click the **Save Policy** button.

2. Create a QoS policy that uses the QoS policy map defined above.

   See the documentation for creating a QoS policy.

3. Use a device template to push the QoS policy to the target device.

   (Note: The device policy defines other parts of the device configuration also. This procedure only affects the QoS policy portion.)
   a. Configuration > Templates
   b. In the list of templates, locate the device template for the target device.

- **c.** In table row for that template, click the **...** button at the right, and select Edit.
- **d.** In the Additional Templates area, in the Policy field, click the dropdown menu and select the policy name.
- **e.** Click **Update**.
- **f.** Click **Next**.
- **g.** In the left pane, select the target device. The configuration appears in the right pane.
- **h.** Click the **Configure Devices** button to push the policy to the device. SD-WAN displays the Task View, showing the status of the update tasks.

4. Load the QoS policy onto the subinterface.

Prerequisite: The subinterface feature template must already have been added to the device template.

- **a.** Configuration > Templates
- **b.** Click **Feature** at the top.
- **c.** In the list of templates, locate the feature template for the subinterface. (This is the subinterface to which you are assigning the QoS policy.)
- **d.** In the Device Templates column, confirm that the feature template is assigned to a device template.
- **e.** In the Devices Attached column, confirm that the feature template is assigned to a device.
- **f.** In table row for the template, click the **...** button at the right, and select Edit.
- **g.** Click **ACL/QoS** to jump to the ACL/QoS section.
- **h.** In the Shaping Rate field, use the dropdown menu to select **Global** or **Device Specific**, and enter a shaping rate value.
- **i.** In the QoS Map field, use the dropdown menu to select **Global** and enter the QoS policy map name.
- **j.** Click **Update**.
- **k.** In the left pane, select the device to display the configuration in the right pane.
- **l.** Click the **Configure Devices** button to push the policy map to the subinterface. SD-WAN displays the Task View, showing the status of the update tasks.

CHAPTER 7

Protocols in Cisco SD-WAN

This chapter discusses the protocols supported in Cisco SD-WAN.

BFD

The BFD protocol, which detects link failures as part of the Cisco SD-WAN high availability solution, is enabled by default on all Cisco Cisco IOS XE SD-WAN devices and you cannot disable it.

The following procedure shows how to create a new BFD template and specify parameters.

1. In Cisco vManage, navigate to **Configuration** > **Templates**.
2. Click the **Feature** tab.
3. Click **Add Template**.
4. Choose a device from device list. Templates applicable to the device you choose are displayed in the right pane.
5. Select the **Cisco BFD** template.
6. Enter a name and description for your template.

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 choose one of the following: Global or Device Specific.

Configure BFD for Application-Aware Routing

To configure the BFD timers used by application-aware routing, click the **Basic Configuration** tab and configure the following parameters:

Table 36: Basic Configuration

Parameter Name	Description
Multiplier	Specify the value by which to multiply the poll interval, to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet configured SLAs.*Range:* 1 through 6*Default:* 6
Poll Interval	Specify how often BFD polls all data plane tunnels on a vEdge router to collect packet latency, loss, and other statistics used by application-aware routing.*Range:* 1 through 4,294,967,296 (2^{32} – 1) milliseconds*Default:* 600,000 milliseconds (10 minutes)

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

CLI equivalent:

```
bfd  app-route
  multiplier number
  poll-interval milliseconds
```

Configure BFD on Transport Tunnels

To configure the BFD timers used on transport tunnels, click the **Color** tab. Next, click **Add New Color**, and configure the following parameters:

Table 37:

Parameter Name	Description
Color	From the drop-down, choose the color of the transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider. *Values:* 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver. Default: default
Hello Interval	Specify how often BFD sends Hello packets on the transport tunnel. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel. Range: 100 through 60000 milliseconds. Default: 1000 milliseconds (1 second)
Multiplier	Specify how many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time. Range: 1 through 60. Default: 7 (for hardware vEdge routers), 20 (for vEdge Cloud software routers).
Path MTU Discovery	Click **On** to enable path MTU discovery for the transport tunnel, or Off to disable. When PMTU discovery is enabled, configuration change in interface MTU reflects immediately in tunnel-mtu and PMTU value is not configurable (it is triggered every 20 mins). Notifications are not sent to Cisco vManage for MTU change. When PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes, but the effective tunnel MTU is 1468 bytes. Default: Enabled.

Parameter Name	Description
Add	Click **Add** to save the data traffic transport tunnel color.

To add another color, click **Add New Color**.

A table lists the transport tunnel colors.

To edit a color, click the Pencil icon. The Update Color popup is displayed. After you make the desired changes, click **Save Changes**.

To remove a color, click the trash icon to the right of the entry.

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

CLI equivalent:

```
bfd  color color
  hello-interval milliseconds
  multiplier number
  pmtu-discovery
```

Other Supported Protocols

This topic lists all the other protocols supported in Cisco SD-WAN.

- DHCP Server: See the System and Interfaces guide for more information.
- BGP, OSPF, OMP: See the Unicast Overlay Routing chapter in this guide for more information.
- PIM, IGMP: See the Multicast Overlay Routing chapter in this guide for more information.