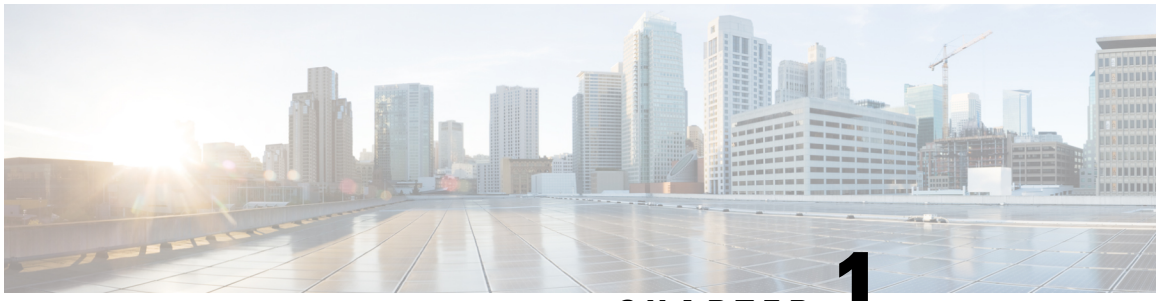
Cisco Catalyst SD-WAN Network Management Guide, Releases 26.x and Later

First Published: 2026-04-24

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

CONTENTS



CHAPTER 1

Read Me First

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

Related References

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

User Documentation

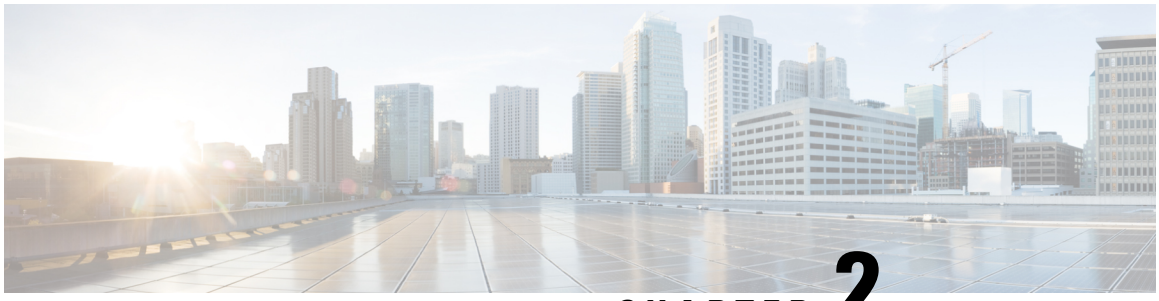
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

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

Documentation Feedback

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



CHAPTER 2

VPN

VPN

A VPN template in Cisco Catalyst SD-WAN is a configuration template that

- enables the creation of separate feature templates for each VPN, and
- supports configuration of VPN 0 and VPN 512 on all device types, with additional VPN templates for segmenting service-side user networks on Cisco IOS XE Catalyst SD-WAN devices.

Types of VPNs

The types of VPNs in Cisco Catalyst SD-WAN include:

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

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

Interfaces in the WAN Transport VPN

A VPN 0 is a WAN transport VPN that

- handles all control plane traffic carried over OMP sessions in the overlay network,

- requires at least one interface configured in VPN 0 for a Cisco IOS XE Catalyst SD-WAN device to participate in the overlay network, and
- mandates that at least one interface connects to a WAN transport network, such as the Internet or an MPLS or a metro Ethernet network.

Tunnel interface configurations

The WAN transport interface, known as a tunnel interface, is configured in VPN 0.

To configure a tunnel interface on a Cisco SD-WAN Controller or a Cisco SD-WAN Manager, you must create an interface in VPN 0, assign an IP address (static or via DHCP), enable the interface with the **no shutdown** command, and mark it as a tunnel interface.

The IP address can be either IPv4 or IPv6. To enable dual stack, configure both address types. Optionally, you can associate a color with the tunnel.

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

On Cisco IOS XE Catalyst SD-WAN devices, tunnel interfaces must have an IP address, a color, and an encapsulation type. For releases before Cisco IOS XE Catalyst SD-WAN Release 17.3.2, dual stack is enabled by configuring both IPv4 and IPv6 addresses. Starting from Release 17.3.2, only one address type is supported per TLOC or interface. Using a second address type requires a second TLOC or interface on which it can be provisioned.

On Cisco Catalyst SD-WAN Controllers and Controller NMSs, interface names can be either ethnumber or loopbacknumber, and only VPN 0 and VPN 512 are supported for interface configuration.

On Cisco SD-WAN Controller and Cisco SD-WAN Manager, *interface-name* can be either **eth** *number* or **loopback** *number*, and only VPN 0 and VPN 512 are supported for interface configuration. Hence, all interfaces are present only on these VPNs.

Dual stack configuration

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

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

Interfaces in the Management

VPN 512 is a default out-of-band management VPN that

- is included as part of the factory-default configuration for out-of-band management, and
- is converted to VRF Mgmt-Intf on Cisco IOS XE Catalyst SD-WAN devices, which use VRFs in place of VPNs.

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

Configure VPN

Use one of these methods to configure VPN parameters:

- Configuration group
- Feature template
- CLI commands

Configure VPN using configuration groups

Configure transport VPN using a configuration group

Before you begin

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

Procedure

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

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

a) Enter the basic configuration information.

Table 1: Basic Configuration

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

b) Enter DNS information.

Table 2: DNS

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

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

c) Enter host happing information.

Table 3: Host Mapping

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

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter the route details.

Table 4: Route

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

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

Add IPv6 Static Route	

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

b) Enter the NAT details

Table 5: NAT

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

c) Enter the service information.

Table 6: Service

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

What to do next

Also see Deploy a Configuration Group.

Configure management VPN using a configuration group

Before you begin

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

Procedure

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

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

a) Enter the basic configuration information.

Table 7: Basic Configuration

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

b) Enter DNS information.

Table 8: DNS

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

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

c) Enter host happing information.

Table 9: Host Mapping

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

d) Enter the IPv4/IPv6 static route information.

Table 10: IPv4/IPv6 Static Route

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

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

Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description

Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route:
	• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv6 address.
	  Administrative distance*: Enter the administrative distance for the route.
	• **Null 0**: When you choose this option, the following field appears:
	  • **NULL0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.
	• **NAT**: When you choose this option, the following field appears:
	  • **IPv6 NAT**: Choose NAT64 or NAT66.

What to do next

Also see Deploy a Configuration Group.

Configure service VPN using a configuration group

This section helps you configure a service VPN (range 1 – 65527, except 512) or the LAN VPN.

Before you begin

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

Procedure

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

Step 2 Create and configure Service VPN in a Service profile.

a) Enter the basic configuration information.

Table 11: Basic Configuration

Field	Description
VPN*	Enter the numeric identifier of the VPN.
Name*	Enter a name for the VPN.

Field	Description
OMP Admin Distance IPv4	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.
OMP Admin Distance IPv6	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.

b) Enter DNS information.

Table 12: DNS

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

c) Enter host happing information.

Table 13: Host Mapping

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

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter advertise OMP information.

Table 14: Advertise OMP

Field	Description
Add OMP Advertise IPv4	

Field	Description
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **bgp** • **ospf** • **ospfv3** • **connected** • **static** • **network** • **aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway. • **eigrp** • **lisp** • **isis**
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Add OMP Advertise IPv6	

Field	Description
Protocol	**Note** Advertising IPv6 OMP routes as network statements is not supported. This applies when using the Service VPN feature in a configuration group, and applies also when using a Cisco VPN feature template. You can configure to advertise: • IPv6 routes by BGP and OSPF protocols • Connected routes, static routes, and aggregate routes The reason for the lack of support is that the Service VPN feature and the Cisco VPN feature template both use the **advertise network** *prefix* command, which does not fully support IPv6 addresses. Choose a protocol to configure route advertisements to OMP, for this VPN: • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway.
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Protocol Sub Type	When you choose the OSPF protocol, specify the sub type as external.

b) Enter route information.

Table 15: Route

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

Field	Description
Subnet Mask*	Enter the subnet mask.
Next Hop/Null 0/VPN/DHCP	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option, the **IPv4 Route Gateway Next Hop** field appears. Enable this option to add the next hop. You can add a hop with and without a tracker. When you click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. When you click **Add Next Hop with Tracker**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. • **Tracker***: Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device. • **Null 0**: When you choose this option, the following field appears: • **IPv4 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **VPN**: When you choose this option, the following field appears: • **IPv4 Route VPN***: Selects VPN as the gateway to direct packets to the transport VPN. • **DHCP**: When you choose this option, the following field appears: • **IPv4 Route Gateway DHCP***: Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address.
Add BGP Routing	Choose a BGP route.
Add OSPF Routing	Choose an OSPF route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description

Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route:
	• **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear:
	  • **Address***: Enter the next-hop IPv6 address.
	  • **Administrative distance***: Enter the administrative distance for the route.
	• **Null 0**: When you choose this option, the following field appears:
	  • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.
	• **NAT**: When you choose this option, the following field appears:
	  • **IPv6 NAT***: Choose NAT64 or NAT66.
	• **Interface**: When you choose this option, the following fields appear:
	  • **Interface Name**: Choose IPv6 interface name for the IPsec tunnel.
	  • **Next Hop**: Enter the IPv6 address and the administrative distance for the next hop.

c) Enter service information.

Table 16: Service

Field	Description
Add Service	
Service Type	Choose a service available at the local site and in the VPN. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**, **TE**, **SIG**
IPv4 Addresses (Maximum: 4)*	Enter up to four IP address, separated by commas. The service is advertised to the Cisco SD-WAN Controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP. You can configure up to four IP addresses.
Tracking*	Cisco Catalyst SD-WAN tests each service device periodically to check whether it is operational. Tracking saves the results of the periodic tests in a service log. Tracking is enabled by default.

d) Enter service route information.

Table 17: Service Route

Field	Description
Add Service Route	
Prefix*	Enter the IP address or prefix. For Umbrella SIG, use any RFC 1918 subnet for Service IP addresses.
Service*	Configure routes pointing to any service. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**.
VPN*	Destination VPN to resolve the prefix.

e) Enter GRE route information.

Table 18: GRE Route

Field	Description
Add GRE Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.
Interface*	Enter the name of one or two GRE tunnels to use to reach the service.
VPN*	Enter the number of the VPN to reach the service. This must be VPN 0.

f) Enter IPSEC route information.

Table 19: IPSEC Route

Field	Description
Add ipSec Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.
Interface*	Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

g) Enter NAT information.

Table 20: NAT

Field	Description
Nat Pool	

Field	Description
NatPool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Prefix Length*	Enter the NAT pool prefix length.
Range Start*	Enter a starting IP address for the NAT pool.
Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Enabled
Direction*	Choose the NAT direction.
Nat64 V4 Pool	
Nat64 V4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Nat 64 V4 Pool Range Start*	Enter a starting IP address for the NAT pool.
Nat 64 V4 Pool Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

h) Enter route leak information.

Table 21: Route leak from Global VPN

Field	Description
Route Protocol*	Choose a protocol to configure leak routes from global VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in service VPN)	

Field	Description
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

Table 22: Route leak to Global VPN

Field	Description
Route Protocol*	Choose a protocol to leak routes from the service VPN that you are configuring to the global VPN: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf**
Select Route Policy	Enter the name of the route policy.
Select Route Policy	Choose a route policy from the drop-down list.

Table 23: Route leak between services

Field	Description
Source VPN	Enter a value of the source VPN.

Field	Description
Route Protocol*	Choose a protocol from the available options to leak routes from the source service VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in Service VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

i) Enter route target information.

Table 24: Route Target

Field	Description
IPv4 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It imports routing information from the target VPN extended community.
Export Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It exports routing information to the target VPN extended community.
IPv6 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It imports routing information from the target VPN extended community.

Field	Description
Export Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It exports routing information to the target VPN extended community.

What to do next

Also see Deploy a Configuration Group.

Configure VPN using templates

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

You can configure a static route through the VPN template.

Procedure

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

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

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

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

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

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

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

b) From the VPN 0 or VPN 512 drop-down list, click **Create Template**. The VPN template form appears.

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

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

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

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

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

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

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

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

Step 9 Configure the VPN template parameters.

a) Configure basic VPN parameters.

Parameter Name	Description
VPN	Enter the numeric identifier of the VPN. Range for Cisco IOS XE Catalyst SD-WAN devices: 0 through 65527 Values for Cisco SD-WAN Controller and Cisco SD-WAN Manager devices: 0, 512
Name	Enter a name for the VPN. **Note** For Cisco IOS XE Catalyst SD-WAN devices, you can't enter a device-specific name for the VPN.
Enhance ECMP keying	Click **On** to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source, and destination IP addresses, as the ECMP hash key. ECMP keying is **Off** by default.
OMP Admin Distance (IPv4)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv4 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251
OMP Admin Distance (IPv6)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv6 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251

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

b) Configure DNS addresses and static hostname mapping.

Parameter Name	Options	Description
Primary DNS Address	Click either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN.	

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

Configure VPN parameters using CLI commands

Configure load-balancing algorithm using CLI commands

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

Follow these steps to configure load-balancing algorithm using CLI commands:

Procedure

Step 1 Select a Cisco Express Forwarding load-balancing algorithm for non Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

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

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

Step 2 Enable load balancing algorithm on an interface for Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

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

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

Map host names to IP addresses using CLI commands

Perform this task to associate host names with IP addresses.

A name server is used to keep track of information associated with domain names. A name server can maintain a database of host name-to-address mappings. Each name can map to one or more IP addresses. In order to use this service to map domain names to IP addresses, you must specify a name server.

Procedure

Step 1 Define a static host name-to-address mapping in the host name cache.

Example:

```
Device(config)# ip host cisco-rtp 192.168.0.148
```

Step 2 Define a default domain name that Cisco Catalyst SD-WAN can use to complete unqualified host names.

Example:

```
Device(config)# ip domain name cisco.com
```

Step 3 Specify one or more hosts that supply name information.

Example:

```
Device(config)# ip name-server 172.16.1.111 172.16.1.2
```

Step 4 Enable DNS-based address translation.

DNS is enabled by default. Use this command if DNS has been disabled.

Example:

```
Device(config)# ip domain lookup
```

The following example configures the host-name-to-address mapping process. IP DNS-based translation is specified, the addresses of the name servers are specified, and the default domain name is given.

```
! 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
```

Verify the VPN configuration

This section provides examples for VPN configurations.

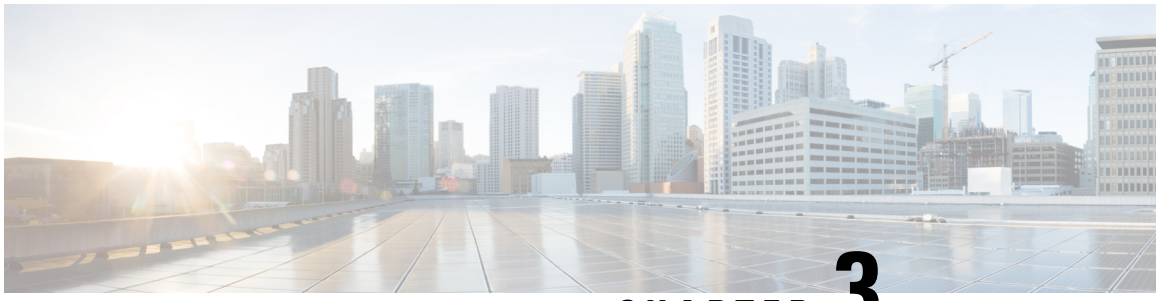
Use the **show sdwan running-config | sec vrf definition Mgmt-intf** command to verify the management interface configurations.

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

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

vrf definition Mgmt-intf
 rd 1:512
 !
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 192.168.20.11 255.255.255.0
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0
!
```

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

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 8000 bits/sec, 12 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
   4839793 packets input, 415574814 bytes, 0 no buffer
   Received 3060073 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   82246 packets output, 41970224 bytes, 0 underruns
   Output 0 broadcasts (0 IP multicasts)
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```



CHAPTER 3

Network Slicing

Feature history of network slicing

Table 25: Feature History

Feature Name	Release Information	Description
Cellular Network Slicing	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature allows multiple networks to exist on the same physical network to optimize the network for different traffic types.

Network slicing

Network slicing is a network architecture solution that:

- partitions a single physical network into multiple virtual slices
- allows each slice to operate with customized network functions and resources
- allocates dedicated resources for diverse service types or customer requirements.

5G network slicing is supported only on 5G standalone networks. It is not available on 5G non-standalone (NSA) networks. The network provider defines a specific set of network functions and resources for each slice or service type. Service type defines the expected behavior of a network slice, specifying its features and services.

The following service types are supported in network slicing:

- Enhanced Mobile Broadband (eMBB): used for high-bandwidth and low-latency applications.

- Ultra-reliable low latency communications (URLLC): used for highly reliable and low-latency transmission requirements.
- Massive Internet of Things (MIoT): used for sending small quantities of data.

Configure network slicing

Before you begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellular gateway in the **Device Solution** column.

For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Procedure

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

Step 2 Create a Configuration Group. A new configuration group is created.

Step 3 In the configuration group, click **Add Profile**.

Step 4 Choose **Transport & Management Profile** from the drop-down list.

Step 5 Click **Edit** to add features to the Transport and Management profile and click **Add New Feature**.

Step 6 Choose **Cellular Controller** from the **Add Feature** drop-down list.

Step 7 Choose **Cellular Profile** from the **Add Fetaure** drop-down list.

Table 26: Cellular Settings

Field	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.

Field	Description
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose a attach profile from the defined profiles.
Data Profile	Choose a data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

Step 8 For the configured **Cellular Controller**, choose the **Cellular Profile** or click **Add New** to add a new cellular profile.

Step 9 Configure **Cellular Profile** using the following table.

Table 27: Cellular Profile Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
Profile ID	Enter the identification number of the profile to use on the router. Range: 1 through 15
Access Point Name	Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be **none**, **pap**, **chap**, or **pap_chap**.
Profile Username	Enter the user name to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6.

Field	Description
No Overwrite	Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled.
Slice Type	Choose the network slice type (SST) for the profile. The options are: • eMBB: Enhanced Mobile Broadband, used for high data throughput. • URLLC: Ultra-Reliable Low Latency Communication, used for high reliability and low latency transmission. • MIoT: Massive IoT, used for many devices transmitting small quantities of data.
Slice Differentiator	Enter the slice differentiator (SD) for the profile. This is an optional value that enables the user equipment (UE) to use multiple slice instances of the same SST. Range: 0 through 16777214
Slot	Enter the associated SIM slot for the profile.

Configure network slicing using CLI

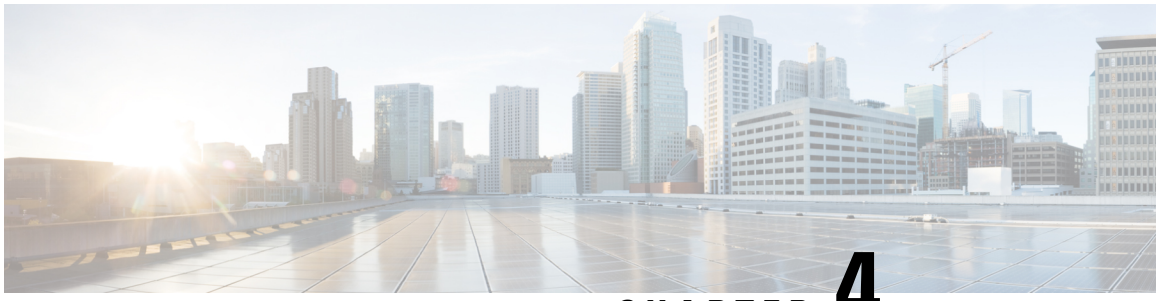
The following example shows how to configure a cellular network slicing using a CLI:

```
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4
   no-overwrite
   slot            Associated sim slot
   slice-type Associated network slice type(SST)

Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type
<1-3>  Slice type number: 1(eMBB), 2(URLLC), 3(MioT)
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type embb
  slice-differentiator Associated Slice Differentiator(SD)  <--- if SD is bypassed here,"FF
 FF FF" wll be used internally as the SD to indicate that there is no SD associated with
this SST.
   slot                           Associated sim slot

Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice
 type
embb slice-differentiator
  <0-16777214>  Slice Differentiator
Device(config-controller)#
Device(config-controller)#$ pdn ipv6  slice-type miot slice-differentiator 6
  slot  Associated sim slot
```

Verify network slicing using CLI

The following is a sample output from the **show cellular** command that displays network slicing configuration and slice type details:

```
Device# show cellular profile 6

Profile 6 = INACTIVE
--------
PDP Type = IPv6
Access Point Name (APN) = TestNSSAI6_URLLC1
Authentication = None
S-NSSAI Slice Type is URLLC
S-NSSAI Slice Differentiator = 1
```



CHAPTER 4

TLOC

TLOC

A TLOC (Transport Locator) is a unique identifier in Cisco Catalyst SD-WAN that

- represents a WAN Edge device's connection to a WAN transport, and
- is defined by the combination of its system IP address, a color indicating the type of transport, and an encapsulation type.

Components of TLOC

A TLOC is made up of three components:

- System IP address: The unique IP address of the SD-WAN device.
- Color: A Cisco Catalyst SD-WAN software construct that identifies the transport tunnel.
- Encapsulation: The method used to encapsulate the overlay tunnel data.

Tunnel interface

A tunnel interface in Cisco Catalyst SD-WAN is a network connection that you configure for secure data transport. On a Cisco SD-WAN Controller or Cisco SD-WAN Manager, you can configure one tunnel interface. On a Cisco IOS XE Catalyst SD-WAN device, you can configure up to eight tunnel interfaces.

To limit the remote TLOCs that the local TLOC can establish BFD sessions with, mark the TLOC with the **restrict** option. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.

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

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

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

STUN server

In Cisco Catalyst SD-WAN, Session Traversal Utilities for NAT (STUN) is a protocol used by Cisco IOS XE Catalyst SD-WAN devices to discover their public IP address and port assigned by a Network Address Translator (NAT).

Use the **allow-service stun** command to enable or disable a Cisco IOS XE Catalyst SD-WAN device from sending requests to a generic STUN server. This allows the device to determine if it is behind a NAT, identify the NAT type, and discover its public IP address and port number. On a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT, you can also configure a tunnel interface to obtain its public IP address and port number from the Cisco SD-WAN Validator.

When you configure the Cisco IOS XE Catalyst SD-WAN device to use the Cisco SD-WAN Validator as a STUN server, the device determines its public IP address and public port number, which enables it to establish TLOC connections and form the overlay fabric over various public transports like broadband or cellular networks. However, the device cannot identify the type of NAT it is behind in this setup. The tunnel interface configured for the Cisco SD-WAN Validator does not carry overlay network control traffic or exchange encryption keys, but BFD establishes connectivity and allows data traffic. Because this tunnel does not support control traffic, you must configure at least one additional tunnel interface to ensure the device can exchange control traffic with the Cisco SD-WAN Controller and Cisco SD-WAN Manager.

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

System IP address

A system interface IP address is a persistent address that

- identifies the Cisco IOS XE Catalyst SD-WAN device,
- is similar to a router ID on a regular router, and
- is used to identify the router from which packets originated.

System IP address configuration

You configure a system interface for each Cisco IOS XE Catalyst SD-WAN device using the **system system-ip** command. Specify the system IP address as an IPv4 address in decimal four-part dotted notation, without including the prefix length; the /32 prefix is implicit. The system IP address must not be within the following ranges: 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, or 240.0.0.0/4 and later. Assign a unique system IP address to each device in the overlay network. You cannot assign this address to another interface in VPN 0.

The system interface is placed in VPN 0 as a loopback interface named **system**. This loopback is not the same as a loopback address that you configure for a specific interface. To display information about the system interface, use the **show interface** command.

Role in OMP TLOC identification

The system IP address is used as one of the attributes of the OMP TLOC (Overlay Management Protocol Transport Locator). Each TLOC is uniquely identified by a 3-tuple: the system IP address, a color, and an encapsulation. Use the **show omp tlocs** command to display TLOC information.

Device management

For device management, configure the same system IP address on a loopback interface located in a service-side VPN appropriate for management purposes. Use a loopback interface because it remains reachable whenever the router is operational and the overlay network is up. Avoid configuring the system IP address on a physical interface, since both the router and the interface must be up for reachability in that case.

Assign the loopback interface to a service-side VPN, which is any VPN other than VPN 0 (the WAN transport VPN) or VPN 512 (the management VPN). Service-side VPNs are used to route data traffic and remain reachable from the data center.

Color

A color is a Cisco Catalyst SD-WAN software construct that

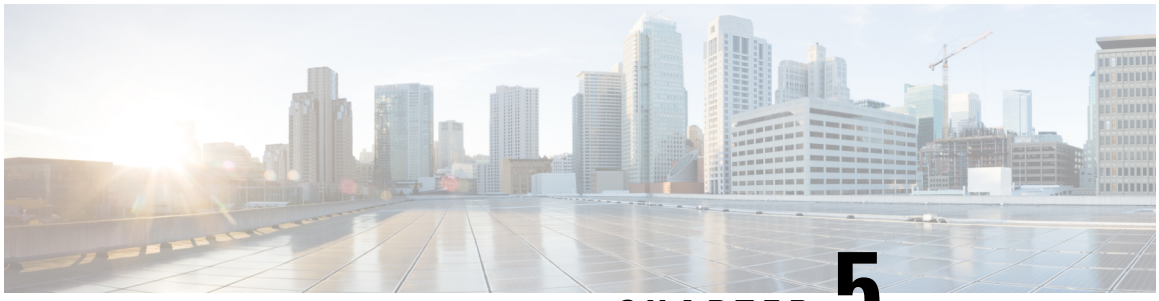
- identifies the transport tunnel,
- includes options such as **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**, and
- designates **metro-ethernet**, **mpls**, and **private1** through **private6** as private colors that use private addresses for private networks, which can be used on public networks only if there is no NAT device between the local and remote Cisco IOS XE Catalyst SD-WAN devices.

Encapsulation

An encapsulation is a required configuration on Cisco IOS XE Catalyst SD-WAN devices that

- specifies the tunnel encapsulation type as either IPsec or GRE, and
- sets the default MTU to 1442 bytes for IPsec and 1468 bytes for GRE, which is enabled by default on all TLOCs, based on BFD path MTU discovery.

You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE Catalyst SD-WAN device, you must configure the same tunnel encapsulation type or types so that the two routers can exchange data traffic. Data transmitted out of an IPsec tunnel can be received only by an IPsec tunnel, and data sent on a GRE tunnel can be received only by a GRE tunnel. The Cisco Catalyst SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE Catalyst SD-WAN device.



CHAPTER 5

TLOC Extension

Feature history for TLOC extension

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

Table 28: Feature History

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

TLOC extension

A TLOC Extension is a Cisco Catalyst SD-WAN feature that

- enables a device to access the opposite WAN transport connected to a neighboring device using a TLOC extension interface, and
- addresses scenarios where devices cannot connect directly to a single transport and only one device can connect to each transport.

Benefits of TLOC extension

There are scenarios when Cisco IOS XE Catalyst SD-WAN devices cannot connect to a single transport directly and only one device can connect to a single transport. A switch is connected to each transport and the devices connect to each transport through the switches. TLOC extension provides the following benefits:

- Eliminates the need for additional switches at branch locations.
- Reduces overall solution costs and simplifies network management.

TLOC extension over IPv6

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a TLOC extension over IPv6 works only if the underlay supports IPv6 addressing on both the Cisco IOS XE Catalyst SD-WAN devices connecting each other.

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

Supported configurations

This feature supports the following requirements:

- Implicit IPv6 ACL on TLOC tunnel interface.
- Private and public color TLOC interfaces.
- Dual stack support. When both IPv4 and IPv6 are configured, the tunnel is built on top of either IPv4 or IPv6, based on the configuration.
- NAT66 support. The limitations of NAT66 also applies to the TLOC extended interface.
- Only the Layer 2 setup supports IPv6 TLOC extension. The following interface types supports IPv6 TLOC extension:
  - Physical interface
  - Physical sub-interface
  - Loopback interface
- Loopback TLOC interface that is bound to either:
  - The WAN transport circuit.
  - An extended WAN interface between two Cisco IOS XE Catalyst SD-WAN devices.

Limitations for TLOC extension over IPv6

SIG

Secure Internet Gateway (SIG) is not supported on TLOC extension over IPv6.

NAT64

NAT64 is not supported for TLOC extension over IPv6.

Layer 3 Connectivity

TLOC extension over IPv6 is not supported for Layer 3 connections.

Control connection persistence

When a TLOC configuration is extended to a peer interface and then to the internet service provider, the extended control connections remain active on the peer interface even after the TLOC extension configuration is removed.

Extender interface configuration

In TLOC extension, the extender interface is part of the Cisco Catalyst SD-WAN. However, configuring a tunnel-interface under the extender interface is optional.

How TLOC extension over IPv6 works

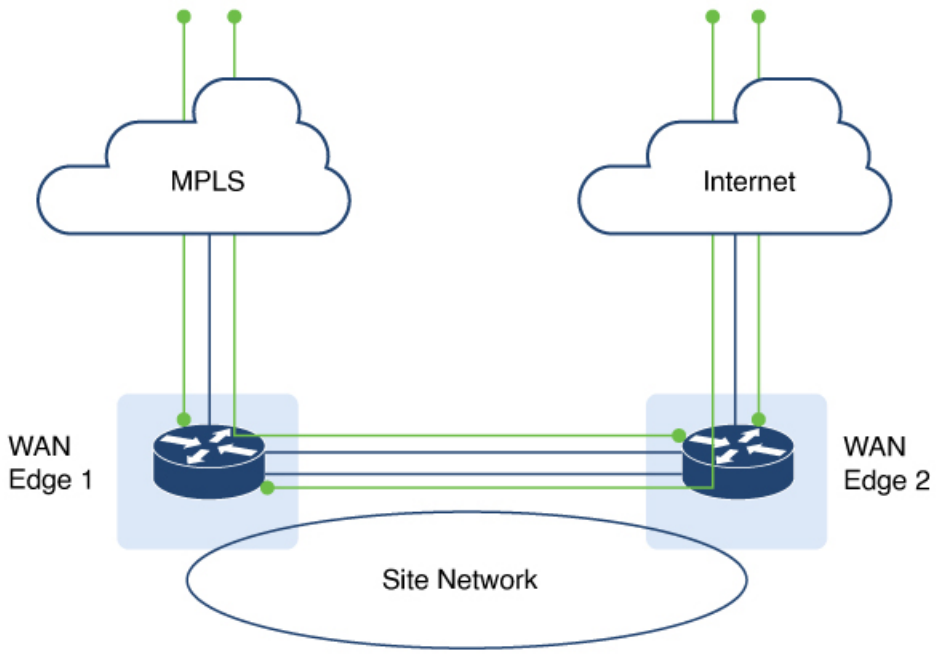
Summary

The key components involved in TLOC extension over IPv6 are:

- Establish TLOC extension interfaces: Each Cisco IOS XE Catalyst SD-WAN device configures a TLOC-extension interface to enable access to the transport network of its neighboring SD-WAN device.
- Access opposite transport via neighbor.

Workflow

Figure 1: TLOC extension



This process outlines how TLOC extension interfaces facilitate transport access and redundancy between two Cisco IOS XE Catalyst SD-WAN devices.

1. SD-WAN device 1 accesses the internet transport through the TLOC-extension interface on SD-WAN device 2, in addition to its direct MPLS connection.
2. SD-WAN device 2 accesses the MPLS transport through the TLOC-extension interface on SD-WAN device 1, in addition to its direct internet connection.

Result

TLOC extension over IPv6 achieves redundancy in a dual-device deployment scenario with only one circuit connection on each device.

Configure TLOC extension using CLI commands

Follow these steps to configure TLOC extension using CLI commands:

Procedure

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

Example:

```
Device# config-transaction
```

Step 2 Enter SD-WAN configuration mode.

Example:

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

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

Example:

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

Step 4 Configure tunnel interface.

Example:

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

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

Example:

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

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

Example:

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

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

Example:

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

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

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

```
On Device1,
Configure TLOC interface on VPN 0
sdwan
interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec
   color custom1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit

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

  ip route 0.0.0.0 0.0.0.0 10.1.19.16

 On Device2,
LTE WAN connection is on Gig1 and this transport is extended to ED1 Gig3 TLOC
interface(custom1).
 sdwan
 int GigabitEthernet3
 tloc-extension GigabitEthernet1
Configure NAT routes on Gig1 or appropriate routes for data traffic to reach back to ED1
via ED2 for Gig3 subnet.
```

Verify TLOC extension

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

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


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