



## **Systems and Interfaces Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12**

**First Published:** 2019-08-15

### **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

---

<b>CHAPTER 1</b>	<b>What's New for Cisco SD-WAN</b>	<b>1</b>
	What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r	<b>1</b>

---

<b>CHAPTER 2</b>	<b>System and Interfaces Overview</b>	<b>5</b>
	Basic Settings for Cisco vManage	<b>9</b>
	Configure Organization Name	<b>10</b>
	Configure Cisco vBond DNS Name or IP Address	<b>11</b>
	Configure Controller Certificate Authorization Settings	<b>11</b>
	Enforce Software Version on Devices	<b>13</b>
	Banner	<b>13</b>
	Create a Custom Banner	<b>14</b>
	Collect Device Statistics	<b>14</b>
	Configure or Cancel vManage Server Maintenance Window	<b>15</b>
	Configure Basic System Parameters	<b>15</b>
	Configure Global Parameters	<b>19</b>
	Create Global Settings Feature Template	<b>20</b>
	CLI Equivalent	<b>21</b>
	Configure NTP using Cisco vManage	<b>22</b>
	Configure NTP	<b>25</b>
	Configure Time using CLI	<b>25</b>
	Configure GPS Using Cisco vManage	<b>25</b>
	Configure System Logging Using CLI	<b>26</b>
	SSH Terminal	<b>27</b>
	Tenant Management	<b>27</b>

---

<b>CHAPTER 3</b>	<b>Configuring User Access and Authentication</b>	<b>31</b>
------------------	---	-----------

Manage Users using vManage	38
Configure User Using CLI	40
Manage a User Group	41
Creating Groups Using CLI	42
Configuring RADIUS Authentication Using CLI	42
Configure SSH Authentication	43
SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices	44
Configure SSH Authentication using CLI on Cisco IOS XE SD-WAN Devices	44
Configure the Authentication Order	44
Role-Based Access with AAA	46
Configuring AAA using vManage Template	55

**CHAPTER 4****Create a Device Template from Feature Templates 63**

Configure Devices	67
Create a Device CLI Template	67
Manage Device Templates	67
View Device Templates	68
Attach and Detach a Device Template	69
Change the Device Rollback Timer	71
Preview Device Configuration and View Configuration Differences	71
Change Variable Values for a Device	72
Configuring Devices using vManage	72
Change Configuration Modes	73
Upload WAN Edge Router Authorized Serial Number File	73
Upload WAN Edge Router Serial Numbers from Cisco Smart Account	74
Export Device Data in CSV Format	74
View and Copy Device Configuration	75
Delete a WAN Edge Router	76
View Template Log and Device Bringup	76
Add a Cisco vBond Orchestrator	76
Configure Cisco vSmart Controllers	77
Create a UCS-E Template	78

**CHAPTER 5****Configure Network Interfaces 83**

Configure VPN	84
VPN	84
Create a VPN Template	84
Changing the Scope for a Parameter Value	86
Configure Basic VPN Parameters	86
Configure DNS and Static Hostname Mapping	87
Configure Interfaces in the WAN Transport VPN (VPN 0)	88
Configure the System Interface	90
Configure Control Plane High Availability	90
Configure Other Interfaces	91
Role-Based Access Control by VPN	92
VPN Dashboard Overview	92
Configure and Manage VPN Segments	93
Configure and Manage VPN Groups	94
Configure User with User group	95
Configure Interface Properties	96
Set the Interface Speed	96
Set the Interface MTU	96
Monitoring Bandwidth on a Transport Circuit	97
Enable DHCP Server using Cisco vManage	98
Configuring PPPoE	101
Configure PPPoE from vManage Templates	101
Configuring VRRP	104
Configure VPN Ethernet Interface	105
Configure Basic Interface Functionality	106
Create a Tunnel Interface	107
Associate a Carrier Name with a Tunnel Interface	108
Limit Keepalive Traffic on a Tunnel Interface	109
Configure an Interface as a NAT Device	109
IPv4 NAT Parameter Values	110
Configure Static NAT	110
IPv6 NAT Parameter Values	111
IPv6 Support for NAT64 Devices	111
Apply Access Lists and QoS Parameters	111

- Add ARP Table Entries 112
- Configuring VRRP 112
- Configure Advanced Properties 113
- VPN Interface Bridge 115
  - Create a Bridging Interface 116
  - Apply Access Lists 117
  - Configure VRRP 117
  - Add ARP Table Entries 118
  - Configure Advanced Properties 119
- VPN Interface DSL IPoE 120
- VPN Interface DSL PPPoA 128
- VPN Interface DSL PPPoE 136
- VPN Interface Ethernet PPPoE 145
- VPN Interface IPsec 152
  - Create VPN IPsec Interface Template 152
  - Basic Configuration 153
  - Configure Dead-Peer Detection 154
  - Configure IKE 154
  - Configure IPsec Tunnel Parameters 158
- VPN Interface Multilink 159
- Configure VPN Interface SVI using vManage 166
- VPN Interface T1/E1 170
  - T1/E1 Controller 173
- Cellular Interfaces 177
  - Configure Cellular Interfaces Using vManage 177
  - Configure Cellular Interfaces Using CLI 185
  - Low-bandwidth Link Optimization 185
- WiFi Radio 189
- WiFi SSID 191

---

**CHAPTER 6 IPv6 Functionality 195**

---

**CHAPTER 7 IP Directed Broadcast 207**

---

**CHAPTER 8**

**CLI Templates for Cisco XE SD-WAN Routers 209**







# CHAPTER 1

## What's New for Cisco SD-WAN



**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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, on page 1](#)

## 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
<b>Getting Started</b>	
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 <a href="#">Cross-Site Request Forgery Prevention</a> .
<b>Systems and Interfaces</b>	

Feature	Description
IPv6 Support for NAT64 Devices	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices. See <a href="#">IPv6 Support for NAT64 Devices</a> .
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 <a href="#">Configure SSH Authentication</a> .
DHCP option support	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. See <a href="#">Configure DHCP</a> .
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 <a href="#">Create a UCS-E Template</a> .
<b>Bridging, Routing, Segmentation, and QoS</b>	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. See <a href="#">QoS on Subinterface</a> .
<b>Policies</b>	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See <a href="#">Configure and Monitor Packet Duplication</a> .
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 <a href="#">Configure Localized Data Policy for IPv4 Using Cisco vManage</a> .
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 <a href="#">Integration with Cisco ACI</a> .
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 <a href="#">Encryption of Lawful Intercept Messages</a> .
<b>Security</b>	
High-Speed Logging for Zone-Based Firewalls	This feature allows a firewall to log records with minimum impact to packet processing. See <a href="#">Firewall High-Speed Logging</a> .
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See <i>Apply Policy to a Zone Pair</i> in <a href="#">Use the Policy Configuration Wizard</a> .

Feature	Description
Secure Communication Using Pairwise IPsec Keys	This feature allows private pairwise IPsec session keys to be created and installed for secure communication between IPsec devices and its peers. See <a href="#">IPsec Pairwise Keys Overview</a> .
<b>Network Optimization and High Availability</b>	
TCP Optimization	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput. See <a href="#">TCP Optimization: Cisco XE SD-WAN Routers</a> .
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 <a href="#">Share VNF Devices Across Service Chains</a> .
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 <a href="#">Monitor Service Chain Health</a> .
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 <a href="#">Manage PNF Devices in Service Chains</a> .
<b>Devices</b>	
Cisco 1101 Series Integrated Services Routers	Cisco SD-WAN capability can now be enabled on Cisco 1101 Series Integrated Services Routers.
<b>Commands</b>	
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 <a href="#">bind</a> command.





## CHAPTER 2

# System and Interfaces Overview

Setting up the basic system-wide functionality of network devices is a simple and straightforward process. These basic parameters include defining host properties, such as name and IP address; setting time properties, including NTP; setting up user access to the devices; defining system log (syslog) parameters; .

In addition, the Cisco SD-WAN software provides a number of management interfaces for accessing the Cisco SD-WAN devices in the overlay network.

### Host Properties

All devices have basic system-wide properties that specify information that the Cisco SD-WAN software uses to construct a view of the network topology. Each device has a system IP address, which provides a fixed location of the device in the overlay network. This address, whose function is similar to that of a router ID on a router, is independent of any of the interfaces and interface IP addresses on the device. The system IP address is one of the four components of each device's TLOC property.

A second host property that must be set on all devices is the IP address of the vBond orchestrator for the network domain, or a DNS name that resolves to one or more IP addresses for vBond orchestrators. The vBond orchestrator automatically orchestrates the bringup of the overlay network, admitting a new device into the overlay and providing the introductions that allow device and vSmart controllers to locate each other.

Two other system-wide host properties are required on all devices, except for the vBond orchestrators, to allow the Cisco SD-WAN software to construct a view of the topology: the domain identifier and the site identifier.

To configure the host properties, see *Cisco SD-WAN Overlay Network Bringup* .

### Time and NTP

The Cisco SD-WAN software implements the Network Time Protocol (NTP) to synchronize and coordinate time distribution across the Cisco SD-WAN overlay network. NTP uses a intersection algorithm to select applicable time servers and avoid issues caused due to network latency. The servers also can redistribute reference time using local routing algorithms and time daemons. NTP is defined in RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification* .

### User Authentication and Access with AAA, RADIUS, and TACACS+

The Cisco SD-WAN software uses Authentication, Authorization, and Accounting (AAA) to provide security for devices on the network. AAA, in combination with RADIUS and TACACS+ user authentication, controls which users are allowed access to devices and what operations they are authorized to perform once they are logged in or connected to the devices.

Authentication refers to the process by which the user trying to access the device is authenticated. To access devices, users log in with name and a password. The local device can authenticate users, or authentication can be performed by a remote device, either by a Remote Authentication Dial-In User Service (RADIUS) server or by a Terminal Access Controller Access-Control System (TACACS+), or by both in sequence.

Authorization determines whether the user is authorized to perform a given activity on the device. In the Cisco SD-WAN software, authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. External groups are also considered when performing authorization; that is, the Cisco SD-WAN software retrieves group names from RADIUS or TACACS+ servers. Each group is assigned privileges that authorize the group members to perform specific functions on the device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.

The Cisco SD-WAN software does not implement AAA accounting.

For more information, see *Role-Based Access with AAA*.

### Authentication for WANs and WLANs

For wired networks (WANs), Cisco SD-WAN devices can run IEEE 802.1X software to prevent unauthorized network devices from gaining access to the WAN. IEEE 802.1X is a port-based network access control (PNAC) protocol that uses a client-server mechanism to provide authentication for devices wishing to connect to the network.

IEEE 802.1X authentication requires three components:

- **Supplicant**—Client device, such as a laptop, that requests access to the WAN. In the Cisco SD-WAN overlay network, a supplicant is any service-side device that is running 802.1X-compliant software. These devices send network access requests to the router.
- **Authenticator**— A network device that provides a barrier to the WAN. In the overlay network, you can configure an interface device to act as an 802.1X authenticator. The device supports both controlled and uncontrolled ports. For controlled ports, the Cisco SD-WAN device acts as an 802.1X port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. For uncontrolled ports, the Cisco SD-WAN, acting as an 802.1X PAE, transmits and receives Extensible Authentication Protocol over IEEE 802 (EAP over LAN, or EAPOL) frames.
- **Authentication server**—Host running authentication software that validates and authenticates supplicants that want to connect to the WAN. In the overlay network, this host is an external RADIUS server. This RADIUS server authenticates each client connected to the 802.1X port interface Cisco SD-WAN router and assigns the interface to a VLAN before the client is allowed to access any of the services offered by the router or by the LAN.

For wireless LANs (WLANs), routers can run IEEE 802.11i prevents unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN. WPA authenticates individual users on the WLAN using a username and password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2-compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done either using preshared keys or through RADIUS authentication.

## Network Segmentation

The Layer 3 network segmentation in Cisco SD-WAN is achieved through VRFs on Cisco IOS XE SD-WANs. When you configure the Network Segmentation on Cisco IOS XE SD-WAN device using Cisco vManage the system automatically maps the VPN configurations to VRF configurations.

## Network Interfaces

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

The overlay network has the following types of VPNs/VRFs:



**Note** Cisco IOS XE SD-WAN devices use VRFs in place of VPNs. When you complete the configuration, on Cisco vManage the system automatically maps the VPN configurations to VRF configurations.

- **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. This is the global VRF on Cisco IOS XE SD-WAN software.
- **VPN 512—Management VPN**, which carries out-of-band network management traffic among the Cisco 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 SD-WAN devices. For controller devices, by default, VPN 512 is not configured. On Cisco IOS XE SD-WAN devices the management VPN is converted to VRF Mgmt-Intf.

For each network interface, you can configure a number of interface-specific properties, such as DHCP clients and servers, VRRP, interface MTU and speed, and PPPoE. At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

## Management and Monitoring Options

There are various ways you can manage and monitor a router. Management interfaces provide access to devices in Cisco SD-WAN overlay network, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

The following management interfaces are available:

- Command-line interface (CLI)
- IP Flow Information Export (IPFIX)
- RESTful API
- SNMP
- System logging (syslog) messages
- vManage web server

## CLI

You can access a command-line interface (CLI) on each device, and from the CLI you configure overlay network features on the local device and gather operational status and information regarding that device. While a CLI is available, it is strongly recommended that you configure and monitor all Cisco SD-WAN network devices from a Cisco vManage web server, which provides visual views of network-wide operations and device status, including drill-downs that display details operation and status data. In addition, the vManage web server provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

You access the CLI by establishing an SSH session to a Cisco SD-WAN device.

For a Cisco SD-WAN device that is being managed by a vManage NMS, if you create or modify the configuration from the CLI, those changes are overwritten by the configuration that is stored in the vManage configuration database.

## IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for monitoring the traffic flowing through Cisco SD-WAN routers in the overlay network and exporting information about the traffic to a flow collector. The exported information is sent in template reports, which contain both information about the flow and data extracted from the IP headers of the packets in the flow.

The Cisco SD-WAN cflowd performs 1:1 traffic sampling. Information about all flows is aggregated in the cflowd records; flows are not sampled. Cisco SD-WAN routers do not cache any of the records that are exported to a collector.

The Cisco SD-WAN cflowd software implements cflowd version 10, as specified in RFC 7011 and RFC 7012.

For a list of elements exported by IPFIX, see [Traffic Flow Monitoring with cflowd](#).

To enable the collection of traffic flow information, you create data policies that identify the traffic of interest and then direct that traffic to a cflowd collector. For more information, see [Traffic Flow Monitoring with Cflowd](#).

You can also enable cflowd visibility directly on Cisco SD-WAN routers without configuring data policy so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. You then monitor the traffic from the vManage GUI or from the router's CLI.

## RESTful API

The Cisco SD-WAN software provides a RESTful API, which is a programmatic interface for controlling, configuring, and monitoring the Cisco SD-WAN devices in an overlay network. You access the RESTful API through the vManage web server.

The Cisco SD-WAN RESTful API calls expose the functionality of Cisco SD-WAN software and hardware features and of the normal operations you perform to maintain the devices and the overlay network itself.

## SNMP

The Simple Network Management Protocol (SNMP) allows you to manage all Cisco SD-WAN devices in the overlay network. The Cisco SD-WAN software supports SNMP v2c.

You can configure basic SNMP properties—device name, location, contact, and community—that allow the device to be monitored by an SNMP NMS.

You can configure trap groups and SNMP servers to receive traps.



The object identifier (OID) for the Internet port of the SNMP MIB is 1.3.6.1.

SNMP traps are asynchronous notifications that a Cisco SD-WAN device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the Cisco SD-WAN device. By default, SNMP traps are not sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

### Syslog Messages

System logging operations use a mechanism similar to the UNIX syslog command to record system-wide, high-level operations that occur on the Cisco SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as those in standard UNIX commands, and you can configure which priority of syslog messages are logged. Messages can be logged to files on the Cisco SD-WAN device or to a remote host.

### vManage NMS

The vManage NMS is a centralized network management system that allows configuration and management of all Cisco SD-WAN devices in the overlay network and provides a dashboard into the operations of the entire network and of individual devices in the network. Each vManage NMS runs on a web server in the network. Three or more vManage web servers are consolidated into a vManage cluster to provide scalability and management support for up to 6,000 Cisco SD-WAN devices, to distribute vManage functions across multiple devices, and to provide redundancy of network management operations.

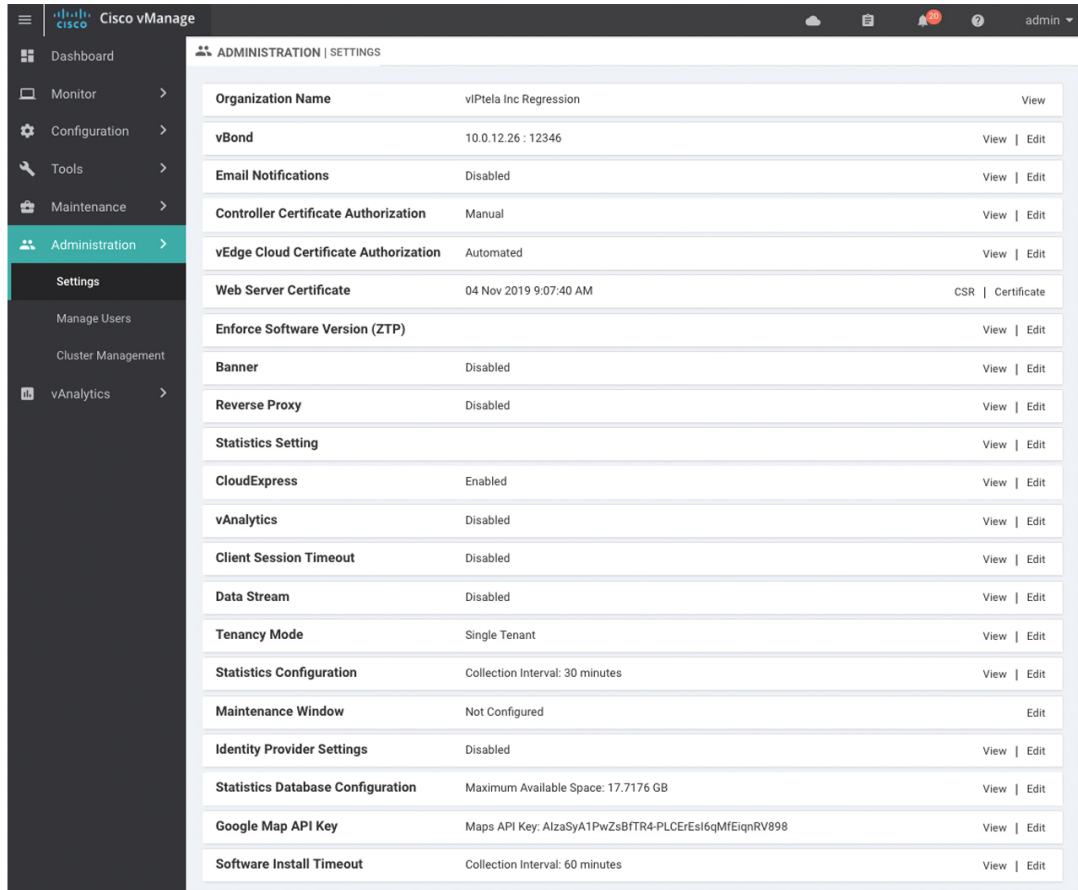
- [Basic Settings for Cisco vManage, on page 9](#)
- [Configure Basic System Parameters, on page 15](#)
- [Configure Global Parameters, on page 19](#)
- [Configure NTP using Cisco vManage, on page 22](#)
- [Configure NTP, on page 25](#)
- [Configure Time using CLI, on page 25](#)
- [Configure GPS Using Cisco vManage, on page 25](#)
- [Configure System Logging Using CLI, on page 26](#)
- [SSH Terminal, on page 27](#)
- [Tenant Management, on page 27](#)

## Basic Settings for Cisco vManage

The System template is used to configure system-level Cisco vManage workflows.

Use the Settings screen to view the current settings and configure the setting for Cisco vManage parameters, including the organization name, vBond orchestrator's DNS name or IP address, certificate settings, and statistics collection.

The current setting for each item is displayed in the bar for each item, immediately following the name.



Setting	Value	Actions
Organization Name	vIPtela Inc Regression	View
vBond	10.0.12.26 : 12346	View   Edit
Email Notifications	Disabled	View   Edit
Controller Certificate Authorization	Manual	View   Edit
vEdge Cloud Certificate Authorization	Automated	View   Edit
Web Server Certificate	04 Nov 2019 9:07:40 AM	CSR   Certificate
Enforce Software Version (ZTP)		View   Edit
Banner	Disabled	View   Edit
Reverse Proxy	Disabled	View   Edit
Statistics Setting		View   Edit
CloudExpress	Enabled	View   Edit
vAnalytics	Disabled	View   Edit
Client Session Timeout	Disabled	View   Edit
Data Stream	Disabled	View   Edit
Tenancy Mode	Single Tenant	View   Edit
Statistics Configuration	Collection Interval: 30 minutes	View   Edit
Maintenance Window	Not Configured	Edit
Identity Provider Settings	Disabled	View   Edit
Statistics Database Configuration	Maximum Available Space: 17.7176 GB	View   Edit
Google Map API Key	Maps API Key: AlzaSyA1PwZsBFTR4-PLCEResl6qMfEiqnRV898	View   Edit
Software Install Timeout	Collection Interval: 60 minutes	View   Edit

368729

## Configure Organization Name

Before you can generate a Certificate Signing Request (CSR), you must configure the name of your organization. The organization name is included in the CSR.

In public key infrastructure (PKI) systems, a CSR is sent to a certificate authority to apply for a digital identity certificate.

To configure the organization name:

1. Click the **Edit** button to the right of the **Organization Name** bar.
2. In the **Organization Name** field, enter the name of your organization. The organization name must be identical to the name that is configured on the vBond orchestrator.
3. In the **Confirm Organization Name** field, re-enter and confirm your organization name.
4. Click **Save**.

Note that once the control connections are up and running, the organization name bar is no longer editable.

## Configure Cisco vBond DNS Name or IP Address

1. Click the **Edit** button to the right of the vBond bar.
2. In the vBond **DNS/IP Address: Port** field, enter the DNS name that points to the vBond orchestrator or the IP address of the Cisco vBond orchestrator and the port number to use to connect to it.
3. Click **Save**.

## Configure Controller Certificate Authorization Settings

Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the Cisco vManage that you generate these certificates and install them on the controller devices—Cisco vBond orchestrators, Cisco vManage, and Cisco vSmart controllers. You can use certificates signed by Symantec, or you can use enterprise root certificates.

The controller certification authorization settings establish how the certification generation for all controller devices will be done. They do not generate the certificates.

You need to select the certificate-generation method only once. The method you select is automatically used each time you add a device to the overlay network.

To have the Symantec signing server automatically generate, sign, and install certificates on each controller device:

1. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Symantec Automated** (Recommended). This is the recommended method for handling controller signed certificates.
3. In the **Confirm Certificate Authorization Change** popup, click **Proceed** to confirm that you wish to have the Symantec signing server automatically generate, sign, and install certificates on each controller device.
4. Enter the first and last name of the requestor of the certificate.
5. Enter the email address of the requestor of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requestor via email; they are also made available through the customer portal.
6. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
8. Confirm your challenge phrase.
9. In the Certificate **Retrieve Interval** field, specify how often the Cisco vManage server checks if the Symantec signing server has sent the certificate.
10. Click **Save**.

To manually install certificates that the Symantec signing server has generated and signed:

1. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Symantec Manual**.

3. In the **Confirm Certificate Authorization Change** popup, click **Proceed** to manually install certificates that the Symantec signing server has generated and signed.
4. Click **Save**.

To use enterprise root certificates:

1. Click the **Edit** button to the right of the **Controller Certificate Authorization** bar.
2. Click **Enterprise Root Certificate**.
3. In the **Confirm Certificate Authorization Change** popup, click **Proceed** to confirm that you wish to use enterprise root certificates.
4. In the **Certificate** box, either paste the certificate, or click **Select a file** and upload a file that contains the enterprise root certificate.
5. By default, the enterprise root certificate has the following properties: To view this information, issue the **show certificate signing-request decoded** command on a controller device, and check the output in the Subject line. For example:
  - Country: United States
  - State: California
  - City: San Jose
  - Organizational unit: ENB
  - Organization: CISCO
  - Domain Name: cisco.com
  - Email: cisco-cloudops-sdwan@cisco.com

```
vSmart# show certificate signing-request decoded
...
Subject: C=US, ST=California, L=San Jose, OU=ENB, O=CISCO, CN=vsmart-uuid
.cisco.com/emailAddress=cisco-cloudops-sdwan@cisco.com
...
```

To change one or more of the default CSR properties:

- a. Click **Set CSR Properties**.
  - b. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).
  - c. Enter the organizational unit (OU) to include in the CSR.
  - d. Enter the organization (O) to include in the CSR.
  - e. Enter the city (L), state (ST), and two-letter country code (C) to include in the CSR.
  - f. Enter the email address (emailAddress) of the certificate requestor.
  - g. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
6. Click **Import & Save**.

## Enforce Software Version on Devices

If you are using the Cisco SD-WAN hosted service, you can enforce a version of the Cisco SD-WAN software to run on a router when it first joins the overlay network. To do so:

1. Ensure that the software image for the desired device software version is present in the vManage software image repository:
  - a. In Cisco vManage, select the **Maintenance > Software Repository** screen.  
The Software Repository screen opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.
  - b. If you need to add a software image, click **Add New Software**.
  - c. Select the location from which to download the software images, either Cisco vManage, Remote Server, or Remote Server - vManage.
  - d. Select an x86-based or a MIPS-based software image.
  - e. Click **Add** to play the image in the repository.
2. In the **Administration > Settings** screen, click the **Edit** button to the right of the Enforce Software Version (ZTP) bar.
3. In the **Enforce Software Version** field, click **Enabled**.
4. From the **Version** drop-down, select the version of the software to enforce on the device when they join the network.
5. Click **Save**.

If you enable this feature on the Cisco vManage, any device joining the network is configured with the version of the software specified in the **Enforce Software Version** field regardless of whether the device was running a higher or lower version of Cisco SD-WAN software.

## Banner

Use the Banner template for Cisco vBond Orchestrators, Cisco vManages, Cisco vSmart Controllers, s, and Cisco IOS XE SD-WAN devices.

- To configure the banner text for login screens using Cisco vManage templates, create a Banner feature template to configure PIM parameters, as described in this topic.
- To configure a login banner for the Cisco vManage system, go to **Administration > Settings**.

### Configure a Banner

1. In Cisco vManage, select the **Configuration > Templates** screen.
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. Click the **Additional Templates** tab located directly beneath the Description field, or scroll to the **Additional Templates** section.
6. From the **Banner** drop-down, click **Create Template**. The **Banner** template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Banner parameters.
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.

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.

9. To set a banner, configure the following parameters:

**Table 2: Parameters to be configured while setting a banner:**

Parameter Name	Description
MOTD Banner	On a Cisco IOS XE SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type <code>\n</code> .
Login Banner	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type <code>\n</code> .

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

*CLI equivalent:*

```
banner{login login-string | motd motd-string}
```

## Create a Custom Banner

To create a custom banner that is displayed after you log in to the Cisco vManage:

1. Click the **Edit** button to the right of the Banner bar.
2. In the **Enable Banner** field, click **Enabled**.
3. In the **Banner Info** text box, enter the text string for the login banner or click **Select a File** to download a file that contains the text string.
4. Click **Save**.

## Collect Device Statistics

To enable or disable the collection of statistics for devices in the overlay network:

1. Click the **Edit** button to the right of the **Statistics Settings** bar. By default, all statistics collection settings are enabled for all Cisco SD-WAN devices.
2. To set statistics collection parameters for all devices in the network, click **Disable All** for the parameter you wish to disable statistics collection for. To return to the saved settings during an edit operation, click **Reset**. To return the saved settings to the factory-default settings, click **Restore Factory Default**.
3. To set statistics collection parameters for individual devices in the network, click **Custom** to select devices on which to enable or disable statistics collection. The **Select Devices** popup screen opens listing the hostname and device IP of all devices in the network. Select one or more devices from the **Enabled Devices** column on the left and click the arrow pointing right to move the device to the **Disabled Devices** column on the right. To move devices from the **Disabled Devices** to the **Enabled Devices** column, select one or more devices and click the arrow pointing left. To select all devices in the **Select Devices** popup screen, click the **Select All** checkbox in either window. Click **Done** when all selections are made.
4. Click **Save**.

## Configure or Cancel vManage Server Maintenance Window

You can set or cancel the start and end times and the duration of the maintenance window for the vManage server.

1. In vManage NMS, select the **Administration > Settings** screen.
2. Click the **Edit** button to the right of the Maintenance Window bar.  
To cancel the maintenance window, click **Cancel**.
3. Click the **Start date and time** drop-down, and select the date and time when the maintenance window will start.
4. Click the **End date and time** drop-down, and select the date and time when the maintenance window will end.
5. Click **Save**. The start and end times and the duration of the maintenance window are displayed in the Maintenance Window bar.

Two days before the start of the window, the vManage Dashboard displays a maintenance window alert notification.

## Configure Basic System Parameters

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

To configure system-wide parameters using vManage templates:

1. Create a **System** feature template to configure system parameters.
2. Create an **NTP** feature template to configure NTP servers and authentication.
3. Configure the organization name and Cisco vBond Orchestrator IP address on the vManage NMS. These settings are appended to the device templates when the templates are pushed to devices.

### Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the **Configuration ► Templates** screen.
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 System, select the **Factory\_Default\_System\_Template** and click **Create Template**. The System template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining System parameters.
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 3:**

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>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.</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Basic System-Wide Configuration

To set up system-wide functionality on a Cisco SD-WAN device, select the **Basic Configuration** tab and then configure the following parameters. Parameters marked with an asterisk are required.



Table 4:

Parameter Field	Description
Site ID* (on routers, vManage NMSs, and vSmart controllers)	Enter the identifier of the site in the Cisco SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco SD-WAN devices that reside in the same site. <i>Range:</i> 1 through 4294967295 ( $2^{32} - 1$ )
System IP*	Enter the system IP address for the Cisco SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.
Timezone*	Select the timezone to use on the device.
Hostname	Enter a name for the Cisco SD-WAN device. It can be up to 32 characters.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Device Groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Controller Groups	List the vSmart controller groups to which the router belongs.
Description	Enter any additional descriptive information about the device.
Console Baud Rate	Select the baud rate of the console connection on the router. <i>Values:</i> 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps) <i>Default:</i> 115200 bps
Maximum OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a vSmart controller. <i>Range:</i> 0 through 100 <i>Default:</i> 2

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

To configure the DNS name or IP address of the vBond orchestrator in your overlay network, go to the **Administration > Settings** screen and click **vBond**.

### Configure Interface Trackers

To track the status of transport interfaces that connect to the internet, click the **Tracker** tab. Then click **Add New Tracker** and configure the following parameters:

Table 5:

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. <i>Range:</i> 100 through 1000 milliseconds <i>Default:</i> 300 milliseconds

Parameter Field	Description
Interval	How often probes are sent to determine the status of the transport interface. <i>Range:</i> 10 through 600 seconds <i>Default:</i> 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. <i>Range:</i> 1 through 10 <i>Default:</i> 3
End Point Type: IP Address	IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address.
End Point Type: DNS Name	DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address.

To save a tracker, click **Add**.

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

To apply a tracker to an interface, configure it in the VPN Interface Cellular, VPN Interface Ethernet, VPN Interface NAT Pool, or VPN Interface PPP configuration templates. You can apply only one tracker to an interface.

### Configure Advanced Options

To configure additional system parameters, click the **Advanced** tab:

**Table 6:**

Parameter Name	Description
Control Session Policer Rate	Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic. <i>Range:</i> 1 through 65535 pps <i>Default:</i> 300 pps
Port Hopping	Click <b>On</b> to enable port hopping, or click <b>Off</b> to disable it. When a Cisco SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. <i>Default:</i> Enabled (on routers); disabled (on vManage NMSs and vSmart controllers)
Port Offset	Enter a number by which to offset the base port number. Configure this option when multiple Cisco SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. <i>Values:</i> 0 through 19
Track Transport	Click <b>On</b> to regularly check whether the DTLS connection between the device and a vBond orchestrator is up. Click <b>Off</b> to disable checking. By default, transport checking is enabled

Parameter Name	Description
Track Interface	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. <i>Range:</i> 1 through 4294967295
Gateway Tracking	Click <b>On</b> to enable or click Off to Disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. <i>Default:</i> Enabled
Collect Admin Tech on Reboot	Click <b>On</b> to collect admin-tech information when the device reboots.
Idle Timeout	Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. <i>Range:</i> 0 through 300 seconds <i>Default:</i> CLI session does not time out

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

*CLI equivalent:*

```

system
  admin-tech-on-failure allow-same-site-tunnels
  control-session-pps rate eco-friendly-mode
  host-policer-pps rate

  icmp-error-pps rate

  idle-timeout seconds multicast-buffer-percent percentage

  port-hop port-offset number
  system-tunnel-mtu bytes timer
  dns-cache-timeout minutes track-default-gateway
  track-interface-tag number

  track-transport upgrade-confirm minutes

```

## Configure Global Parameters

Use the Global Settings template to configure global parameters for all Cisco SD-WAN devices.

To configure global settings using vManage:

1. Create a feature template to configure global settings.
2. Create a device template and include the Global Settings feature template.
3. (Recommended) Before applying the device template to a device, use the View Configuration Differences feature to review the differences between the configuration currently on the device and the configuration to be sent to the device (overwriting its existing configuration).

### Limitations

SD-WAN can apply the global settings feature template only to devices running Cisco IOS XE Gibraltar 17.2 or later.

## Create Global Settings Feature Template

1. In vManage, select **Configuration** (gear icon) ► **Templates**.
2. Click the **Feature** tab.
3. Click **Add Template**.
4. In the left pane, select a device type.
5. In the right pane, select the **Global Settings** template.
6. Provide a name and description for the template.
7. For each of the parameters, use the default or set custom values as desired.

Parameter	Description
<b>Services</b>	
HTTP Server	Enable/disable HTTP server.
HTTPS Server	Enable/disable secure HTTPS server.
Passive FTP	Enable/disable passive FTP.
IP Domain-Lookup	Enable/disable domain name server (DNS) lookup.
Arp Proxy	Enable/disable proxy ARP.
RSH/RCP	Enable/disable remote shell (RSH) and remote copy (RCP) on the device.
Telnet (Outbound)	Enable/disable outbound telnet.
CDP	Enable/disable Cisco Discovery Protocol (CDP).
<b>Other Settings</b>	
TCP Keepalives (In)	Enable/disable generating keepalives on idle incoming network connections.
TCP Keepalives (Out)	Enable/disable generating keepalives on idle outgoing network connections.
TCP Small Servers	Enable/disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable/disable small UDP servers (for example, ECHO).
Console Logging	Enable/disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable/disable the originator of a packet to determine which path to use to get to the destination.

Parameter	Description
VTY Line Logging	Enable/disable the device to display log messages to a VTY session in real time.
SNMP IFINDEX Persist	Enable/disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable/disable BOOTP server. This enables the device to listen for the bootp packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.
<b>NAT 64</b>	
UDP Timeout	NAT64 translation timeout for UDP Range: 1 to 65536 (seconds)
TCP Timeout	NAT64 translation timeout for TCP Range: 1 to 65536 (seconds)
<b>HTTP Authentication</b>	
HTTP Authentication	HTTP authentication mode Possible values: Local, AAA

8. Enter a name for the template and click **Save**.

## CLI Equivalent

Services:

```
[no] ip http server
[no] ip http secure-server
[no] ip ftp passive
[no] ip domain lookup
[no] ip arp proxy disable
[no] ip rcmd rsh-enable
[no] ip rcmd rcp-enable
(Telnet outbound enable) line vty 0 4, transport input telnet ssh
(Telnet outbound disable) line vty 0 4, transport input ssh
[no] cdp run enable
```

Other settings:

```
[no] service tcp-keepalives-in
[no] service tcp-keepalives-out
[no] service tcp-small-servers
[no] service udp-small-server
[no] logging console
[no] ip source-route
[no] logging monitor
[no] snmp-server ifindex persist
[no] ip bootp server
```

NAT 64:

```

nat64 translation timeout udp timeout
nat64 translation timeout tcp timeout

```

HTTP Authentication:

```
ip http authentication {local | aaa}
```

## Configure NTP using Cisco vManage

Configure network time protocol (NTP) servers on your devices in order to synchronize time across all devices in the Cisco Overlay Network. You can configure up to four NTP servers, and they must all be located or reachable in the same VPN.

Other devices are allowed to ask a Cisco SD-WAN device for the time, but no devices are allowed to use the Cisco SD-WAN device as an NTP server.

To configure NTP using Cisco vManage templates:

1. Create an NTP feature template to configure NTP parameters, as described in this article.
2. Configure the timezone in the System template.

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the **Configuration** > **Templates** screen.
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. Select the **Basic Information** tab.
6. Under **Additional System Templates**, located to the right of the screen, click **NTP**.
7. From the **NTP** drop-down, click **Create Template**. The NTP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining NTP parameters.
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 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 7:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Configure NTP Servers

To configure NTP servers, select the Server tab and click **Add New Server**. Then configure the following parameters. Parameters marked with an asterisk are required to configure NTP.

Table 8:

Parameter Name	Description
Hostname/IP Address*	Enter the IP address of an NTP server or of a DNS server that knows how to reach the NTP server.
Authentication Key*	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the Trusted Keys field, under the Authentication tab (discussed below).
VPN ID*	Enter the number of the VPN to use to reach the NTP server or the VPN in which the NTP server is located. If you configure multiple NTP servers, they must all be located or reachable in the same VPN.  <i>Range: 0 through 65530</i>
Version*	Enter the version number of the NTP protocol software. <i>Range: 1 through 4</i> <i>Default: 4</i>
Source Interface	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.

Parameter Name	Description
Prefer	Click On if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one with the highest stratum level.

To add the NTP server, click **Add**.

To add another NTP server, click **Add New Server**. You can configure up to four NTP servers. The Cisco SD-WAN software uses the server at the highest stratum level.

To edit an NTP server, click the pencil icon to the right of the entry.

To delete an NTP server, click the trash icon to the right of the entry.

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

### Configure NTP Authentication

To configure authentication keys used to authenticate NTP servers, in the **Authentication** tab, click the **Authentication Key** tab. Then click Add New Authentication Key, and configure the following parameters. Parameters marked with an asterisk are required to configure NTP.

**Table 9:**

Parameter Name	Description
Authentication Key*	Select the following values: <ul style="list-style-type: none"> <li>• Authentication Key—Enter an MD5 key ID. It can be a number from 1 through 65535.</li> <li>• Authentication Value—Enter either a cleartext key or an AES-encrypted key.</li> </ul>
Authentication Value*	Enter an MD5 authentication key. For the key to be used, you must designate it as trusted. To associate a key with a server, enter the same value as you use for the the Authentication Key field on the Server tab.

To configure trusted keys used to authenticate NTP servers, in the Authentication tab, click the **Trusted Keys** tab and configure the following parameters;

**Table 10:**

Parameter Name	Description
Trusted Keys*	Enter the MD5 authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value as you use for the the Authentication Key field on the Server tab.



# Configure NTP

## Configure Network-Wide Time with NTP

To coordinate and synchronize time across all devices in the Cisco SD-WAN overlay network, configure the IP address or DNS server address of an NTP server on each device.

```
config-terminal
 ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

# Configure Time using CLI

You can set the time locally on your without using NTP if you do not need to ensure that time is synchronized across an entire network of devices. You can also set the time locally on any device as it is joining the network, in addition to configuring an NTP server. The local time gets overwritten by the official NTP time once the device contacts the NTP server.

```
clock set 12:00:00 31 May 2019
```

# Configure GPS Using Cisco vManage

Use the GPS template for all Cisco cellular routers running Cisco SD-WAN software.

For Cisco devices running Cisco SD-WAN software, you can configure the GPS and National Marine Electronics Association (NMEA) streaming. You enable both these features to allow 4G LTE routers to obtain GPS coordinates.

## Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the **Configuration > Templates** screen.
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. Select the **Cellular** tab.
6. In **Additional Cellular Controller Templates**, click **GPS**.
7. To create a custom template for GPS, click the **GPS** drop-down and then click **Create Template**. The GPS template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining GPS parameters.
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 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 either **Device Specific** or **Global**.

### Configure GPS

To configure GPS parameters for the cellular router, configure the following parameters. Parameters marked with an asterisk are required to configure the GPS feature.

**Table 11:**

Parameter Name	Description
GPS	Click <b>On</b> to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: <ul style="list-style-type: none"> <li>• MS-based—Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor.</li> <li>• Standalone—Use satellite information when determining position.</li> </ul>
NMEA	Click <b>On</b> to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE NIM to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.
Source Address	Enter the IP address of the interface that connects to the router's NIM.
Destination Address	Enter the IP address of the marine NMEA server.
Destination Port	Enter the number of the port to use to send NMEA data to the server.

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

### Release Information

Introduced in Cisco vManage Release 18.1.1.

## Configure System Logging Using CLI

Use the following command to configure system logging on Cisco SDWAN.

```
config-transaction [IP address | description | alarm | buffered | buginf | console |
discriminator
esm | event | facility | file | history | host | origin-id | persistent | rate-limit |
snmp-authfail | snmp-trap | source-interface
trap | userinfo]
```

## SSH Terminal

Use the SSH Terminal screen to establish an SSH session to a Cisco vEdge device. From an SSH session, you can issue CLI commands on a Cisco vEdge device.

### Establish an SSH Session to a Device

To establish an SSH session to a device:

1. From the left pane, select the device on which to collect statistics:
  - a. Select the device group to which the device belongs.
  - b. If needed, sort the device list by its status, hostname, system IP, site ID, or device type.
  - c. Click on the device to select it.
2. Enter the username and password to log in to the device.

You can now issue CLI commands to monitor or configure the device.

## Tenant Management

Use the Tenant Management screen to add tenants to a Cisco vManage server that is operating in multitenant mode.

### Add a Tenant

1. In the left pane, click the **Add Tenant** button.
2. In the **Add Tenant** window:
  - a. Enter a name for the tenant. It can be up to 128 characters and can contain only alphanumeric characters.
  - b. Enter a description for the tenant. It can be up to 256 characters and can contain only alphanumeric characters.
  - c. Enter the name of the organization. The name is case-sensitive. It is the name in the certificates for all Cisco SD-WAN network devices, and it must be identical on all devices in the overlay network.
  - d. In the URL subdomain field, enter the domain name for the tenant. The domain name must include the provider's domain name. You must also configure this same domain name when you enable multitenancy mode, in **vManage Administration > Settings > Tenancy Mode**
  - e. Click **Save**.
3. The Create Tenant screen is displayed, and the Status column shows In progress. To view status messages related to the creation of the tenant, click the > to the left of the status column. After about 1 minute, the Status column changes to Success, and the tenant table shows the tenant's system IP address.

### View All Tenants

To view a summary of information about all tenants, in the center of the top bar, click the provider name.

### View a Single Tenant

To view a summary of information about a single tenant:

1. In the center of the top bar, click the provider name.
2. In the table of tenants, click the tenant name. The summary information displays to the right of the name.
3. To hide the summary information, click the tenant name a second time.

To view the Cisco vManage dashboard for a single tenant:

1. In the center of the top bar, click **Select Tenant** to the right of the provider name.
2. Select the tenant name from the drop-down.

### Edit a Tenant

1. In the left pane, click the name of the tenant.
2. In the right pane, click the Pencil icon to the right of the tenant's name.
3. In the **Edit Tenant** popup, modify the tenant's name, description, or domain name.
4. Click **Save**.

### Remove a Tenant

1. In the left pane, click the name of the tenant.

2. In the right pane, click the **Trash** icon to the right of the tenant's name.
3. In the **Delete Tenant** popup, enter your Cisco vManage password and click **Save**.





## CHAPTER 3

# Configuring User Access and Authentication

This article describes how to use AAA in combination with RADIUS and TACACS+ to configure authentication, authorization, and accounting for users wishing to access Cisco vEdge devices.

### Configuring AAA

AAA allows you to configure local users on the Cisco vEdge device. AAA configuration is done in two steps:

- Configure users—First, you configure usernames and passwords for individuals who are allowed to access the Cisco vEdge device. The Cisco SD-WAN software provides one standard username, **admin**, and you can also create custom usernames, as needed.
- Configure groups—Second, you place users in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. See Role-Based Access for AAA for more information about user and group privileges and the authorization that they provide.

### Creating Users

The Cisco SD-WAN software provides one standard username, **admin**. Only a user who is logged in as the admin user is permitted to create additional users.

To create a user account, configure the username and password, and place the user into a group:

```
Viptela(config)# system aaaViptela(config)# user  
username  
password  
passwordViptela(config-aaa)# group  
group-name
```

*username* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (\_), and periods (.). The name cannot contain any uppercase letters. Some usernames are reserved, so you cannot configure them. For a list of them, see the **aaa** configuration command.

*password* is the password for the user. Each username must have a password, and each user is allowed to change their own password. The CLI immediately encrypts the string and never displays a readable version of the password. When a user is logging in to the Cisco vEdge device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and they must wait 15 minutes before attempting to log in again.

*group-name* is the name of one of the standard Cisco SD-WAN groups (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an **admin** user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

The factory-default password for the **admin** username is **admin**. It is strongly recommended that you modify this password the first time you configure a Cisco vEdge device.

```
Viptela(config)# system aaa admin password
password
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and never displays a readable version of the password. For example:

```
vEdge(config-user-admin)# show config
system
aaa
  user admin
    password $1$xULc8yYH$k71cTjvKESmeIGgImNDaC.
  !
  user eve
    password $1$8z3q4qoU$F6DMBr9vPBF0s/s145ax5.
    group basic
  !
!
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to use to verify the password:

```
Viptela(config)# system aaa radius-servers
tag
```

*tag* is a string that you defined with the **radius server tag** command, as described below.

### Creating Groups

The Cisco SD-WAN software provides three fixed group names: **basic**, **netadmin**, and **operator**. The username **admin** is automatically placed in the **netadmin** usergroup.

To create a custom group with specific authorization, configure the group name and privileges:

```
Viptela(config)# system
aaa usergroup group-name
task
privilege
```

*group-name* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (\_), and periods (.). The name cannot contain any uppercase letters. Some group names are reserved, so you cannot configure them. For a list of them, see the **aaa** configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).



In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

In the following example, the **basic** user group has full access to the **system** and **interface** portions of the configuration and operational commands, and the **operator** user group can use all operational commands but can make no modifications to the configuration:

```
vEdge# show running-config system aaa
system
aaa
  usergroup basic
    task system read write
    task interface read write
  !
  usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
  !
  user admin
    password $1$tokPB7tf$VchR2JI9Sw1/dqgkq9S.
  !
!
```

### Configuring RADIUS Authentication

To have a Cisco vEdge device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
Viptela(config)# system radiusViptela(config-radius)# server
ip-addressViptela(config-server)# secret-key
passwordViptela(config-server)# priority
numberViptela(config-server)# auth-port
port-numberViptela(config-server)# acct-port
port-numberViptela(config-server)# source-interface
interface-nameViptela(config-server)# tag
tagViptela(config-server)# vpn
vpn-id
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Cisco vEdge device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections. To change these port numbers, use the **auth-port** and **acct-port** commands.

If the RADIUS server is reachable via a specific interface, configure that interface with the **source-interface** command.

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long.

Then associate the tag with the **radius-servers** command when you configure AAA, and when you configure interfaces for 802.1X and 802.11i.

If the RADIUS server is located in a different VPN from the Cisco vEdge device, configure the server's VPN number so that the Cisco vEdge device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When a Cisco vEdge device is trying to locate a RADIUS server, it goes through the list of servers three times. To change this, use the **retransmit** command, setting the number to a value from 1 to 1000:

```
Viptela(config-radius)# retransmit
number
```

When waiting for a reply from the RADIUS server, a Cisco vEdge device waits 3 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Viptela(config-radius)# timeout
seconds
```

### Configuring TACACS+ Authentication

To have a Cisco vEdge device use TACACS+ servers for user authentication, configure one or up to 8 servers:

```
Viptela(config)# system tacacs Viptela(config)# server
ip-addressViptela(config-server)# secret-key
passwordViptela(config-server)# priority
numberViptela(config-server)# auth-port
port-numberViptela(config-server)# source-interface
interface-nameViptela(config-server)# vpn
vpn-id
```

For each TACACS+ server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear-text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the TACACS+ server. The password must match the one used on the server. To configure more than one TACACS+ server, include the **server** and **secret-key** commands for each server.

The remaining TACACS+ configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Cisco vEdge device uses port 49 to connect to the TACACS+ server. To change this, use the **auth-port** command.

If the TACACS+ server is reachable via a specific interface, configure that interface with the **source-interface** command.

If the TACACS+ server is located in a different VPN from the Cisco vEdge device, configure the server's VPN number so that the Cisco vEdge device can locate it. If you configure multiple TACACS+ servers, they must all be in the same VPN.

By default, PAP is used as the authentication type for the password for all TACACS+ servers. You can change the authentication type to ASCII:

```
Viptela(config-tacacs)# authentication ascii
```

When waiting for a reply from the TACACS+ server, a Cisco vEdge device waits 5 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Viptela(config-tacacs) # timeout
seconds
```

### Configuring the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Cisco vEdge device through an SSH session or a console port. The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the **system radius server** command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco vEdge device is denied.

To modify the default order, use the **auth-order** command:

```
Viptela(config-system-aaa) # auth-order (local | radius | tacacs)
```

Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

To have the "admin" user use the authentication order configured in the **auth-order** command, use the following command:

```
Viptela(config-system-aaa) # admin-auth-order
```

If you do not include this command, the "admin" user is always authenticated locally.

You can configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user, either because the user has entered invalid credentials or because the authentication server is unreachable (or all the servers are unreachable):

```
Viptela(config-system-aaa) # auth-fallback
```

Fallback to a secondary or tertiary authentication mechanism happens when the higher-priority authentication server fails to authenticate a user, either because the credentials provided by the user are invalid or because the server is unreachable.

The following examples illustrate the default authentication behavior and the behavior when authentication fallback is enabled:

- If the authentication order is configured as **radius local**:
  - With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
  - With authentication fallback enabled, local authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access to a user.
- If the authentication order is configured as **local radius**:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
  - With authentication fallback enabled, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device. In this case, the behavior of two authentication methods is identical.
- If the authentication order is configured as **radius tacacs local**:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.
  - With authentication fallback enabled, TACACS+ authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access a user. Local authentication is used next, when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.

If a remote server validates authentication but does not specify a user group, the user is placed into the user group **basic**.

If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user **basic**, with a home directory of /home/basic.

If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of /home/username (so, /home/eve).

### Configuring NAS Attributes

For RADIUS and TACACS+, you can configure Network Access Server (NAS) attributes for user authentication and authorization. To do this, you create a vendor-specific attributes (VSA) file, also called a RADIUS dictionary or a TACACS+ dictionary, on the RADIUS or TACACS+ server that contains the desired permit and deny commands for each user. The Cisco vEdge device retrieves this information from the RADIUS or TACACS+ server.

The VSA file must be named dictionary.Cisco SD-WAN, and it must contain text in the following format:

```
localhost$ more dictionary.viptela
# -*- text -*-
#
# dictionary.viptela
```

```
#
#
# Version:      $Id$
#
VENDOR          Viptela                      41916
BEGIN-VENDOR    Viptela
ATTRIBUTE       Viptela-Group-Name          1    string
```

The Cisco SD-WAN software has three predefined user groups, as described above: **basic**, **netadmin**, and **operator**. These groups have the following permissions:

```
Viptela# show aaa usergroup
GROUP    USERS  TASK          PERMISSION
-----
basic    -      system        read
          interface    read
netadmin admin  system        read write
          interface    read write
          policy       read write
          routing     read write
          security    read write
operator -      system        read
          interface    read
          policy       read
          routing     read
          security    read
```

To create new user groups, use this command:

```
Viptela(config)# system aaa usergroup
group-name task privilege
```

Here is a sample user configuration on a RADIUS server, which for FreeRADIUS would be in the file "users":

```
user1  Cleartext-password := "user123"
        Service-Type = NAS-Prompt-User,
        Viptela-Group-Name = operator,

user1  Cleartext-password := "user123"           Service-Type = NAS-Prompt-User,
Viptela-Group-Name = operator,
```

Then in the dictionary on the RADIUS server, add a pointer to the VSA file:

```
$INCLUDE /usr/share/freeradius/dictionary.viptela
```

For TACACS+, here is a sample configuration, which would be in the file tac\_plus.conf:

```
group = test_group {
    default service = permit
    service = ppp protocol = ip {
        Viptela-Group-Name = operator
    }
}

user = user1 {
    pap = cleartext "user123"
    member = test_group
}
```

- [Manage Users using vManage, on page 38](#)
- [Configure User Using CLI, on page 40](#)
- [Manage a User Group, on page 41](#)
- [Creating Groups Using CLI, on page 42](#)

- [Configuring RADIUS Authentication Using CLI, on page 42](#)
- [Configure SSH Authentication, on page 43](#)
- [Configure the Authentication Order, on page 44](#)
- [Role-Based Access with AAA, on page 46](#)
- [Configuring AAA using vManage Template, on page 55](#)

## Manage Users using vManage

Use the Manage Users screen to add, edit, or delete users and user groups from the vManage NMS.

Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from the vManage NMS.

### Add a User

To perform operations on a device, you configure usernames and passwords for users who are allowed to access the device. The Cisco SD-WAN software provides one standard username, **admin**, and you can create custom usernames, as needed. We recommend that you configure strong passwords for users.

To add a user:

1. In the Users tab, click Add User.
2. In the Add User popup window, enter the full name, username, and password for the user. Note that uppercase characters are not allowed in usernames.
3. From the User Groups drop-down list, select the groups that the user will be a member of.
4. Click Add. The user is then listed in the user table.

### Delete a User

If a user no longer needs access to devices, you can delete the user. When you delete a user, that user no longer has access to the device. Deleting a user does not force log out the user if the user is logged in.

To delete a user:

1. In the Users tab, select the user you wish to delete.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the user.

### Edit User Details

Editing user details lets you update login information for a user, and add or remove a user from a user group. If you edit details for a user who is logged in, the changes take effect after the user logs out.

To edit user details:

1. In the Users tab, select the user whose details you wish to edit.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit login details, and add or remove the user from user groups.
4. Click Update.

### Change User Password

You can update passwords for users as needed. We recommend that you use strong passwords.

To change a password for a user:

1. In the Users tab, select the user whose password you wish to change.
2. Click the More Actions icon to the right of the column and click Change Password.
3. Enter, and then confirm, the new password. Note that the user, if logged in, is logged out.
4. Click Done.

## Configure User Using CLI

You can use the CLI to configure user credentials on each edge device. In this way, you can create additional users to give them access specific devices. The credentials that you create for a user by using the CLI can be different than the vManage credentials for the user, and you can create different credentials for a user on each device. Any Cisco IOS XE SD-WAN device user with the `netadmin` privilege can create a new user.

To create a user account, configure the username and password, and place the user into a group:

```
Device(config)# aaa authentication login user1 group basic
Device(config)# aaa authentication login user2 group operator
Device(config)# aaa authentication login user3 group netadmin
```

*username* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (\_), and periods (.). The name cannot contain any uppercase letters. Some usernames are reserved, so you cannot configure them. For a list of them, see the `aaa` configuration command.

*password* is the password for the user. Each username must have a password, and each user is allowed to change their own password. The CLI immediately encrypts the string and never displays a readable version of the password. When a user is logging in to the Cisco IOS XE SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and they must wait 15 minutes before attempting to log in again.

*group-name* is the name of one of the standard Cisco SD-WAN groups (**basic**, **netadmin**, or **operator**) or of a group configured with the `usergroup` command (discussed below). If an **admin** user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

The factory-default password for the **admin** username is **admin**. It is strongly recommended that you modify this password the first time you configure a Cisco IOS XE SD-WAN device.

```
Device(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeK1Wrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and never displays a readable version of the password. For example:

```
Device(config)# show run
...
aaa authentication login default local
aaa authentication login user1 group basic
aaa authentication login user2 group operator
aaa authentication login user3 group netadmin
aaa authorization exec default local
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to use to verify the password:

```
Device(config)# radius server tag
```

*tag* is a string that you defined with the `radius server tag` command, as described below.



# Manage a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. The Cisco SD-WAN software provides three standard user groups, and you can create custom user groups, as needed:

- **basic**—Includes users who have permission to view interface and system information.
- **netadmin**—Includes the admin user, by default, who can perform all operations on the vManage NMS. You can add other users to this group.
- **operator**—Includes users who have permission only to view information.

To add a user group:

1. In the User Groups tab, click Add User Group.
2. In the Add User Group popup window, enter the user group name and select the desired read and write permissions for each feature. Note that uppercase characters are not allowed in user group names.
3. Click OK. The user group is then listed in the left pane.

Each user group can have read or write permission for the features listed below. Write permission includes read permission.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed in the vManage Dashboard screen.

## Delete a User Group

You can delete a user group when it is no longer needed. For example, you might delete a user group that you created for a specific project when that project ends.

1. In the User Groups tab, click the name of the user group you wish to delete. Note that you cannot delete any of the three standard user groups—basic, netadmin, and operator.
2. Click the Trash icon.
3. Click OK to confirm deletion of the user group.

## Edit User Group Privileges

You can edit group privileges for an existing user group. This procedure lets you change configured feature read and write permissions for the user group needed.

1. In the User Groups tab, select the name of the user group whose privileges you wish to edit. Note that you cannot edit privileges for the three standard user groups—basic, netadmin, and operator.
2. Click the Edit button located directly above the privilege level table, and edit privileges as needed.
3. Click Save.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

## Creating Groups Using CLI

The Cisco SD-WAN software provides three fixed group names: **basic**, **netadmin**, and **operator**. The username **admin** is automatically placed in the **netadmin** usergroup.

If needed, you can create additional custom groups and configure privilege roles that the group members have. To create a custom group with specific authorization, configure the group name and privileges:

```
Device(config)# aaa authentication login user1 group radius enable
Device(config)# aaa authentication login user2 group radius enable
Device(config)# aaa authentication login user3 group radius enable
Device(config)#
```

*group-name* can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (\_), and periods (.). The name cannot contain any uppercase letters. Some group names are reserved, so you cannot configure them. For a list of them, see the `aaa` configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Cisco SD-WAN-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

## Configuring RADIUS Authentication Using CLI

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

To have a Cisco IOS XE SD-WAN device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
Deviceconfig-transaction
Device(config)# radius server test address ipv4 10.1.1.55 acct-port 110
Device(config-radius-server)# key 33
Device(config-radius-server)# exit
Device(config)# radius server test address ipv4 10.1.1.55 auth-port 330
Device(config-radius-server)# key 55
Device(config-radius-server)#
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Cisco IOS XE SD-WAN device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections. To change these port numbers, use the **auth-port** and **acct-port** commands.

If the RADIUS server is reachable via a specific interface, configure that interface with the **source-interface** command.

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1X, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long. Then associate the tag with the **radius-servers** command when you configure AAA, and when you configure interfaces for 802.1X and 802.11i.

If the RADIUS server is located in a different VPN from the Cisco IOS XE SD-WAN device, configure the server's VPN number so that the Cisco IOS XE SD-WAN device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When waiting for a reply from the RADIUS server, a Cisco IOS XE SD-WAN device waits 3 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Device# config-transaction
Device(config)# aaa group server radius server-10.99.144.201
Device(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit
3
```

## Configure SSH Authentication

*Table 12: Feature History*

Feature Name	Release Information	Description
Secure Shell Authentication Using RSA Keys	Cisco IOS XE SD-WAN Release 16.12.1b	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server.

The Secure Shell (SSH) protocol provides secure remote access connection to network devices.

SSH supports user authentication using public and private keys. To enable SSH authentication, public keys of the users are stored in the home directory of authenticating user in the following location:

```
~<user>/.ssh/authorized_keys
```

A new key is generated on the client machine which owns the private-key. Any message encrypted using the public key of the SSH server is decrypted using the private key of the client.

### Restrictions for SSH Authentication on Cisco SD-WAN

- The range of SSH RSA key size supported by Cisco IOS XE SD-WAN devices is from 2048 to 4096. SSH RSA key size of 1024 and 8192 are not supported.
- A maximum of two keys per user are allowed on Cisco IOS XE SD-WAN devices.

## SSH Authentication using vManage on Cisco IOS XE SD-WAN Devices

1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Feature** tab, click **Create Template**.
3. From the **Device Model** check box, select the type of device for which you are creating the template.
4. From the **Basic Information** tab, choose **AAA-CISCO** template.
5. From the Local tab, New User section, enter the SSH RSA Key. You must enter the complete public key from the `id_rsa.pub` file in the SSH RSA Key text box.

## Configure SSH Authentication using CLI on Cisco IOS XE SD-WAN Devices

SSH key based login is supported on IOS. Per user a maximum of 2 keys can be supported. Also, IOS only supports RSA based keys.

Traditional IOS CLI, allow support for:

- Key-string
- Key-hash – The key-string is base64 decoded and MD5 hash is run on it.

However, the transaction yang model has provision to only copy the key-hash (instead of the entire key-string). vManage does this conversion and pushes the configuration to the device.

### Public Keys supported on Cisco IOS XE SD-WAN Devices

- SSH-RSA

## Configure the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE SD-WAN device through an SSH session or a console port. The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running configuration on the local device.
- If local authentication fails, and if you have not configured authentication fallback (with the **auth-fallback** command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the **system radius server** command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the **system tacacs server** command. If a TACACS+ server is reachable, the user is

authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.

- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Cisco IOS XE SD-WAN device is denied.

Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

If you do not include this command, the "admin" user is always authenticated locally.

Fallback to a secondary or tertiary authentication mechanism happens when the higher-priority authentication server fails to authenticate a user, either because the credentials provided by the user are invalid or because the server is unreachable.

The following examples illustrate the default authentication behavior and the behavior when authentication fallback is enabled:

- If the authentication order is configured as **radius local**:
  - With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
  - With authentication fallback enabled, local authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access to a user.
- If the authentication order is configured as **local radius**:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
  - With authentication fallback enabled, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device. In this case, the behavior of two authentication methods is identical.
- If the authentication order is configured as **radius tacacs local**:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.
  - With authentication fallback enabled, TACACS+ authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access a user. Local authentication is used next, when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.

If a remote server validates authentication but does not specify a user group, the user is placed into the user group **basic**.

If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user **basic**, with a home directory of /home/basic.

If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of /home/username (so, /home/eve).

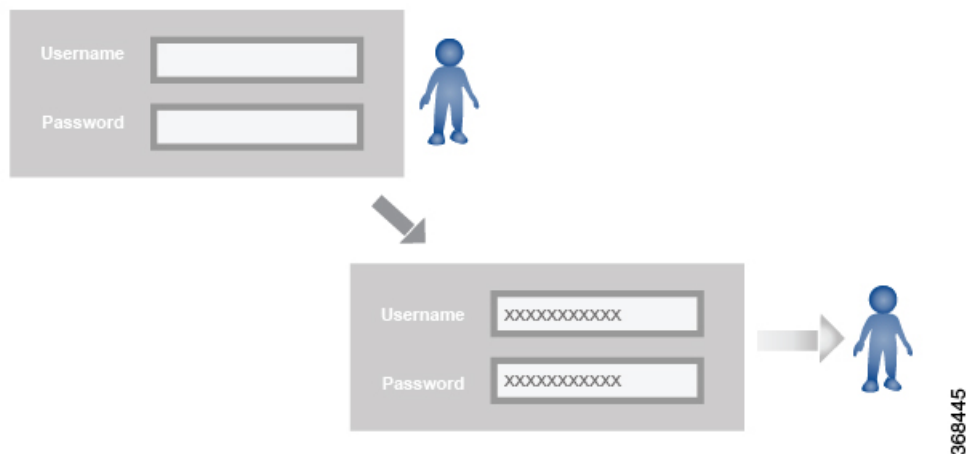
## Role-Based Access with AAA

The Cisco SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE SD-WAN devices. Role-based access consists of three components:

- Users are those who are allowed to log in to a Cisco IOS XE SD-WAN device.
- User groups are collections of users.
- Privileges are associated with each group. They define the commands that the group's users are authorized to issue.

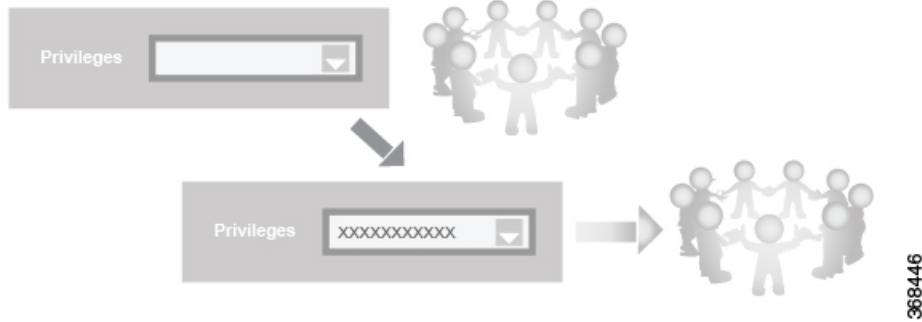
### Users and User Groups

All users who are permitted to perform operations on a Cisco IOS XE SD-WAN device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.

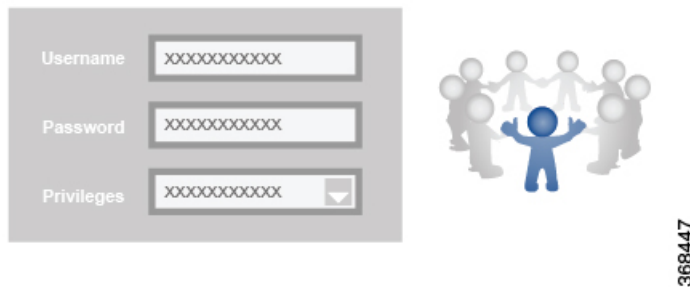


The Cisco SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the **admin** user, because this user is automatically in the user group **netadmin** and is permitted to perform all operations on the Cisco IOS XE SD-WAN device.



The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco SD-WAN software elements.



The Cisco SD-WAN software provides three standard user groups. The two groups **basic** and **operator** are configurable. While you can use these two groups for any users and privilege levels, the **basic** group is designed to include users who have permission to both view and modify information on the device, while the **operator** group is designed to include users who have permission only to view information. The third group is **net admin**, which is non-configurable. By default, it includes the **admin** user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.



**Note** Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

**Privileges for Role-Based Access**

Role-based access privileges are arranged into five categories, which are called *tasks*:

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.

- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

The tables in the following sections detail the AAA authorization rules for users and user groups. These authorization rules apply to commands issued from the CLI and to those issued from Netconf.

### User Authorization Rules for Operational Commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE SD-WAN device can execute most operational commands. However, only the **admin** user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user self password password** command and then committing that configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

The following tables lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

CLI Command	Any User	Admin User
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X (users in netadmin group only)
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X



CLI Command	Any User	Admin User
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X
request (everything else)	—	X
rollback (configuration mode command)	—	X (users in netadmin group only)
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user <i>self</i> password <i>password</i> (configuration mode command) (Note: A user cannot delete themselves)		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X

CLI Command	Any User	Admin User
tools nping	X	X
tracert	X	X
vshell	X	X (users in netadmin group only)

### User Group Authorization Rules for Operational Commands

The following table lists the user group authorization roles for operational commands.

Operational Command	Interface	Policy	Routing	Security	System
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			

Operational Command	Interface	Policy	Routing	Security	System
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	

Operational Command	Interface	Policy	Routing	Security	System
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X

Operational Command	Interface	Policy	Routing	Security	System
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X

Operational Command	Interface	Policy	Routing	Security	System
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

### User Group Authorization Rules for Configuration Commands

The following table lists the user group authorization rules for configuration commands.

Configuration Command	Interface	Policy	Routing	Security	System
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
omp		X	X		X
policy		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn (everything else, including creating, deleting, and naming)					X
wlan	X				

# Configuring AAA using vManage Template

Configuring AAA by using the vManage template lets you make configuration setting in vManage and then push the configuration to selected devices of the same type. This procedure is a convenient way to configure several of the same type of devices at one time.

Use the AAA template for Cisco vBond Orchestrators, vManage NMSs, Cisco vSmart Controllers, and Cisco IOS XE SD-WAN devices.

Cisco IOS XE SD-WAN devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.



---

**Note** You must configure a local user with a secret key via the template if you are using PPP or using MLPPP with CHAP.

---

## Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the **Configuration** ► **Templates** screen.
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. Select the **Basic Information** tab.
6. To create a custom template for AAA, select the Factory\_Default\_AAA\_Template and click Create Template. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
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.

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 13:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 IOS XE SD-WAN device to a device template .</p> <p>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 IOS XE SD-WAN device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Configure Authentication Order and Fallback

You can configure the authentication order and authentication fallback for device. The authentication order specifies the order in which the system attempts to authenticate user, and provides a way to proceed with authentication if the current authentication method is unavailable. Fallback provides a mechanism for authentication if the user cannot be authenticated or if a RADIUS or TACACS+ server is unreachable.

To configure AAA authentication order and authentication fallback on a Cisco IOS XE SD-WAN device, select the Authentication tab and configure the following parameters:

Table 14:

Parameter Name	Description
Authentication Order	<p>The default order is local, then radius, and then tacacs.</p> <p>To change the default order of authentication methods that the software tries when verifying user access to a Cisco IOS XE SD-WAN device:</p> <ol style="list-style-type: none"> <li>1. Click the dropdown arrow to display the list of authentication methods.</li> <li>2. In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method.</li> </ol> <p>If you select only one authentication method, it must be <b>local</b>.</p>



Parameter Name	Description
Authentication Fallback	Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable.
Admin Authentication Order	Have the "admin" user use the authentication order configured in the Authentication Order parameter. If you do not configure the admin authentication order, the "admin" user is always authenticated locally.
Disable Netconf Logs	Click On to disable the logging of Netconf events. By default, these events are logged to the auth.info and messages log files.
Disable Audit Logs	Click On to disable the logging of AAA events. By default, these events are logged to the auth.info and messages log files.
RADIUS Server List	List the tags for one or two RADIUS servers. Separate the tags with commas. You set the tag under the RADIUS tab.

*CLI equivalent:*

### Configure Local Access for Users and User Groups

You can configure local access to a device for users and user groups. Local access provides access to a device if RADIUS or TACACS+ authentication fails.

To configure local access for individual users, select the Local tab. To add a new user, select the User tab, click Add New User, and configure the following parameters:

**Table 15:**

Parameter Name	Description
Name	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.  The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, <i>The YANG 1.1 Data Modeling Language</i> .  Each username must have a password. Users are allowed to change their own passwords.  The default password for the admin user is admin. We strongly recommended that you change this password.
Description	Enter a description for the user.

Parameter Name	Description
User Groups	Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group.

Click Add to add the new user. Click Add New User again to add additional users.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To make this configuration, select the Local tab, select the User Group tab, click Add New User Group, and configure the following parameters:

**Table 16:**

Parameter Name	Description
Name	Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The Cisco SD-WAN software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group. The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved.
Feature	The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for Read, Write, and None to assign privileges to the group for each role.

Click Add to add the new user group.

To add another user group, click Add New User Group again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

*CLI equivalent:*

### Configure RADIUS Authentication

Configure RADIUS authentication if you are using RADIUS in your deployment.

To configure RADIUS authentication, select the RADIUS tab and configure the following parameters:

Table 17:

Parameter Name	Description
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server. <i>Range: 1 through 1000Default: 3</i>
Timeout	Specify how long to wait to receive a reply form the RADIUS server before retransmitting a request. <i>Range: 1 through 1000Default: 5 seconds</i>

To configure a connection to a RADIUS server, select the RADIUS tab, click Add New Radius Server, and configure the following parameters:

Table 18:

Parameter Name	Description
Address	Enter the IP address of the RADIUS server host.
Tag	Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1X, and IEEE 802.11i to use a specific RADIUS server or servers. For Cisco IOS XE SD-WAN devices running Cisco SD-WAN software, this field is ignored.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. <i>Default: Port 1812</i>
Accounting Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. <i>Range: 0 through 65535Default: 1813</i>
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Cisco IOS XE SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
Source Interface	Enter the name of the interface on the local device to use to reach the RADIUS server.
VPN ID	Enter the number of the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN.
Priority	Enter the priority of a RADIUS server. A server with a lower number is given priority. <i>Range: 0 through 7Default: 0</i>

Click Add to add the new RADIUS server.

To add another RADIUS server, click Add New RADIUS Server again.

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

### Configure TACACS+ Authentication

Configure TACACS+ authentication if you are using TACACS+ in your deployment.

To configure the device to use TACACS+ authentication, select the TACACS tab and configure the following parameters:

**Table 19:**

Parameter Name	Description
Timeout	Enter how long to wait to receive a reply from the TACACS+ server before retransmitting a request. <i>Range: 1 through 1000Default: 5 seconds</i>
Authentication	Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII.

To configure a connection to a TACACS+ server, select the TACACS tab, click Add New TACSCS Server, and configure the following parameters:

**Table 20:**

Parameter Name	Description
Address	Enter the IP address of the TACACS+ server host.
Authentication Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. <i>Default: Port 49</i>
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Cisco IOS XE SD-WAN device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.
Source Interface	Enter the name of the interface on the local device to use to reach the TACACS+ server.
VPN ID	VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN.
Priority	Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number. <i>Range: 0 through 7Default: 0</i>

Click Add to add the new TACACS server.

To add another TACACS server, click Add New TACACS Server again.

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*





# CHAPTER 4

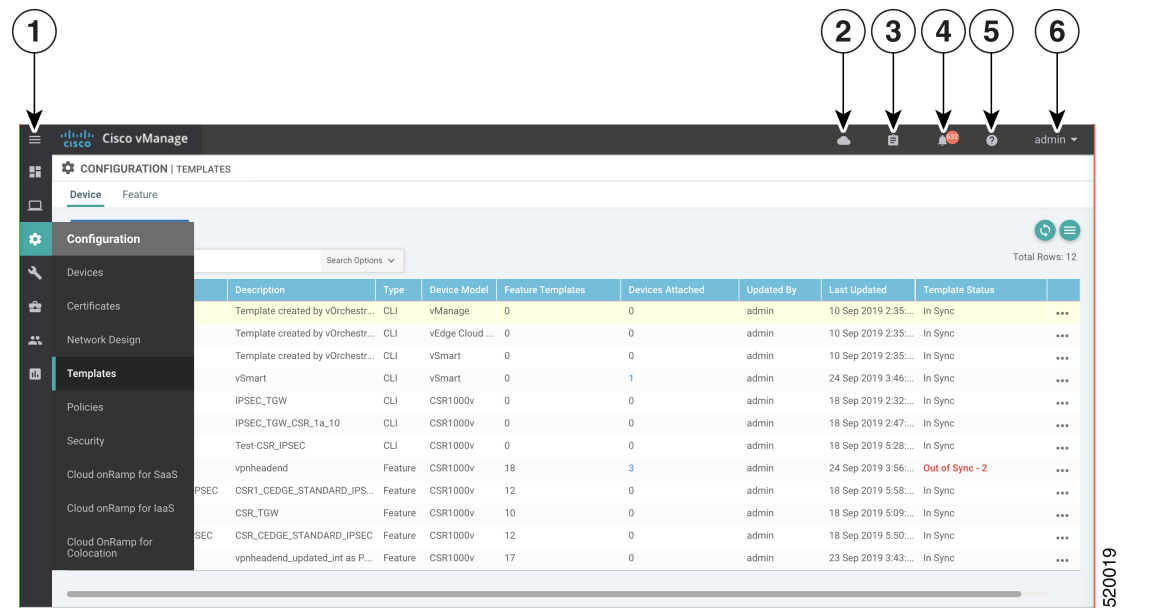
## Create a Device Template from Feature Templates

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Cisco SD-WAN software feature. Some feature templates are mandatory, indicated with an asterisk (\*), and some are optional. Each mandatory feature template, and some of the optional ones, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named `Factory_Default_feature-name_Template`) or you can create a custom feature template.

### Create a Device Template from Feature Templates

To create a device template:

**Figure 1: Create a Device Template Using Cisco vManage**



1	Menu
2	CloudExpress

3	Tasks
4	Alarms
5	Help
6	User Profile

1. In the Device tab, click the Create Template drop-down and select From Feature Template.
2. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (\*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.
6. To create a custom template for a feature, select the desired factory-default feature template and click Create Template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.
7. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
8. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
9. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.
10. 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 21:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Use Variable Values in Configuration Templates .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

1. For some groups of parameters, you can mark the entire group as device-specific. To do this, click the Mark as Optional Row box. These parameters are then grayed out so that you cannot enter a value for them in the feature template. You enter the value or values when you attach a device to a device template.
2. Click Save.
3. Repeat Steps 7 through 13 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in Available Feature Templates.
4. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see Available Feature Templates .

1. From the Templates title bar, select Feature.
2. Click the Add Template button.
3. In the left pane, from Select Devices, select the type of device for which you are creating a template. You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.
4. In the right pane, select the feature template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters. If the

feature has optional parameters, the bottom of the template form shows a plus sign (+) after the required parameters.

5. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
6. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter's value box
8. Click the plus sign (+) below the required parameters to set the values of optional parameters.
9. Click Save.
10. Repeat Steps 2 to 9 for each additional feature template you wish to create.
11. From the Templates title bar, select Device.
12. Click the Create Template drop-down and select From Feature Template.
13. From the Device Model drop-down, select the type of device for which you are creating the device template. vManage NMS displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (\*). The remaining templates are optional.
14. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (\_). It cannot contain spaces or any other characters.
15. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
16. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.
17. To use the factory-default configuration, click Create to create the device template. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.
18. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.
19. Repeat Step 18 for each factory-default feature template you wish to modify.
20. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

- [Configure Devices, on page 67](#)

# Configure Devices

## Create a Device CLI Template

To create a device template by entering a CLI text-style configuration directly on the vManage NMS:

1. In the Device tab, click the Create Template drop-down and select CLI Template.
2. From the Device Type drop-down, select the type of device for which you are creating the template.
3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (\_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format `{{variable-name}}`; for example, `{{hostname}}`.
7. Click Add. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

## Manage Device Templates

### Edit a Device Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.

You cannot change the name of a device or feature template when that template is attached to a device.

Note that you can edit templates simultaneously from one or more vManage servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

### Delete a Template

Deleting a template does not remove the associated configuration from devices.

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Delete.
3. Click OK to confirm deletion of the template.

### Copy a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Copy.
3. Enter a new template name and description.
4. Click Copy.

### Edit a CLI Device Template

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Device CLI Template window, edit the template.
4. Click Update.

## View Device Templates

•

### View a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click View.

### View Device Templates Attached to a Feature Template

1. In the Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Device Templates. The View Attached Device Templates popup window opens, displaying the names of the device templates to which the feature template is attached.

### View Devices Attached to a Device Template

For a device template that you created from feature templates:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices.

3. In the Attach Devices window, click the Attached Devices tab.

For a device template that you created from a CLI template:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Devices.

## Attach and Detach a Device Template

On Cisco Cisco IOS XE SD-WAN devices in the overlay network, you can perform the same operations, in parallel, from one or more vManage servers. You can perform the following template operations in parallel:

- Attach devices to a device template
- Detach devices from a device template
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click Update ► Configure Devices, all other template operations—including attach devices, detach devices, and edit device values—are locked on all vManage servers until the update operation completes. This means that a user on another vManage server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more vManage servers, at the same time. However, if any one of these operations is in progress on one vManage server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

### Attach Devices to a Device Template

To attach one or more devices to a device template:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices. The Attach Devices dialog box opens with the Select Devices tab selected
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.
5. Click Attach.
6. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
  - Enter the values manually for each device either in the table column or by clicking the More Actions icon to the right of the row and clicking Edit Device Template. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.

- Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.
1. Click Update
  2. Click Next. If any devices have the same system IP address, a pop-up or an error message is displayed when you click Next. Modify the system IP addresses so that there are no duplicates, and click Save. Then click Next again.
  3. In the left pane, select the device, to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the Config Preview tab in the upper right corner is selected. Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the Back button to edit the variable values entered in the previous screen.
  4. If you are attaching a Cisco IOS XE SD-WAN device, click Configure Device Rollback Timer located at the bottom of the left pane, to configure the time interval at which the device rolls back to its previous configuration if the router loses its control connection to the overlay network. The Configure Device Rollback Time dialog box is displayed.
    - a. From the Devices drop-down, select a device.
    - b. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
    - c. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password field pops up. Enter the password that you used to log in to the vManage NMS.
    - d. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
    - e. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.
    - f. The table at the bottom of the Configure Device Rollback Time dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the Trash icon to right right of the device name.
    - g. Click Save.
  5. Click Configure Devices to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

### Export a Variables Spreadsheet in CSV Format for a Template

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Export CSV.

## Change the Device Rollback Timer

By default, when you attach a Cisco IOS XE SD-WAN device to a configuration template, if the router is unable to successfully start after 5 minutes, it returns to, or rolls back to, the previous configuration. For a configuration that you have created from the CLI, you can change the device's rollback timer:

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane displays the device's configuration, and the Config Preview tab in the upper right corner is selected.
3. In the left pane, click the name of a device.
4. Click Configure Device Rollback Timer located at the bottom of the left pane. The Configure Device Rollback Time dialog box is displayed.
5. From the Devices drop-down, select a device.
6. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
7. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password field pops up. Enter the password that you used to log in to the vManage NMS.
8. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
9. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.
10. The table at the bottom of the Configure Device Rollback Time dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the Trash icon to right right of the device name.
11. Click Save.
12. Click Configure Devices to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

## Preview Device Configuration and View Configuration Differences

For a configuration that you have created from the CLI:

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane displays the device's configuration, and the Config Preview tab in the upper right corner is selected.
3. In the left pane, click the name of a device.
4. Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the Back button to edit the variable values entered in the previous screen.

5. Click Configure Devices to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

## Change Variable Values for a Device

For a configuration that you have created from device configuration templates, if the templates contain variables, the vManage NMS can automatically populate the variables with actual values when you attach the templates to the devices. To do this, you create an Excel file that lists the variable values for each device and save the file in CSV format. You can also enter values for these variables manually.

After you have pushed the configuration to a device, you can change the value assigned to any variable:

1. In the Device tab, select the device template.
2. Click the More Actions icon to the right of the row, and click Change Device Values. The screen displays a table of all the devices that are attached to that device template.
3. For the desired device, click the More Actions icon to the right of the row, and click Edit Device Template.
4. In the Update Device Template pop-up, enter values for the items in the variable list.
5. Click Update.
6. Click Next.
7. Click Configure Devices to push the configuration to the device. The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to the left of the row to display details of the push operation.

## Configuring Devices using vManage

Use the **Devices** screen to add and delete devices, toggle the mode of a device between CLI and vManage, upload the WAN Edge Serial number file, export bootstrap configuration and, and perform other device-related tasks.



1	Menu
2	CloudExpress
3	Tasks
4	Alarms
5	Help
6	User Profile

## Change Configuration Modes

A device can be in either of these configuration modes:

- vManage mode—A template is attached to the device and you cannot change the configuration on the device by using the CLI.
- CLI mode – No template is attached to the device and the device can be configured locally by using the CLI.

When you attach a template to a device from vManage, it puts the device in vManage mode. You can change the device back to CLI mode if needed to make local changes to its configuration.

To toggle a router from vManage mode to CLI mode:

1. In WAN Edge List tab, select a device.
2. Click the Change Mode drop-down and select CLI mode.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

To toggle a controller device from vManage mode to CLI mode:

1. In the Controllers tab, select a device.
2. Click the Change Mode drop-down.
3. Select CLI mode and then select the device type. The Change Mode CLI window opens.
4. From the vManage mode pane, select the device and click the right arrow to move the device to the CLI mode pane.
5. Click Update to CLI Mode.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

## Upload WAN Edge Router Authorized Serial Number File

The WAN Edge router authorized serial number file contains the chassis and serial numbers of all valid Cisco IOS XE SD-WAN devices in the overlay network. You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to the vManage NMS. Then, from the vManage NMS, you send it to the controllers in the network. This file is required to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

To upload the WAN edge router authorized serial number file to the vManage NMS and then download it to all the controllers in the overlay network:

1. In the WAN Edge List tab, click Upload WAN Edge List.
2. In the Upload WAN Edge List window:
  - a. Click Choose File and select the WAN edge router authorized serial number file you received from Cisco SD-WAN.
  - b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.
  - c. Click Upload.

A list of routers in the network is displayed in the router table, with details about each router.

## Upload WAN Edge Router Serial Numbers from Cisco Smart Account

Chassis and serial numbers of all valid Cisco IOS XE SD-WAN devices in the overlay network are required to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to the vManage NMS and then download it to all the controllers in the overlay network:

1. In the WAN Edge List tab, click Sync Smart Account.
2. In the Sync Smart Account window:
  - a. Enter the username and password for your Smart account..
  - b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.
  - c. Click Sync.

A list of routers in the network is displayed in the router table, with details about each router.

## Export Device Data in CSV Format

In an overlay network, you might have multiple devices of the same type that have identical or effectively identical configurations. For example, in a network with redundant Cisco vSmart Controllers, each controller must be configured with identical policies. Another example is a network with Cisco IOS XE SD-WAN devices at multiple sites, where each Cisco IOS XE SD-WAN device is providing identical services at each site.

Because the configurations for these devices are essentially identical, you can create one set of feature templates, which you then consolidate into one device template that you use to configure all the devices. You can create an Excel file in CSV format that lists the variables and defines each device specific variable value for each device. Then you can load the file when you attach a device template to a device.

To export data for all devices to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format.

## View and Copy Device Configuration

### View a Device's Running Configuration

Running configuration is configuration information that vManage obtains from the memory of a device. This information can be useful for troubleshooting.

To view a device's running configuration:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Running Configuration.

### View a Device's Local Configuration

Local configuration is configuration that vManage has stored for a device. This information can be useful for troubleshooting or for determining how to access a device if, for example, a device is not reachable from vManage.

To view a device's local configuration created using Configuration ► Templates:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Local Configuration.

### Copy Router Configuration

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

To copy the configuration from the old router to the new router:

1. In the Configuration ► Certificates screen, mark the new Cisco IOS XE SD-WAN device as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the old router.
3. Click the More Actions icon to the right of the row and click Copy Configuration.
4. In the Copy Configuration window, select the new router.
5. Click Update to confirm the copy of the configuration.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

1. In the Configuration ► Certificates screen, mark the new router as valid.
2. Click Send to Controller.

## Delete a WAN Edge Router

Deleting a router removes its serial and chassis numbers from the WAN edge router serial number list and permanently removes the router's configuration from the vManage NMS. Delete a router if you need to remove it from your deployment.

1. In the Configuration ► Certificates screen, mark the WAN Edge router as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the router.
3. Click the More Actions icon to the right of the row and click Delete WAN Edge.
4. Click OK to confirm deletion of the device.
5. In the Configuration ► Certificates screen, click Send to Controller.

## View Template Log and Device Bringup

### View Log of Template Activities

A log of template activities contains information that relates to creating, editing, and deleting configuration templates, and the status of attaching configuration templates to devices. This information can be useful for troubleshooting.

To view a log of template activities:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Template Log.

### View Status of Device Bringup

You can view the status of the operations involved in bringing a router or controller up in the overlay network. This information can help you monitor these operations.

To view the status of a device bringup:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Device Bring Up.

## Add a Cisco vBond Orchestrator

A Cisco vBond Orchestrator automatically orchestrates connectivity between Cisco IOS XE SD-WAN devices and vManage controllers. If any Cisco IOS XE SD-WAN device or Cisco vSmart Controller is behind a NAT, the Cisco vBond Orchestrator also serves as an initial NAT-traversal orchestrator. To add a Cisco vBond Orchestrator:

1. In the Controllers tab, click the Add Controller drop-down and select vBond.
2. In the Add vBond window:
  - a. Enter the management IP address of the vBond controller.
  - b. Enter the username and password to access the vBond orchestrator.
  - c. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.

d. Click Add.

3. Repeat Steps 1 and 2 to add additional Cisco vBond Orchestrators.

The new Cisco vBond Orchestrator is added to the list of controllers in the Controllers screen.

## Configure Cisco vSmart Controllers

### Add a vSmart Controller

After the Cisco vBond Orchestrator authenticates Cisco IOS XE SD-WAN devices, the Cisco vBond Orchestrator provides Cisco IOS XE SD-WAN devices information that they need to connect to the Cisco vSmart Controller. A Cisco vSmart Controller controls the flow of data traffic throughout the network via data and app-route policies. To configure Cisco vSmart Controllers:

1. In the Controllers tab, click the Add Controller drop-down and select vSmart.
2. In the Add vSmart window:
  - a. Enter the system IP address of the Cisco vSmart Controller.
  - b. Enter the username and password to access the Cisco vSmart Controller.
  - c. Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.
  - d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.  
The TLS (Transport Socket Layer) protocol that provides communications security over a network.
  - e. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.
  - f. Click Add.
3. Repeat Steps 1 and 2 to add additional Cisco vSmart Controllers. The vManage NMS can support up to 20 Cisco vSmart Controllers in the network.

The new Cisco vSmart Controller is added to the list of controllers in the Controllers screen.

### Edit Controller Details

Editing controller details lets you update the IP address and login credentials of a controller device. To edit controller details:

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Edit window, edit the IP address and the login credentials.
4. Click Save.

### Delete a Controller

Deleting a controller removes it from the overlay. Delete a controller if you are replacing it or if you no longer need it in your network.

To delete a controller:

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm the removal of the device and all its control connections.

### Configure Reverse Proxy on Controllers

To configure reverse proxy on an individual vManage NMS and Cisco vSmart Controller:

1. In the Controllers tab, select the device.
2. Click the More Actions icon to the right of the row, and click Add Reverse Proxy. The Add Reverse Proxy popup is displayed.
3. Click Add Reverse Proxy.
4. Configure the private IP address and port number for the device. The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.
5. Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.
6. If the vManage NMS or Cisco vSmart Controller has multiple cores, repeat Steps 4 and 5 for each core.
7. Click Add.

To enable reverse proxy in the overlay network, in vManage NMS select Administration ► Settings. Then click Edit to the right of the Reverse Proxy bar, click Enabled, and click Save.

## Create a UCS-E Template

*Table 22: Feature History*

Feature Name	Release Information	Feature Description
Create a UCS-E Template	Cisco IOS XE SD-WAN Release 16.12.1b	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template.

For more information about the Cisco Unified Computing System (UCS) E-Series Servers, see the [Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Hardware Installation Guide](#).

1. From the vManage menu, select Configuration ► Templates.
2. Click Feature.
3. Click Add Template.
4. Select a Cisco IOS XE SD-WAN device from the list.
5. From the Other Templates section, click UCSE.

The UCSE Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for configuring the Integrated Management Controller (IMC).

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

### Configure Bay and Slot for Template

Click the Basic Configuration tab to configure the bay and the slot for the template.

Parameter Name	Description
Bay	Specify the number for the SAS drive bays.
Slot	Specify the slot numbers for the mezzanine adapters.

### IMC Configuration

Click the IMC tab to configure the IMC parameters for the template.

Parameter Name	Description
Access Port	<p>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.</p> <p>Not all hardware models have a dedicated access port. See the Release Notes for your Cisco SD-WAN release for the supported hardware.</p> <p>Available options:</p> <ul style="list-style-type: none"> <li>• Dedicated</li> <li>• Shared</li> </ul> <p>The type of port, GE or TE, depends on the hardware model.</p> <p>For example:</p> <pre>Router(config-ucse)#imc access-port shared-lom ? GE1 GE1 TE2 TE2 TE3 TE3 console Console failover Failover</pre> <p>Some hardware models have GE ports whereas some have TE ports.</p> <p>Depending on the hardware module, the appropriate port (GE or TE) needs to be configured. Otherwise you will get an error.</p> <ul style="list-style-type: none"> <li>• You can obtain the UCS-E module hardware model type by using the following commands: <ul style="list-style-type: none"> <li><b>show inventory</b></li> <li><b>show platform</b></li> </ul> </li> <li>• Failover - sub-option under Shared.</li> </ul> <p>For example:</p> <pre>Router(config)#ucse subslot 1/0 Router(config-ucse)#imc access-port ? MGMT MGMT Interface shared-lom Shared LOM  Router(config-ucse)#imc access-port shared-lom ? GE1 GE1 TE2 TE2 TE3 TE3 console Console failover Failover</pre>
IPv4 Address	Provide the UCS-E management port address.



Parameter Name	Description
Default Gateway	Gateway tracking determine, for static routes, whether the next hop is reachable before adding that route to the device's route table.  Default: Enabled.
VLAN ID	Provide the VLAN number, which can be a value from 1 through 4094.
Assign Priority	Assign the priority.

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices.
Device Specific (indicated by a host icon)	<p>Use a device-specific value for the parameter.</p> <p>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.</p> <p>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.</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p>
Default	When Default is selected, this field is not enabled.





## CHAPTER 5

# Configure Network Interfaces

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

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

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



---

**Note** To maximize the efficiency of the load-balancing among Cisco vSmart Controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE SD-WAN devices in the domain. Example of a sequential numbering schemes is 172.1.1.1, 172.1.1.2, 172.1.1.3, and so on.

---



---

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

---

- [Configure VPN, on page 84](#)
- [Configure Interfaces in the WAN Transport VPN \(VPN 0\), on page 88](#)
- [Configure the System Interface, on page 90](#)
- [Configure Control Plane High Availability, on page 90](#)
- [Configure Other Interfaces, on page 91](#)
- [Role-Based Access Control by VPN, on page 92](#)
- [Configure Interface Properties, on page 96](#)
- [Enable DHCP Server using Cisco vManage, on page 98](#)
- [Configuring PPPoE, on page 101](#)
- [Configuring VRRP , on page 104](#)
- [Configure VPN Ethernet Interface, on page 105](#)
- [VPN Interface Bridge, on page 115](#)
- [VPN Interface DSL IPoE, on page 120](#)
- [VPN Interface DSL PPPoA, on page 128](#)
- [VPN Interface DSL PPPoE, on page 136](#)
- [VPN Interface Ethernet PPPoE, on page 145](#)

- [VPN Interface IPsec](#) , on page 152
- [VPN Interface Multilink](#), on page 159
- [Configure VPN Interface SVI using vManage](#), on page 166
- [VPN Interface T1/E1](#), on page 170
- [Cellular Interfaces](#), on page 177
- [WiFi Radio](#), on page 189
- [WiFi SSID](#), on page 191

## Configure VPN

### VPN

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

To configure VPNs using Cisco vManage templates, follow this general workflow:

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

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

- **VPN 0—Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
  - **VPN 512—Management VPN**, which carries out-of-band network management traffic among the Cisco IOS XE 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 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 SD-WAN devices.
2. Create interface feature templates to configure the interfaces in the VPN. See [VPN-Interface-Ethernet](#).

## 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 NMS, 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.



The screenshot displays the Cisco vManage interface for creating a VPN template. The breadcrumb navigation shows 'Feature Template > Add Template > VPN'. The 'Device Type' is 'ISR4331'. There are input fields for 'Template Name' and 'Description'. Below these are tabs for various configuration sections: 'Basic Configuration', 'DNS', 'Advertise OMP', 'IPv4 Route', 'IPv6 Route', 'Service', 'GRE Route', and 'IPSEC Route'. The 'Basic Configuration' tab is selected, showing a 'VPN' dropdown menu with '0' selected, a 'Name' field, and two toggle options: 'Enhance ECMP Keying' (checked) and 'Enable TCP Optimization' (checked). A vertical ID '520025' is visible on the right side of the form area.

**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.

## Changing the Scope for a Parameter Value

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

Parameter Name	Description
 Device Specific	<p>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.</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see <a href="#">_Create a Template Variables Spreadsheet</a></p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
 Global	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

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

## Configure Basic VPN Parameters

To configure basic VPN parameters, choose 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*	<p>Enter the numeric identifier of the VPN.</p> <p>Range for Cisco IOS XE SD-WAN devices: 0 through 65527</p> <p>Values for Cisco vSmart Controller and Cisco vManage devices: 0, 512</p>

Parameter Name	Description
Name	Enter a name for the VPN.  <b>Note</b> 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 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
<b>Primary DNS Address</b>	Select either <b>IPv4</b> or <b>IPv6</b> , and enter the IP address of the primary DNS server in this VPN.	
<b>New DNS Address</b>	Click <b>New DNS Address</b> 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.	
	<b>Mark as Optional Row</b>	Check <b>Mark as Optional Row</b> 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.
	<b>Hostname</b>	Enter the hostname of the DNS server. The name can be up to 128 characters.
	<b>List of IP Addresses</b>	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.
To save the DNS server configuration, click <b>Add</b> .		

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

### Mapping Host Names to IP Addresses

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

## Configure Interfaces in the WAN Transport VPN (VPN 0)

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

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

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




---

**Note** You can configure IPv6 addresses only on transport interfaces, that is, only in VPN 0.

---

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

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

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

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

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

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

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

On Cisco IOS XE SD-WAN devices, you must configure the tunnel encapsulation. The encapsulation can be either IPsec or GRE. For IPsec encapsulation, the default MTU is 1442 bytes, and for GRE it is 1468 bytes. These values are a function of overhead required for BFD path MTU discovery, which is enabled by default on all TLOCs. (For more information, see Configuring Control Plane and Data Plane High Availability



Parameters.) You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE 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 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 SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE SD-WAN device.

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

Service	Cisco vSmart Controller	Cisco vSmart Controller
<b>all</b> (Overrides any commands that allow or disallow individual services)	X	X
<b>bgp</b>	—	—
<b>dhcp</b> (for DHCPv4 and DHCPv6)	—	—
<b>dns</b>	—	—
<b>https</b>	X	—
<b>icmp</b>	X	X
<b>netconf</b>	X	—
<b>ntp</b>	—	—
<b>ospf</b>	—	—
<b>sshd</b>	X	X
<b>stun</b>	X	X

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

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

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

## Configure the System Interface

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

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

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

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

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

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

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



---

**Note** Use of port-channels on the Service Side VPN is not supported on Cisco IOS XE SD-WAN devices.

---

## Configure Control Plane High Availability

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

# Configure Other Interfaces

## Configure Interfaces in the Management (VRF mgmt-intf)

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

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

```
Device# show sdwan running-config | sec vrf definition Mgmt-intf
vrf definition Mgmt-intf
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
=====
interface GigabitEthernet0
  no shutdown
  vrf forwarding Mgmt-intf
  negotiation auto
exit
=====
config-t
ip route vrf Mgmt-intf 10.0.0.1 10.0.0.1
```

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

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 12 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
  4839793 packets input, 415574814 bytes, 0 no buffer
  Received 3060073 broadcasts (0 IP multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  82246 packets output, 41970224 bytes, 0 underruns
  Output 0 broadcasts (0 IP multicasts)
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
```

```
0 output buffer failures, 0 output buffers swapped out
```



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

### Configure Loopback Interfaces

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

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

### Configure Subinterfaces

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

For example:

```
interface GigabitEthernet0/0/0
description Main interface
no shutdown
arp timeout 1200
no ip address
ip mtu 1504
mtu 1504

interface GigabitEthernet0/0/0.100
description LAN VPN 1
no shutdown
encapsulation dot1Q 100
ip address 10.0.0.1 255.255.255.0
ip mtu 1500
mtu 1500
```

## Role-Based Access Control by VPN

### VPN Dashboard Overview

Users configured with VPN group can access only the VPN Dashboard, and it is read-only access. User with Admin access can create the VPN groups and has access to both Admin Dashboard and VPN Dashboard(s). Admin user can view these dashboards in the left panel as shown in the following figures:

Segment ID	Reference
100	0
Discovered_VPN_333	0
Discovered_VPN_111	0

VPN GROUP: Select VPN Group

VPN SEGMENT: All segments

No group data to display. Select VPN group to see details.

Device Health View (Total 2)	Site Health (Total 2)	WAN Edge Health (Total 2)
<p>2</p> <p>WAN Edge Devices</p> <p>2</p> <p>Status</p>	<p>Full WAN Connectivity: 2 sites</p> <p>Partial WAN Connectivity: 0 sites</p> <p>No WAN Connectivity: 0 sites</p>	<p>2 Normal</p> <p>0 Warning</p> <p>0 Error</p>

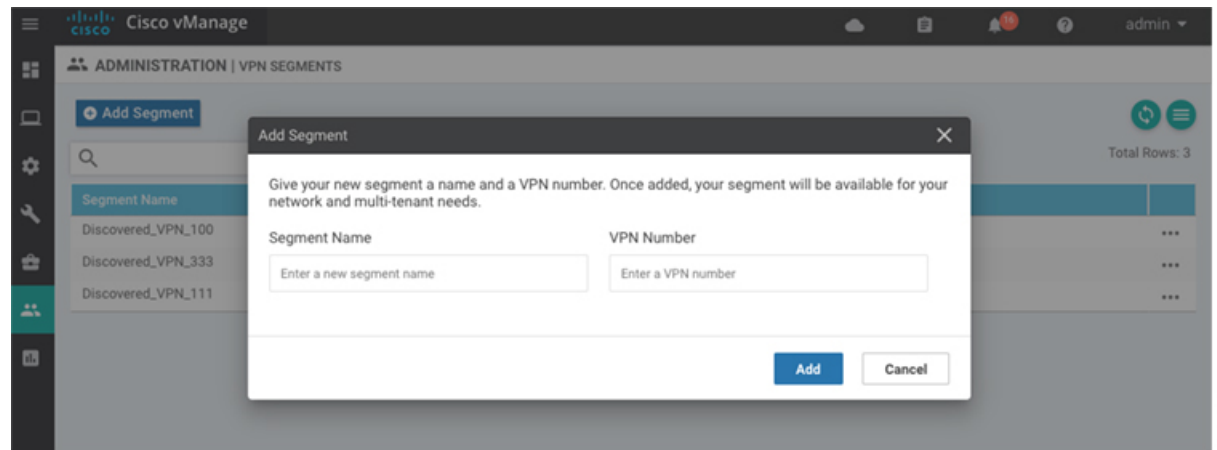
520038

## Configure and Manage VPN Segments

To configure VPN Segments:

1. Navigate to **Administration > VPN Segments** in Cisco vManage. The following web page displays with the list of segments that are configured.
2. To edit or delete an existing segment, click the **Edit or Delete** in the More Info (...) column on the right side.

- To add new segment, click **Add Segment**. Add Segment window appears.

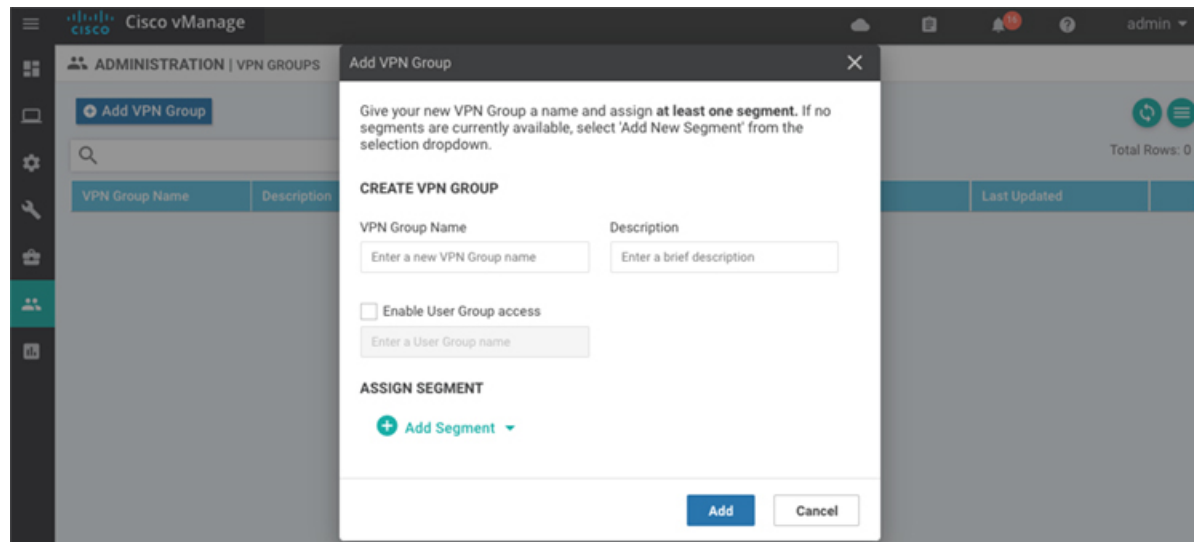


- Enter the name of the segment in the **Segment Name** field.
- Enter the number of VPNs you want to configure in VPN Number field.
- Click **Add** to add a new segment.

## Configure and Manage VPN Groups

To configure VPN Groups:

- Navigate to **Administration > VPN Groups** in Cisco vManage. The following web page displays with the list of segments that are configured.
- To edit or delete an VPN group, click the **Edit or Delete** in the More Info (...) column on the right side.
- To view the existing VPN in the dashboard, click on **View Dashboard** in the More Info column. The VPN Dashboard displays the device details of the VPN device configured.
- To add new VPN group, click **Add Group**. Add VPN Group window appears.

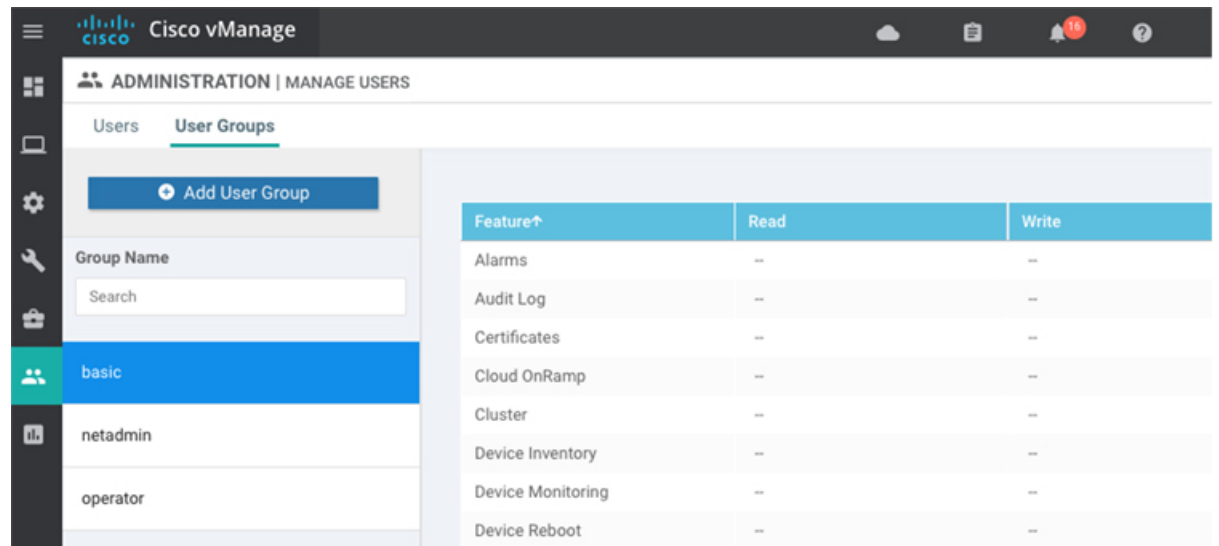


5. In the Create VPN Group pane, Enter VPN group name in the **VPN Group Name** field.
6. Enter a brief description of the VPN in the **Description** field.
7. Enable the user group access checkbox and enter the User Group Name.
8. In the Assign Segment pane, click on Add Segment drop-down to add new or existing segment to the VPN group.
9. Enter the Segment Name and VPN Number in the respective fields.
10. Click **Add** to add the configure VPN group to a device.

## Configure User with User group

To create users with user group that is associated with the VPN group:

1. Navigate to **Administration > Manage Users** from Cisco vManage. The manage Users window appears.
2. To edit, delete, or change password for an existing user, click the **Edit, Delete, or Change Password** in the More Info (...) column on the right side.
3. Click on **Add User** to add a new user.
4. In the Add New User page, add **Full Name, Username, Password, and Confirm Password details**.
5. In the User Group drop-down, select the user group where you want to add a user.
6. If you want to add a User Group, click on **Add User Group** button.



7. Enter the user group name in the **Group Name** field.
8. Select the Read or Write checkbox that you want to assign to a user group as shown in the figure.

## Configure Interface Properties

### Set the Interface Speed

When a Cisco IOS XE SD-WAN device comes up, the Cisco SD-WAN software autodetects the SFPs present in the router and sets the interface speed accordingly. The software then negotiates the interface speed with the device at the remote end of the connection to establish the actual speed of the interface. To display the hardware present in the router, use the **show hardware inventory** command:

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

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

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

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

### Set the Interface MTU

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

The MTU can range from 576 through 2000 bytes.



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

For Cisco vBond Orchestrator, Cisco vManage, and Cisco vSmart Controller devices, you can configure interfaces to use ICMP to perform path MTU (PMTU) discovery. When PMTU discovery is enabled, the device automatically negotiates the largest MTU size that the interface supports in an attempt to minimize or eliminate packet fragmentation:

On Cisco IOS XE SD-WAN device, the Cisco SD-WAN BFD software automatically performs PMTU discovery on each transport connection (that is, for each TLOC, or color). BFD PMTU discovery is enabled by default, and it is recommended that you use it and not disable it. To explicitly configure BFD to perform PMTU discovery, use the **bfd color pmtu-discovery** configuration command. However, you can choose to instead use ICMP to perform PMTU discovery:

BFD is a data plane protocol and so does not run on Cisco vBond Orchestrator, Cisco vManage, and Cisco vSmart Controller devices.

## Monitoring Bandwidth on a Transport Circuit

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

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

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

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

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

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

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

# Enable DHCP Server using Cisco vManage

Table 23: Feature History

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

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

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

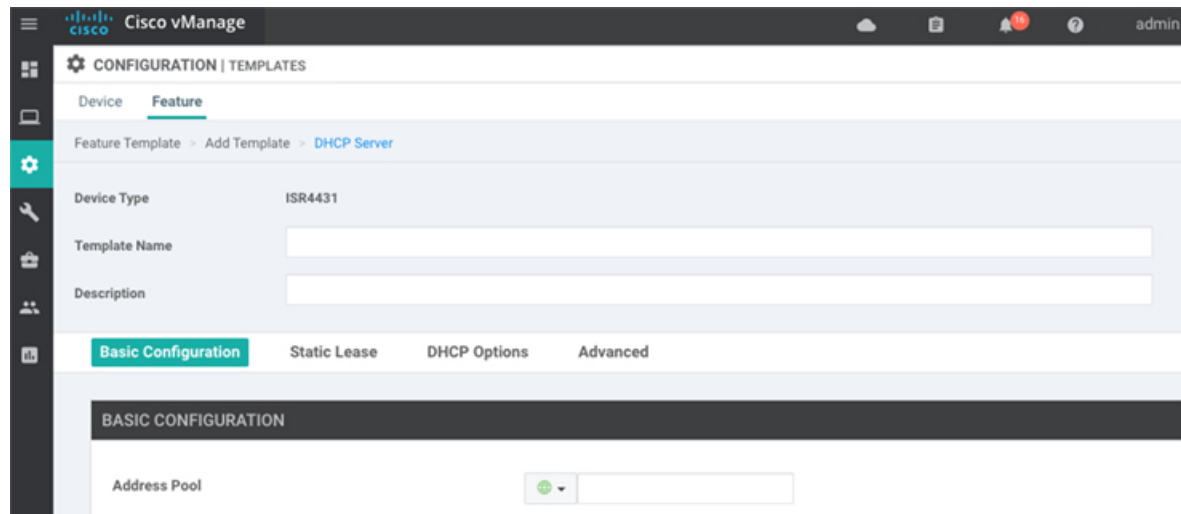
To configure a Cisco SD-WAN device to act as a DHCP server using Cisco vManage templates:

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

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

## Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
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. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface.
8. From the Sub-Templates drop-down, select DHCP Server.
9. From the DHCP Server drop-down, click Create Template. The DHCP-Server template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining DHCP Server parameters.



10. 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.
11. 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.

### Minimum DHCP Server Configuration

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

**Table 24:**

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

Parameter Name	Description
Administrative State	Select Up to enable or Down to disable the DHCP functionality on the interface. By default, DHCP server functionality is disabled on an interface.

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

### Configure Static Leases

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

**Table 25:**

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

To edit a static lease, click the pencil icon to the right of the entry.

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

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

### Configure Advanced Options

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

**Table 26:**

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

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

### Configure DHCP server using CLI

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

### Release Information

Introduced in Cisco vManage NMS in Release 15.2.

## Configuring PPPoE

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

To configure PPPoE client on a Cisco SD-WAN device, you create a PPP logical interface and link it to a physical interface. The PPPoE connection comes up when the physical interface comes up. You can link a PPP interface to only one physical interface on a Cisco SD-WAN device, and you can link a physical interface to only one PPP interface. To enable more than one PPPoE interfaces on a Cisco SD-WAN device, configure multiple PPP interfaces.

It is recommended that you configure quality of service (QoS) and shaping rate on a PPPoE-enabled physical interface, and not on the PPP interface.

PPPoE-enabled physical interfaces do not support:

- 802.1Q
- Subinterfaces
- NAT, PMTU, and tunnel interfaces. These are configured on the PPP interface and therefore not available on PPPoE-enabled interfaces.

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

## Configure PPPoE from vManage Templates

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

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

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

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

**Table 27:**

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

1. In vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select Cisco IOS XE SD-WAN device Cloud or a router model.
5. In the right pane, select the VPN-Interface-PPP template.
6. In the template, configure the following parameters:

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

1. In the vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select Cloud or a router model.

5. In the right pane, select the VPN-Interface-PPP-Ethernet template.
6. In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
Shutdown	Click No to enable the PPPoE-enabled interface.
Interface Name	Enter the name of the physical interface in VPN 0 to associate with the PPP interface.
Description (optional)	Enter a description for the PPPoE-enabled interface.
IP Configuration	Assign an IP address to the physical interface: <ul style="list-style-type: none"> <li>• To use DHCP, select Dynamic. The default administrative distance of routes learned from DHCP is 1.</li> <li>• To configure the IP address directly, enter of the IPv4 address of the interface.</li> </ul>
DHCP Helper (optional)	Enter up to four IP addresses for DHCP servers in the network.
Save	Click Save to save the feature template.

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

1. In the vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select Cloud or a router model.
5. In the right pane, select the VPN template.
6. In the template, configure the following parameters:

Parameter Field	Procedure
Template Name	Enter a name for the template. It can be up to 128 alphanumeric characters.
Description	Enter a description for the template. It can be up to 2048 alphanumeric characters.
VPN Identifier	Enter VPN identifier 0.
Name	Enter a name for the VPN.
Other interface parameters	Configure the desired interface properties.
Save	Click Save to save the feature template.

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

1. In the vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Device.
3. Click Create Template, and from the drop-down list select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the device template. vManage NMS displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (\*).
5. Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.
6. In the Transport & Management VPN section, under VPN 0, from the drop-down list of available templates, select the desired feature template. The list of available templates are the ones that you have previously created.
7. In the Additional VPN 0 Templates section to the right of VPN 0, click the plus sign (+) next to VPN Interface PPP.
8. In the VPN-Interface-PPP and VPN-Interface-PPP-Ethernet fields, select the feature templates to use.
9. To configure multiple PPPoE-enabled interfaces in VPN 0, click the plus sign (+) next to Sub-Templates.
10. To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
11. Click Create to create the device template.

To attach a device template to a device:

1. In the vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Device.
3. Select a template.
4. Click the More Actions icon to the right of the row and click Attach Device.
5. In the Attach Device window, either search for a device or select a device from the Available Device(s) column to the left.
6. Click the arrow pointing right to move the device to the Selected Device(s) column on the right.
7. Click Attach.

## Configuring VRRP

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



For a VRRP interface to operate, its physical interface must be configured in VPN 0:

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

The group number identifies the virtual router. You can configure a maximum of 24 groups on a router. In a typical VRRP topology, two physical routers are configured to act as a single virtual router, so you configure the same group number on interfaces on both these routers.

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

Within each VRRP group, the router with the higher priority value is elected as primary VRRP. By default, each virtual router IP address has a default primary election priority of 100, so the router with the higher IP address is elected as primary. You can modify the priority value, setting it to a value from 1 through 254.

The primary VRRP periodically sends advertisement messages, indicating that it is still operating. If backup routers miss three consecutive VRRP advertisements, they assume that the primary VRRP is down and elect a new primary VRRP. By default, these messages are sent every second. You can change the VRRP advertisement time to be a value from 1 through 3600 seconds.

By default, VRRP uses the state of the interface on which it is running, to determine which router is the primary virtual router. This interface is on the service (LAN) side of the router. When the interface for the primary VRRP goes down, a new primary VRRP virtual router is elected based on the VRRP priority value. Because VRRP runs on a LAN interface, if a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, you can configure one of the following:

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

If all OMP sessions are lost on the primary VRRP router, VRRP elects a new default gateway from among all the gateways that have one or more active OMP sessions even if the gateway chosen has a lower VRRP priority than the current primary VRRP router. With this option, VRRP failover occurs once the OMP state changes from up to down, which occurs when the OMP hold timer expires. (The default OMP hold timer interval is 60 seconds.) Until the hold timer expires and a new primary VRRP is elected, all overlay traffic is dropped. When the OMP session recovers, the local VRRP interface claims itself as primary VRRP even before it learns and installs OMP routes from the Cisco vSmart Controllers. Until the routers are learned, traffic is also dropped.

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

If all OMP sessions are lost, VRRP failover occurs as described for the **track-omp** option. In addition, if reachability to all the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the router determines the primary VRRP.

As discussed above, the IEEE 802.1Q protocol adds 4 bytes to each packet's length. Hence, for packets to be transmitted, either increase the MTU size on the physical interface in VPN 0 (the default MTU is 1500 bytes) or decrease the MTU size on the VRRP interface.

## Configure VPN Ethernet Interface

**Step 1** In Cisco vManage, select the **Configuration > Templates** screen.

- 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:
- Click the **Transport & Management VPN** tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
  - Under **Additional VPN 0 Templates**, located to the right of the screen, click **Cisco VPN Interface Ethernet**.
  - From the VPN Interface drop-down, click **Create Template**. The **Cisco VPN Interface Ethernet** template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
- Step 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.
- Step 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.

## 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
<b>Shutdown*</b>			Click <b>No</b> to enable the interface.
<b>Interface name*</b>			Enter a name for the interface. For Cisco IOS XE SD-WAN devices, you must: <ul style="list-style-type: none"> <li>• Spell out the interface names completely (for example, GigabitEthernet0/0/0).</li> <li>• 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.</li> </ul>
<b>Description</b>			Enter a description for the interface.
<b>IPv4 / IPv6</b>			Click <b>IPv4</b> to configure an IPv4 VPN interface. Click <b>IPv6</b> to configure an IPv6 interface.

Parameter Name	IPv4 or IPv6	Options	Description
<b>Dynamic</b>	Click <b>Dynamic</b> to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.		
	<b>Both</b>	<b>DHCP Distance</b>	Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.
	<b>IPv6</b>	<b>DHCP Rapid Commit</b>	Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments.  Click <b>On</b> to enable DHCP rapid commit Click <b>Off</b> to continue using the regular commit process.
<b>Static</b>	Click <b>Static</b> to enter an IP address that doesn't change.		
	<b>IPv4</b>	<b>IPv4 Address</b>	Enter a static IPv4 address.
	<b>IPv6</b>	<b>IPv6 Address</b>	Enter a static IPv6 address.
<b>Secondary IP Address</b>	<b>IPv4</b>	Click <b>Add</b> to enter up to four secondary IPv4 addresses for a service-side interface.	
<b>IPv6 Address</b>	<b>IPv6</b>	Click <b>Add</b> to enter up to two secondary IPv6 addresses for a service-side interface.	
<b>DHCP Helper</b>	<b>Both</b>	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.	
<b>Block Non-Source IP</b>	<b>Yes / No</b>	Click <b>Yes</b> to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click <b>No</b> 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 <b>On</b> to create a tunnel interface.

Parameter Name	Description
Color	Select a color for the TLOC.
Port Hop	Click <b>On</b> to enable port hopping, or click <b>Off</b> 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 <a href="#">System</a> configuration template.  Default: Enabled  vManage NMS and Cisco vSmart Controller default: Disabled
Allow Service	Select <b>On</b> or <b>Off</b> 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**.

## Associate a Carrier Name with a Tunnel Interface

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

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

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

## Limit Keepalive Traffic on a Tunnel Interface

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

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

- For a tunnel connection between two controller devices, the tunnel uses the lower hello interval and the higher tolerance interval for the connection between the two devices. (Controller devices are vBond controllers, vManage NMSs, and vSmart controllers.) This choice is made in case one of the controllers has a slower WAN connection. The hello interval and tolerance times are chosen separately for each pair of controller devices.
- For a tunnel connection between a Cisco IOS XE SD-WAN device and any controller device, the tunnel uses the hello interval and tolerance times configured on the router. This choice is made to minimize the amount traffic sent over the tunnel, to allow for situations where the cost of a link is a function of the amount of traffic traversing the link. The hello interval and tolerance times are chosen separately for each tunnel between a Cisco IOS XE SD-WAN device and a controller device.

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

```
Device(config-tunnel-interface)# hello-interval milliseconds
Device(config-tunnel-interface)# hello-tolerance seconds
```

The default hello interval is 1000 milliseconds, and it can be a time in the range 100 through 600000 milliseconds (10 minutes). The default hello tolerance is 12 seconds, and it can be a time in the range 12 through 600 seconds (10 minutes). The hello tolerance interval must be at most one-half the OMP hold time. The default OMP hold time is 60 seconds, and you configure it with the **omp timers holdtime** command.

## Configure an Interface as a NAT Device

You can configure IPv4 and IPv6 interfaces to act as a network address translation (NAT) device for applications such as port forwarding. To configure a NAT device:

1. In the **Cisco VPN Interface Ethernet Template**, click the **NAT** tab, and select either **IPv4** or **IPv6**.
2. Change the scope from Default (blue check) to **Global** (green globe).
3. Click **On** to enable NAT (IPv4) or NAT64 (IPv6). The correct set of parameters will display.
4. Enter the parameter values.
5. To save the feature template, click **Save**.



**Note** Optionally, click **Static NAT** to enable those parameters.

## IPv4 NAT Parameter Values

### Configure Static NAT

To configure a static NAT of service-side source IP addresses:

1. In the **Cisco VPN Interface Ethernet Template**, click the **NAT** tab, and select either **IPv4** or **IPv6**.
  - . Click **New Static NAT** and configure the following parameters to add a static NAT mapping:

*Table 28:*

Parameter Name	Description
Mark as Optional Row	Check <b>Mark as Optional Row</b> 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.
Source IP	Enters the NAT private source IP address.
Translated Source IP Address	Maps a public IP address to a private source address, enter the public IP address.
Static NAT Direction	Selects the direction in which to perform network address translation.
inside	Translates the IP address of packets that are coming from the service side of the device and that are destined for the transport side of the router.
outside	Translates the IP address of packets that are coming to the device from the transport side device and that are destined for a service-side device.
Source VPN ID	Configures Source VPN ID

2. To save the NAT mapping, click **Add**.
3. To save the feature template, click **Save**.

## IPv6 NAT Parameter Values

Table 29: IPv4 NAT Parameter Values

Parameter Name	Description
UDP Timeout	<p>Enter the timeout value for User Datagram Protocol (UDP) traffic</p> <ol style="list-style-type: none"> <li>1. Change the scope from Default to <b>Global</b>.</li> <li>2. Enter a timeout value.</li> </ol> <p>Range: 1–536870 seconds Default: 1 second</p>
TCP Timeout	<p>Enter the timeout value for Transmission Control Protocol (TCP) traffic.</p> <ol style="list-style-type: none"> <li>1. Change the scope from Default to <b>Global</b>.</li> <li>2. Enter a timeout value.</li> </ol> <p>Enter a timeout value. Default: 60 seconds</p>

## IPv6 Support for NAT64 Devices

Table 30: Feature History

Feature Name	Release Information	Description
IPv6 Support for NAT64 Devices	Cisco IOS XE SD-WAN Release 16.12.1b	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices.

### Configure NAT64 CLI Equivalent on Cisco IOS XE SD-WAN Devices

```
interface GigabitEthernet3
  no shutdown
  arp timeout 1200
  vrf forwarding 1
  ip address 10.1.19.15 255.255.255.0
  negotiation auto
  nat64 enable
  nat64 prefix stateful 2001::F/64 vrf 1

  nat64 v4 pool pool1 10.1.1.10 10.1.1.100
  nat64 v6v4 list global-list pool pool1 vrf 1
  nat64 translation timeout tcp 60
  nat64 translation timeout udp 1
```

## Apply Access Lists and QoS Parameters

Quality of service (QoS) helps determine how a service will perform. By configuring QoS, enhance the performance of an application on the WAN. To configure a shaping rate for an interface and to apply a QoS

map, a rewrite rule, access lists, and policers to a interface, select the ACL/QoS tab and configure the following parameters:

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

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

## Add ARP Table Entries

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

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

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

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

## Configuring VRRP

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



Parameter Name	Description
Group ID	Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255
Priority	Enter the priority level of the router. The router with the highest priority is elected as primary VRRP router. If two routers have the same priority, the one with the higher IP address is elected as primary VRRP router. Range: 1 through 254 Default: 100
Timer	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP routers. Range: 1 through 3600 seconds Default: 1 second
Track OMP Track Prefix List	By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which router is the primary virtual router. If a router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:  <b>Track OMP</b> —Click <b>On</b> 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.  <b>Track Prefix List</b> —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 routers determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local router and the peer running VRRP.

## Configure Advanced Properties

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

Parameter Name	Description
Duplex	Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. Default: full

Parameter Name	Description
MAC Address	Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
PMTU Discovery	Click <b>On</b> to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.
Flow Control	Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. Values: autonet, both, egress, ingress, none Default: autoneg
TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None
Speed	Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, or 1000 Mbps Default: Autonegotiate (10/100/1000 Mbps)
Clear-Don't-Fragment	Click <b>On</b> to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Autonegotiation	Click <b>Off</b> to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.  Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface.
GRE Tunnel Source IP	Enter the IP address of the extended WAN interface.
Xconnect (on IOS XE routers)	Enter the name of a physical interface on the same router that connects to the WAN transport.

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

# VPN Interface Bridge

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

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

To configure a bridge interface using Cisco vManage templates:

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

## Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the **Configuration** > **Templates** screen.
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. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the **Service VPN** section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface Bridge.
8. From the VPN Interface Bridge drop-down, click Create Template. The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.
9. In 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 31:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Release Information

Introduced in Cisco vManage NMS in Release 15.3. In Release 18.2, add support for disabling ICMP redirect messages.

## Create a Bridging Interface

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

Table 32:

Parameter Name	Description
Shutdown*	Click <b>No</b> to enable the interface.
Interface name*	Enter the name of the interface, in the format <b>irb number</b> . The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to.
Description	Enter a description for the interface.
IPv4 Address*	Enter the IPv4 address of the router.

Parameter Name	Description
DHCP Helper	Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Block Non-Source IP	Click <b>Yes</b> to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.
Secondary IP Address (on Cisco IOS XE SD-WAN devices)	Click <b>Add</b> to configure up to four secondary IPv4 addresses for a service-side interface.

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

*CLI equivalent:*

## Apply Access Lists

### Apply Access Lists

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

**Table 33:**

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

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

*CLI equivalent:*

## 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 34:**

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. <i>Range:</i> 1 through 255

Parameter Name	Description
Priority	Enter the priority level of the router. The router with the highest priority is elected as primary VRRP router. If two Cisco IOS XE SD-WAN devices have the same priority, the one with the higher IP address is elected as primary VRRP router. <i>Range:</i> 1 through 254 <i>Default:</i> 100
Timer	Specify how often the primary VRRP router sends VRRP advertisement messages. If subordinate routers miss three consecutive VRRP advertisements, they elect a new primary VRRP router. <i>Range:</i> 1 through 3600 seconds <i>Default:</i> 1 second
Track OMP Track Prefix List	By default, VRRP uses 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 devices determine the primary VRRP router.
IP Address	Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local Cisco IOS XE SD-WAN device and the peer running VRRP.

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

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

## Add ARP Table Entries

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

*Table 35:*

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**.

*CLI equivalent:*

## Configure Advanced Properties

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

**Table 36:**

Parameter Name	Description
MAC Address	<p>MAC addresses can be static or dynamic. A static MAC address is manually configured as opposed to a dynamic MAC address that is one learned via an ARP request. You can configure a static MAC on a router's interface or indicate a static MAC that identifies a router's interface.</p> <p>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.</p>
IP MTU	<p>Similar to MTU, IP MTU only affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented.</p> <p>Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes</p>
TCP MSS	<p>TCP MSS will affect any packet that contains an initial TCP header that flows through the router. When configured, TCP MSS will be examined against the MSS exchanged in the three-way handshake. The MSS in the header will be lowered if the configured setting is lower than what is in the header. If the header value is already lower, it will flow through unmodified. The end hosts will use the lower setting of the two hosts. If the TCP MSS is to be configured, it should be set it at 40 bytes lower than the minimum path MTU.</p> <p>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. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None</p>
Clear-Dont-Fragment	<p>Configure Clear-Dont-Fragment if there are packets arriving on an interface with the DF-bit set. If these packets are larger than the MTU will allow, they are dropped. If you clear the df-bit, the packets will be fragmented and sent.</p> <p>Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</p>
ARP Timeout	<p>ARP Timeout controls how long we maintain the ARP cache on a router.</p> <p>Specify how long it takes for a dynamically learned ARP entry to time out.</p> <p><i>Range:</i> 0 through 2678400 seconds (744 hours) <i>Default:</i> 1200 seconds (20 minutes)</p>

Parameter Name	Description
ICMP Redirect	<p>ICMP Redirects are sent by a router to the sender of an IP packet when a packet is being routed sub-optimally.</p> <p>The ICMP Redirect informs the sending host to forward subsequent packets to that same destination through a different gateway.</p> <p>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</p>

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

## VPN Interface DSL IPoE


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

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

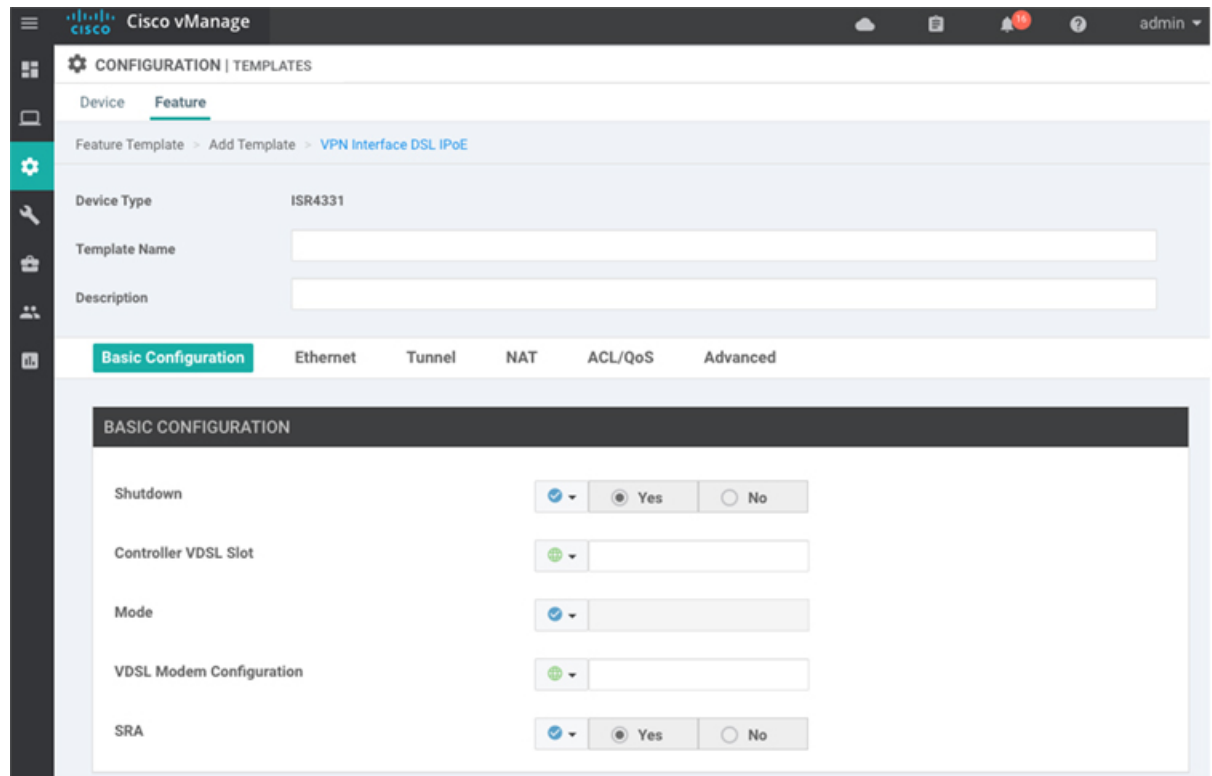
To configure DSL interfaces on Cisco IOS XE SD-WAN devices using Cisco vManage templates:

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

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
  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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
  6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL IPoE.
  7. From the VPN Interface DSL IPoE drop-down, click Create Template. The VPN Interface DSL IPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IPoE Interface parameters.
- 
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 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 37:**

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices.  Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

### Configure IPoE Functionality

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

**Table 38:**

Parameter Name	Description
Shutdown*	Click No to enable the VDSL controller interface.
Controller VDSL Slot*	Enter the slot number of the controller VDSL interface, in the format <i>slot/subslot/port</i> (for example, 0/2/0).
Mode*	Select the operating mode of the VDSL controller from the drop-down: <ul style="list-style-type: none"> <li>• Auto—Default mode.</li> <li>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.</li> <li>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.</li> <li>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.</li> <li>• ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.</li> <li>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..</li> </ul>
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco vManage NMS. If the command is not valid, it is not executed.
SRA	Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

To save the feature template, click Save.

### Configure the Ethernet Interface

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

**Table 39:**

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

To save the feature template, click Save.

### Create a Tunnel Interface

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

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

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

**Table 40:**

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection	If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.
Maximum Control Connections	Specify the maximum number of Cisco vSmart Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.  <i>Range: 0 through 8Default: 2</i>

Parameter Name	Description
Cisco vBond Orchestrator As STUN Server	Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco vSmart Controllers that the tunnel interface is not allowed to connect to. <i>Range:</i> 0 through 100
Cisco vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco vManage NMS. <i>Range:</i> 0 through 8 <i>Default:</i> 5
Port Hop	Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <i>Default:</i> Enabled
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select On or Off for each service to allow or disallow the service on the interface.

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

**Table 41:**

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

Parameter Name	Description
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

### Configure the Interface as a NAT Device

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

**Table 42:**

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

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

Table 43:

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

To save a port forwarding rule, click Add.

To save the feature template, click Save.

### Apply Access Lists

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

Table 44:

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

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

To save the feature template, click Save.

### Configure Other Interface Properties

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

**Table 45:**

Parameter Name	Description
Bandwidth Upstream	When the bandwidth of traffic transmitted on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE SD-WAN devices and Cisco vManage NMSs only), BW Upstream issues notifications.  For transmitted traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
Bandwidth Downstream	When the bandwidth of traffic received on a physical interface in the WAN transport VPN (VPN 0) exceeds a specific limit by 85 percent (on Cisco IOS XE SD-WAN devices and Cisco vManage NMSs only), BW Downstream issues notifications.  For received traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
IP MTU	IP MTU affects IP packets. If an IP packet exceeds the IP MTU, then the packet will be fragmented.  Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes
TCP MSS	In a single TCP/IPv4 datagram, the TCP Maximum Segment Size (MSS) defines the maximum data that a host will accept. This TCP/IPv4 datagram might be fragmented at the IPv4 layer. The MSS value is sent as a TCP header option only in TCP SYN segments.  Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
TLOC Extension	Use a TLOC Extension to bind an interface and connect another Cisco IOS XE SD-WAN device at the same physical site to the local router's WAN transport interface (on Cisco IOS XE SD-WAN devices only).  Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.

Parameter Name	Description
Tracker	<p>Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet rather than having to first go to a router in a data center. In this situation, enabling NAT on the transport interface splits the TLOC between the local router and the data center into two, with one going to the remote router and the other going to the internet.</p> <p>When you enable transport tunnel tracking, the software periodically probes the path to the internet to determine whether it is up. If the software detects that this path is down, it withdraws the route to the internet destination, and traffic destined to the internet is then routed through the data center router. When the software detects that the path to the internet is again functioning, the route to the internet is reinstalled.</p> <p>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</p>
IP Directed-Broadcast	<p>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.</p> <p>A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.</p> <p>If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.</p>

To save the feature template, click Save.

### Release Information

Introduced in Cisco vManage NMS in Release 18.4.1.

## VPN Interface DSL PPPoA

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

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

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

To configure DSL interfaces on Cisco routers using Cisco vManage templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.



### Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoA.
7. From the VPN Interface DSL PPPoA drop-down, click Create Template. The VPN Interface DSL PPPoA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP parameters.

The screenshot shows the Cisco vManage interface for configuring a template. The top navigation bar includes the Cisco logo, 'Cisco vManage', and a user profile 'admin'. Below this is a breadcrumb trail: 'CONFIGURATION | TEMPLATES' with sub-breadcrumbs 'Device' and 'Feature'. The main content area is titled 'Feature Template > Add Template > VPN Interface DSL PPPoA'. It contains a form with the following fields: 'Device Type' (set to 'ISR4331'), 'Template Name' (empty), and 'Description' (empty). Below the form is a tabbed interface with 'Basic Configuration' selected, and other tabs for 'ATM', 'PPP', 'Tunnel', 'NAT', 'ACL/QoS', and 'Advanced'. The 'BASIC CONFIGURATION' section includes several settings: 'Shutdown' (checked), 'Controller VDSL Slot' (empty), 'Mode' (empty), 'VDSL Modem Configuration' (empty), 'SRA' (checked), 'Bandwidth Upstream' (empty), and 'Bandwidth Downstream' (empty). Each setting has a dropdown arrow and a radio button for 'Yes' or 'No'.

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 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 46:**

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Configure VDSL Controller Functionality

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

**Table 47:**

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

Parameter Name	Description
Mode*	<p>Select the operating mode of the VDSL controller from the drop-down:</p> <ul style="list-style-type: none"> <li>• Auto—Default mode.</li> <li>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.</li> <li>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.</li> <li>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.</li> <li>• ANSI—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.</li> <li>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.</li> </ul>
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco vManage NMS. If the command is not valid, it is not executed.
SRA	Enabled by default. Click No to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

To save the feature template, click Save.

### Configure the ATM Interface

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

**Table 48:**

Parameter Name	Description
ATM Interface Name	Enter a name for the ATM interface, in the format <i>subslot/port</i> (for example 2/0). You do not need to enter the slot number, because it must always be 0.
Description	Enter a description for the interface.
VPI and VCI	Create an ATM permanent virtual circuit (PVC), in the format <i>vpi/vci</i> . Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).

Parameter Name	Description
Encapsulation	Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down: <ul style="list-style-type: none"> <li>• AAL5 MUX—Dedicate the PVC to a single protocol.</li> <li>• AAL5 NLPID—Use NLPID multiplexing.</li> <li>• AAL5 SNAP—Multiplex two or more protocols on the same PVC.</li> </ul>
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.
VBR-NRT	Configure variable bit rate non-real-time parameters: <ul style="list-style-type: none"> <li>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.</li> <li>• Sustainable Cell Rate—Enter the sustainable cell rate, in Kbps.</li> <li>• Maximum Burst Size—This size can be 1 cell.</li> </ul>
VBR-RT	Configure variable bit rate real-time parameters: <ul style="list-style-type: none"> <li>• Peak Cell Rate—Enter a value from 48 through 25000 Kbps.</li> <li>• Average Cell Rate—Enter the average cell rate, in Kbps.</li> <li>• Maximum Burst Size—This size can be 1 cell.</li> </ul>

To save the feature template, click Save.

### Configure the PPP Authentication Protocol

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

**Table 49:**

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: <ul style="list-style-type: none"> <li>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters.</li> <li>• PAP—Enter the username and password provided by your ISP. <i>username</i> can be up to 255 characters.</li> <li>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</li> </ul>

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 can have up to four TLOCs.

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

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

**Table 50:**

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection	If the Cisco IOS XE SD-WAN device has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.
Maximum Control Connections	Specify the maximum number of Cisco vSmart Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. <i>Range: 0 through 8Default: 2</i>
Cisco vBond Orchestrator As STUN Server	Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the Cisco IOS XE SD-WAN device is located behind a NAT.
Exclude Controller Group List	Set the Cisco vSmart Controllers that the tunnel interface is not allowed to connect to. <i>Range: 0 through 100</i>
Cisco vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco vManage NMS. <i>Range: 0 through 8Default: 5</i>
Port Hop	Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <i>Default: Enabled</i>
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select On or Off for each service to allow or disallow the service on the interface.

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

Table 51:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. <i>Range:</i> 0 through 4294967295 <i>Default:</i> 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

### 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 52:

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

To save the feature template, click Save.

### Configure Other Interface Properties

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

Table 53:

Parameter Name	Description
PMTU Discovery	Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TCP 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. <i>Range: 552 to 1460 bytes</i> <i>Default: None</i>
Clear Dont Fragment	Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. <i>Range: 0 through 7</i>
Autonegotiate	Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.

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

To save the feature template, click Save.

### Release Information

Introduced in Cisco vManage NMS in Release 18.3.

## VPN Interface DSL PPPoE

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

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

To configure DSL interfaces on Cisco routers using Cisco vManage templates:

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

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoE.
7. From the VPN Interface DSL PPPoE drop-down, click Create Template. The VPN Interface DSL PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PPPoE Interface parameters.



The screenshot shows the Cisco vManage interface for configuring a feature template. The breadcrumb trail is: Feature Template > Add Template > VPN Interface DSL PPPoE. The device type is set to ISR4331. The 'Basic Configuration' tab is active, showing the following parameters:

Parameter	Value / Options
Shutdown	Yes (selected), No
Controller VDSL Slot	+ [ ]
Mode	[ ]
VDSL Modem Configuration	+ [ ]
SRA	Yes (selected), No

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 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 54:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Configure VDSL Controller Functionality

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



**Note** If your deployment includes devices with DSL, you must include DSL interface templates in Cisco vManage, even if these templates are not used.

Table 55:

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

Parameter Name	Description
Mode*	Select the operating mode of the VDSL controller from the drop-down: <ul style="list-style-type: none"> <li>• Auto—Default mode.</li> <li>• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.</li> <li>• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.</li> <li>• ADSL2+— Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.</li> <li>• ANSI—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.</li> <li>• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps..</li> </ul>
VDSL Modem Configuration	Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the Cisco vManage NMS. If the command is not valid, it is not executed.
SRA	Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

To save the feature template, click Save.

### Configure the Ethernet Interface on VDSL Controller

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

**Table 56:**

Parameter Name	Description
Ethernet Interface Name	Enter a name for the Ethernet interface, in the format <i>subslot/port</i> (for example 2/0). You do not need to enter the slot number, because it must always be 0.
VLAN ID	Enter the VLAN identifier of the Ethernet interface.
Description	Enter a description for the interface.
Dialer Pool Member	Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.
PPP Max Payload	Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. <i>Range:</i> 64 through 1792 bytes

Parameter Name	Description
Dialer IP	Configure the IP prefix of the dialer interface. This prefix is that of the node in the destination that the interface calls. <ul style="list-style-type: none"> <li>Negotiated—Use the address that is obtained during IPCP negotiation.</li> </ul>

To save the feature template, click Save.

### Configure the PPP Authentication Protocol

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

**Table 57:**

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: <ul style="list-style-type: none"> <li>CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters.</li> <li>PAP—Enter the username and password provided by your ISP. <i>username</i> can be up to 255 characters.</li> <li>PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</li> </ul>

To save the feature template, click Save.

### Create a Tunnel Interface

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

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

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

**Table 58:**

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection	If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.

Parameter Name	Description
Maximum Control Connections	Specify the maximum number of Cisco vSmart Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.  <i>Range: 0 through 8Default: 2</i>
Cisco vBond Orchestrator As STUN Server	Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco vSmart Controllers that the tunnel interface is not allowed to connect to. <i>Range: 0 through 100</i>
Cisco vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco vManage NMS. <i>Range: 0 through 8Default: 5</i>
Port Hop	Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <i>Default: Enabled</i>
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select On or Off for each service to allow or disallow the service on the interface.

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

**Table 59:**

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

Parameter Name	Description
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

### Configure the Interface as a NAT Device

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

**Table 60:**

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

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

**Table 61:**

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

To save a port forwarding rule, click Add.

To save the feature template, click Save.

### Apply Access Lists

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

**Table 62:**

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

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

To save the feature template, click Save.

### Configure Other Interface Properties

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

**Table 63:**

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

To save the feature template, click Save.

### Release Information

Introduced in Cisco vManage NMS in Release 18.3.



# VPN Interface Ethernet PPPoE


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

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

To configure interfaces on Cisco routers using Cisco vManage templates:

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

## Navigate to the Template Screen and Name the Template

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
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. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Ethernet PPPoE.
7. From the VPN Interface Ethernet PPPoE drop-down, click Create Template. The VPN Interface Ethernet PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Ethernet PPPoE parameters.  

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.

The screenshot shows the Cisco vManage interface for configuring a feature template. The breadcrumb trail is: Feature Template > Add Template > VPN Interface Ethernet PPPoE. The device type is set to ISR4331. The configuration is divided into tabs: Basic Configuration (selected), PPP, Tunnel, NAT, ACL/QoS, and Advanced. Under the Basic Configuration tab, several parameters are listed with their respective scope drop-down menus:

- Shutdown: Radio buttons for Yes (selected) and No.
- Ethernet Interface Name: A text input field with a scope drop-down menu.
- VLAN ID: A text input field with a scope drop-down menu.
- Description: A text input field with a scope drop-down menu.
- Dialer Pool Member: A text input field with a scope drop-down menu.
- PPP Maximum Payload: A text input field with a scope drop-down menu.

520023

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 64:**

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>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 <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

### Configure PPPoE Functionality

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

**Table 65:**

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

To save the feature template, click Save.

### Configure the PPP Authentication Protocol

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

**Table 66:**

Parameter Name	Description
PPP Authentication Protocol	Select the authentication protocol used by the MLP: <ul style="list-style-type: none"> <li>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters.</li> <li>• PAP—Enter the username and password provided by your ISP. <i>username</i> can be up to 255 characters.</li> <li>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</li> </ul>

To save the feature template, click Save.

### Create a Tunnel Interface

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

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

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

**Table 67:**

Parameter Name	Description
Tunnel Interface	Click On to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection	If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.
Maximum Control Connections	Specify the maximum number of Cisco vSmart Controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. <i>Range: 0 through 8Default: 2</i>
Cisco vBond Orchestrator As STUN Server	Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Controller Group List	Set the Cisco vSmart Controllers that the tunnel interface is not allowed to connect to. <i>Range: 0 through 100</i>
Cisco vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the Cisco vManage NMS. <i>Range: 0 through 8Default: 5</i>
Port Hop	Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <i>Default: Enabled</i>
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select On or Off for each service to allow or disallow the service on the interface.

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

Table 68:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. <i>Range:</i> 0 through 4294967295 <i>Default:</i> 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

### Configure the Interface as a NAT Device

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

Table 69:

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

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

Table 70:

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

To save a port forwarding rule, click Add.

To save the feature template, click Save.

### Apply Access Lists

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

Table 71:

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

To save the feature template, click Save.

### Configure Other Interface Properties

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

Table 72:

Parameter Name	Description
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
IP MTU	Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None

Parameter Name	Description
TLOC Extension	Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
IP Directed-Broadcast	Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

To save the feature template, click Save.

#### Release Information

Introduced in Cisco vManage NMS in Release 18.4.1.

## VPN Interface IPsec

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

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

## Create VPN IPsec Interface Template

- 
- Step 1** From the Cisco vManage menu, select **Configuration > Templates**.
  - Step 2** Click **Feature**.
  - Step 3** Click **Add Template**.
  - Step 4** Select a Cisco IOS XE SD-WAN device from the list.
  - Step 5** From the VPN section, click **VPN Interface IPsec**. The Cisco VPN Interface IPsec template displays.
  - Step 6** In 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 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.
-



## Basic Configuration

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

Parameter Name	Options/Format	Description
Shutdown*	Yes / No	Click <b>No</b> to enable the interface; click <b>Yes</b> to disable.
Interface Name*	ipsec number (1...255)	Enter the name of the IPsec interface. <i>Number</i> can be from 1 through 255.
Description	Enter a description of the IPsec interface.	
IPv4 Address*	ipv4-prefix/length	Enter the IPv4 address of the IPsec interface. The address must have a /30 subnet.
Source*	Set the source of the IPsec tunnel that is being used for IKE key exchange:	
	IP Address	Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in <b>VPN 0</b> .
	Interface	Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in <b>VPN 0</b> .
Destination*	Set the destination of the IPsec tunnel that is being used for IKE key exchange.	
	IPsec Destination IP Address	Enter an IPv4 address that points to the destination.
	TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.  <i>Range:</i> 552 to 1960 bytes  <i>Default:</i> None
	IP MTU	Specify the maximum transmission unit (MTU) size of packets on the interface.  <i>Range:</i> 576 through 2000  <i>Default:</i> 1500 bytes

### CLI Equivalent

```
crypto
  interface tunnel ifnum
    no shutdown
    vrf forwarding vrf_id
    ip address ip_address[mask]
    tunnel source wanif_ip
    tunnel mode {ipsec ipv4 | gre ip}
    tunnel destination gateway_ip
    tunnel protection ipsec profile ipsec_profile_name
```

## Configure Dead-Peer Detection

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

Parameter Name	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection.  Range: 10 through 3600 seconds  Default: Disabled
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.  Range: 2 through 60  Default: 3

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

### CLI Equivalent

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

## Configure IKE

Table 73: Feature History

Feature Name	Release Information	Description
SHA256 Support for IPsec Tunnels	Cisco IOS XE Release Amsterdam 17.2.1r	This feature adds support for HMAC_SHA256 algorithms for enhanced security.

To configure IKE, select the **IKE** tab and configure the following parameters:



#### Note

When you create an IPsec tunnel on a Cisco IOS XE SD-WAN device, IKE Version 1 is enabled by default on the tunnel interface.

### IKE Version 1 and IKE Version 2

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

Parameter Name	Options	Description
<b>IKE Version</b>	1 IKEv1 2 IKEv2	Enter <b>1</b> to select IKEv1. Enter <b>2</b> to select IKEv2. <i>Default:</i> IKEv1
<b>IKE Mode</b>	<b>Aggressive mode</b> <b>Main mode</b>	For IKEv1 only, specify one of the following modes: <ul style="list-style-type: none"> <li>• Aggressive mode - Negotiation is quicker, and the initiator and responder ID pass in the clear.</li> <li>• Establishes an IKE SA session before starting IPsec negotiations.</li> </ul> <p><b>Note</b> For IKEv2, there is no mode.</p> <p><i>Default:</i> Main mode</p>
<b>IPsec Rekey Interval</b>	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. <i>Range:</i> 1 hour through 14 days <i>Default:</i> 14400 seconds (4 hours)
<b>IKE Cipher Suite</b>	<b>3DES</b> <b>192-AES</b> <b>256-AES</b> <b>AES</b> <b>DES</b>	Specify the type of authentication and encryption to use during IKE key exchange. <i>Default:</i> 256-AES
<b>IKE Diffie-Hellman Group</b>	<b>2</b> <b>14</b> <b>15</b> <b>16</b>	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. <ul style="list-style-type: none"> <li>• 1024-bit modulus</li> <li>• 2048-bit modulus</li> <li>• 3072-bit modulus</li> <li>• 4096-bit modulus</li> </ul> <p><i>Default:</i> 4096-bit modulus</p>

Parameter Name	Options	Description
<b>IKE Authentication</b>	Configure IKE authentication.	
	<b>Preshared Key</b>	Enter the password to use with the preshared key.
	<b>IKE ID for Local End Point</b>	If the remote IKE peer requires a local end point identifier, specify it. <i>Range:</i> 1 through 64 characters <i>Default:</i> Tunnel's source IP address
	<b>IKE ID for Remote End Point</b>	If the remote IKE peer requires a remote end point identifier, specify it. <i>Range:</i> 1 through 64 characters <i>Default:</i> Tunnel's destination IP address

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

### Change the IKE Version from IKEv1 to IKEv2

To change the IKE version, do the following:

1. Select the **Basic Configuration** tab.
2. Use the **shutdown** parameter with the **yes** option (**yes shutdown**) to shut down the tunnel.
3. Remove the ISAKMP profile from the IPsec profile.
4. Attach the IKEv2 profile with the IPsec profile.



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

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



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

### CLI Equivalent for Changing the IKE Version



**Note** There is no single CLI for changing the IKE version. You need to follow the sequence of steps listed in the Change the IKE Version from IKEv1 to IKEv2 section.

### CLI Equivalents for IKEv1

#### ISAKMP CLI Configuration for IKEv1

```

crypto
  isakmp
    keepalive 60-86400 2-60 {on-demand | periodic}
    policy policy_num
      encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
      hash {sha384 | sha256 | sha}
      authentication pre-share
      group {2 | 14 | 16 | 19 | 20 | 21}
      lifetime 60-86400
    profile ikev1_profile_name
      match identity address ip_address [mask]
      keyring keyring_name

```

### IPsec CLI Configuration for IKEv1

```

profile ipsec_profile_name
  set transform-set transform_set_name
  set isakmp-profile ikev1_profile_name
  set security-association
    lifetime {kilobytes disable | seconds 120-2592000}
    replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
  set pfs group {14 | 16 | 19 | 20 | 21}
  keyring keyring_name
  pre-shared-key address ip_address [mask] key key_string
  ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
  esp-sha256-hmac] mode tunnel

```

### Summary Steps

1. enable
2. configure terminal
3. crypto isakmp policy *priority*
4. encryption {des | 3des | aes | aes 192 | aes 256 }
5. hash {sha | sha256 | sha384 | md5 }
6. authentication {rsa-sig | rsa-encr | pre-share }
7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

### CLI Equivalent for IKE2

```

crypto
  ikev2
    proposal proposal_name
      encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
      integrity {sha256 | sha384 | sha512}
      group {2 | 14 | 15 | 16}
    keyring ikev2_keyring_name
    peer peer_name
      address tunnel_dest_ip [mask]
      pre-shared-key key_string
    profile ikev2_profile_name

```

```

match identity remote address ip_address
authentication {remote | local} pre-share
keyring local ikev2_keyring_name
lifetime 120-86400

```

## Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

Parameter Name	Options	Description
<b>IPsec Rekey Interval</b>	3600 - 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
<b>IKE Replay Window</b>	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
<b>IPsec Cipher Suite</b>	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm
<b>Perfect Forward Secrecy</b>	<b>2</b> 1024-bit modulus <b>14</b> 2048-bit modulus <b>15</b> 3072-bit modulus <b>16</b> 4096-bit modulus <b>none</b>	Specify the PFS settings to use on the IPsec tunnel. Select one of the following Diffie-Hellman prime modulus groups: 1024-bit – group-2 2048-bit – group-14 3072-bit – group-15 4096-bit – group-16 none –disable PFS. <i>Default: group-16</i>

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

### CLI Equivalent

```

crypto
 ipsec
   profile ipsec_profile_name
     set ikev2-profile ikev2_profile_name
     set security-association
       lifetime {seconds 120-2592000 | kilobytes disable}
       replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}}
     set pfs group {2 | 14 | 15 | 16 | none}
     set transform-set transform_set_name

```

### Release Information

Introduced in Cisco vManage for Cisco IOS XE SD-WAN Release 16.11.x.

## VPN Interface Multilink

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



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

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

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

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

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage, select the **Configuration** > **Templattesscreen**.
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 multilink interface in the transport VPN (VPN 0):
  - a. Click the **Transport & Management VPN** tab located 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 Multilink Controller**.
6. If you are configuring the multilink interface 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, enter the number of the service VPN.
  - c. Under Additional VPN Templates, located to the right of the screen, click **VPN Interface Multilink Controller**.
7. From the **VPN Interface Multilink Controller** drop-down, click **Create Template**. The VPN Multilink template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining multilink Interface parameters.

The screenshot displays the Cisco vManage interface for configuring a feature template. The breadcrumb trail is: Feature Template > Add Template > VPN Interface Multilink. The 'Device Type' is set to 'ASR1001-HX'. The 'Template Name' and 'Description' fields are empty. The 'Basic Configuration' tab is selected, showing the following parameters:

- Shutdown:** A dropdown menu with a checkmark, and radio buttons for 'Yes' (selected) and 'No'.
- Interface Name:** A dropdown menu with a plus sign and a text field containing 'Multilink'.
- Description:** A dropdown menu with a checkmark and an empty text field.
- MultiLink Group Number:** A dropdown menu with a plus sign and an empty text field.

'Save' and 'Cancel' buttons are located at the bottom of the configuration area.

520035

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 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 74:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>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 .</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a> .</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>
Global (indicated by a globe icon)	<p>Enter a value for the parameter, and apply that value to all devices.</p> <p>Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</p>

### Configure a Multilink Interface

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



**Note** If you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

Table 75:

Parameter Name	Description
Shutdown*	Click <b>No</b> to enable the multilink interface.
Interface Name*	Enter the number of the MLP interface. It can be a number from 1 through 65,535.
Description	Enter a description for the multilink interface.
Multilink Group Number*	Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter.

Parameter Name	Description
IPv4 Address*	To configure a static address, click <b>Static</b> and enter an IPv4 address.  To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click <b>Dynamic</b> . You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.
IPv6 Address*	To configure a static address for an interface in VPN 0, click <b>Static</b> and enter an IPv6 address.  To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click <b>Dynamic</b> . You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
IP MTU	Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes

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

### Configure the PPP Authentication Protocol

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

**Table 76:**

Parameter Name	Description
Authentication Protocol	Select the authentication protocol used by the MLP: <ul style="list-style-type: none"> <li>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <i>hostname</i> can be up to 255 characters.</li> <li>• PAP—Enter the username and password provided by your ISP. <i>username</i> can be up to 255 characters.</li> <li>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click <b>Same Credentials</b> for PAP and CHAP.</li> </ul>

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

### Create a Tunnel Interface

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

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

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

**Table 77:**

Parameter Name	Description
Tunnel Interface	Click <b>On</b> to create a tunnel interface.
Color	Select a color for the TLOC.
Control Connection	If the router has multiple TLOCs, click <b>No</b> to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.
Maximum Control Connections	Specify the maximum number of Cisco vSmart Controller that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. <i>Range: 0 through 8Default: 2</i>
vBond As STUN Server	Click <b>On</b> to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the device is located behind a NAT.
Exclude Controller Group List	Set the Cisco vSmart Controller that the tunnel interface is not allowed to connect to. <i>Range: 0 through 100</i>
vManage Connection Preference	Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS. <i>Range: 0 through 8Default: 5</i>
Port Hop	Click <b>On</b> to enable port hopping, or click <b>Off</b> to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <i>Default: Enabled</i>
Low-Bandwidth Link	Select to characterize the tunnel interface as a low-bandwidth link.
Allow Service	Select <b>On</b> or <b>Off</b> for each service to allow or disallow the service on the interface.

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

Table 78:

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. <i>Range:</i> 0 through 4294967295 <i>Default:</i> 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit	Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

### 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 79:

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

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

### Configure Other Interface Properties

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

Table 80:

Parameter Name	Description
PMTU Discovery	Click <b>On</b> to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the Cisco 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. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
Clear Dont Fragment	Click <b>On</b> to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. <i>Range:</i> 0 through 7
Autonegotiate	Click <b>Off</b> to turn off autonegotiation. By default, an interface runs in autonegotiation mode.

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

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

### Release Information

Introduced in Cisco vManage in Release 18.3.

## Configure VPN Interface SVI using vManage

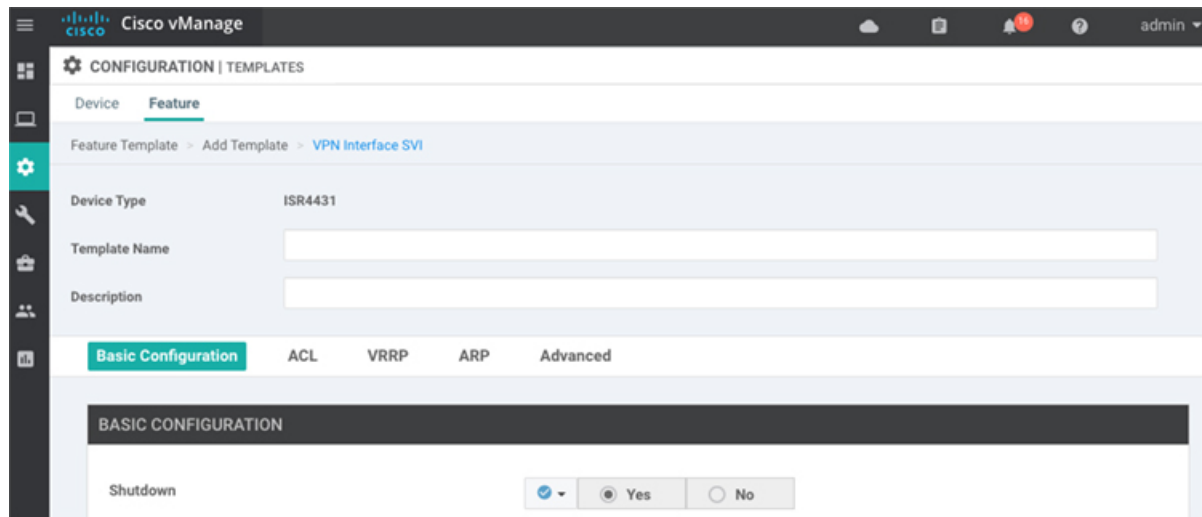
Use the VPN Interface SVI template to configure SVI for Cisco IOS XE SD-WAN devices. You configure a switch virtual interface (SVI) to configure a VLAN interface.

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.



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 81: Feature History*

Feature Name	Release Information	Description
Support for Configuring Secondary IP Address	Cisco IOS XE Release Amsterdam 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 82:

Parameter Name	Description
Shutdown*	Click <b>No</b> to enable the VLAN interface.
VLAN Interface Name*	Enter the VLAN identifier of the interface. <i>Range:</i> 1 through 1094.
Description	Enter a description for the interface.
IP MTU	Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1500. <i>Default:</i> 2000 bytes
IPv4* or IPv6	Click to configure one or more IPv4 or 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 <b>Add</b> 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 <b>Add</b> 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 83:

Parameter Name	Description
Ingress ACL – IPv4	Click <b>On</b> and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click <b>On</b> and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Ingress Policer	Click <b>On</b> and specify the name of the policer to apply to packets being received on the interface.
Egress Policer	Click <b>On</b> 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 84:**

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. <i>Range:</i> 1 through 255
Priority	Enter the priority level of the router. The router with the highest priority is elected as the primary router. If two Cisco IOS XE SD-WAN devices have the same priority, the one with the higher IP address is elected as the primary one. <i>Range:</i> 1 through 254 <i>Default:</i> 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. <i>Range:</i> 1 through 3600 seconds <i>Default:</i> 1 second
Track OMP Track Prefix List	By default, VRRP uses 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 <b>On</b> 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 85:

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 86:

Parameter Name	Description
TCP MSS	Specify the maximum segment size (MSS) of TCP 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. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. <i>Range:</i> 0 through 2678400 seconds (744 hours) <i>Default:</i> 1200 (20 minutes)

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

## VPN Interface T1/E1

Use the VPN Interface T1/E1 template for Cisco SD-WANs running the Cisco SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco vManage templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.
2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters.
3. Create a VPN feature template to configure VPN parameters.

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage, select the **Configuration** > **Templates** screen.
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:



**Note** **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.

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

6. To create a template for VPNs 1 through 511, and 513 through 65530:
  - a. Click the **Service VPN** tab 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 **VPN Interface**.

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

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

### Configure Basic Interface Functionality

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

**Table 87:**

Parameter Name	Description
Shutdown*	Click <b>No</b> to enable the interface.
Interface name*	Enter a name for the interface. The name should be in the format <b>serial slot / subslot / port : channel-group</b> .  You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.
Description	Enter a description for the interface.
IPv4 Address*	Enter an IPv4 address.
IPv6 Address*	Enter an IPv6 address.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
IP MTU	Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 1500 bytes

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

### Release Information

Introduced in Cisco vManage Release 18.2.

## T1/E1 Controller

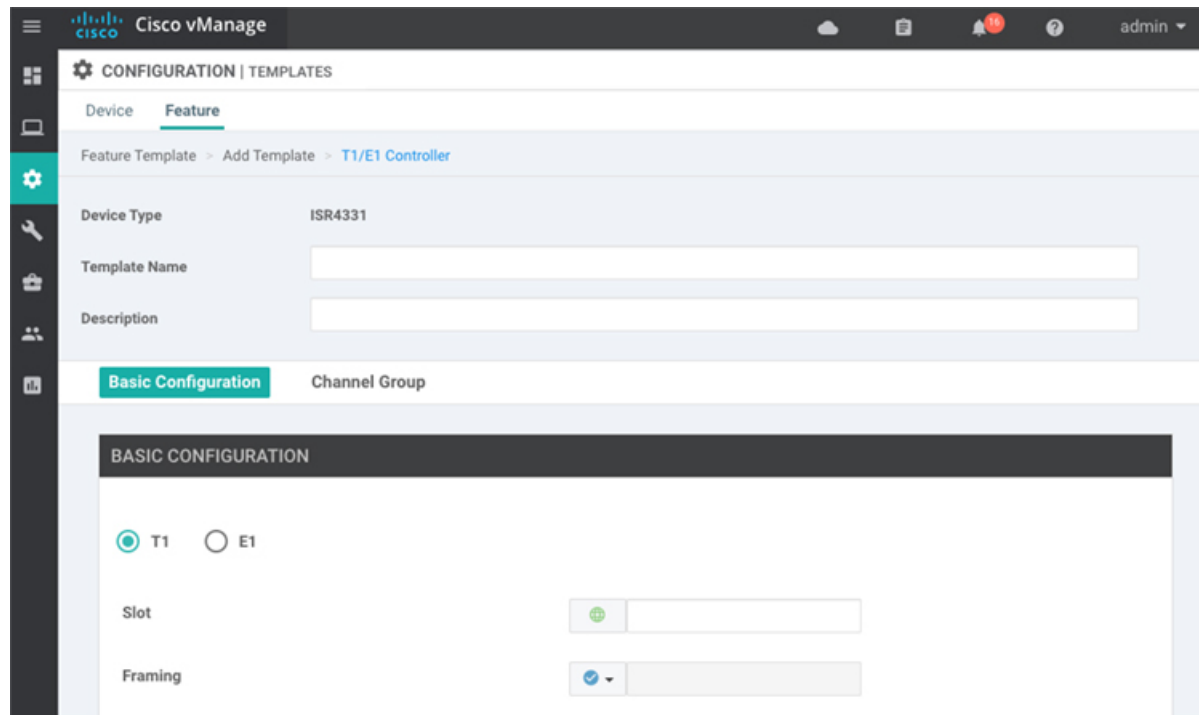
Use the T1/E1 Controller template for Cisco IOS XE SD-WAN devices running the Cisco SD-WAN software.

To configure the T1/E1 interfaces in a VPN using Cisco vManage templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters.
3. Create a VPN feature template to configure VPN parameters.

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage, select the Configuration ► Templates screen.
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 **VPN Interface**.
  - c. From the **VPN Interface** drop-down, click **Create Template**. The **VPN Interface T1/E1** template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet 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 **VPN Interface**.
  - d. From the **VPN Interface** drop-down, click **Create Template**. The **VPN Interface Ethernet** template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.



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.

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:

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

### Configure a T1 Controller

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

**Table 88:**

Parameter Name	Description
Slot*	Enter the number of the slot in which the T1 NIM is installed. <i>Range: 0 through 6</i>

Parameter Name	Description
Framing*	Enter the T1 frame type: <ul style="list-style-type: none"> <li>• <b>esf</b>—Send T1 frames as extended superframes. This is the default.</li> <li>• <b>sf</b>—Send T1 frames as superframes. Superframing is sometimes called D4 framing.</li> </ul>
Line Code	Select the line encoding to use to send T1 frames: <ul style="list-style-type: none"> <li>• <b>ami</b>—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.</li> <li>• <b>b8zs</b>—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes</li> </ul>
Clock Source	Select the clock source: <ul style="list-style-type: none"> <li>• <b>internal</b>—Use the controller framer as the primary clock.</li> <li>• <b>line</b>—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.</li> </ul>
Line Mode	If you choose the Line clock source, select whether the line is a primary or a secondary line.
Description	Enter a description for the controller.
Channel Group	Enter the number of the channel group. If you do so, you must enter a time slot in the Time Slot field. <i>Range:</i> 0 through 30
Time Slot	Enter the time slot or time slots that are part of the channel group. <i>Range:</i> 1 through 24
Cable Length	Select the cable length to configure the attenuation <ul style="list-style-type: none"> <li>• <b>long</b>—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer than 660 feet.</li> <li>• <b>short</b>—Set the transmission attenuation for cables that are 660 feet or shorter.</li> </ul> <p>There is no default length.</p>

Parameter Name	Description
Length	<p>If you specify a value in the <b>Cable Length Field</b>, enter the length of the cable.</p> <p>For short cables, the length values can be:</p> <ul style="list-style-type: none"> <li>• 110—Length from 0 through 110 feet</li> <li>• 220—Length from 111 through 220 feet</li> <li>• 330—Length from 221 through 330 feet</li> <li>• 440—Length from 331 through 440 feet</li> <li>• 550—Length from 441 through 550 feet</li> <li>• 660—Length from 551 through 660 feet</li> </ul> <p>For long cables, the length values can be:</p> <ul style="list-style-type: none"> <li>• 0 dB</li> <li>• -7.5 dB</li> <li>• -15 dB</li> <li>• -22.5 dB</li> </ul>

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

### Configure an E1 Controller

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

**Table 89:**

Parameter Name	Description
Slot*	<p>Enter the number of the slot in which the E1 NIM is installed.</p> <p><i>Range:</i> 0 through 6</p>
Framing*	<p>Enter the E1 frame type:</p> <ul style="list-style-type: none"> <li>• <b>crc4</b>—Use cyclic redundancy check 4 (CRC4). This is the default.</li> <li>• <b>no-crc4</b>—Do not use CRC4.</li> </ul>
Line Code*	<p>Select the line encoding to use to send E1 frames:</p> <ul style="list-style-type: none"> <li>• <b>ami</b>—Use alternate mark inversion (AMI) as the linecode.</li> <li>• <b>hdb3</b>—Use high-density bipolar 3 as the linecode. This is the default.</li> </ul>



Parameter Name	Description
Clock Source	Select the clock source: <ul style="list-style-type: none"> <li>• internal—Use the controller framer as the primary clock.</li> <li>• line—Use phase-locked loop (PLL) on the interface. This is the default.</li> </ul>
Line Mode	If you choose the Line clock source, select whether the line is a primary or secondary line. If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line.
Description	Enter a description for the controller.
Channel Group	To configure the serial WAN on the E1 interface, enter a channel group number. <i>Range:</i> 0 through 30
Time Slot	For a channel group, configure the timeslot. <i>Range:</i> 1 through 31

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

#### Release Information

Introduced in Cisco vManage Release 18.1.1.

## Cellular Interfaces

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

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

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

## Configure Cellular Interfaces Using vManage

To configure cellular interfaces using vManage templates:

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



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

### Create VPN Interface Cellular

1. In vManage NMS, select the **Configuration** > **Templates** screen.
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. Click the **Transport & Management VPN** tab or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, click **VPN Interface Cellular**.

The screenshot shows the Cisco vManage interface for creating a template. The breadcrumb is 'Feature Template > Add Template > VPN Interface Cellular'. The 'Device Type' is 'ISR4331'. There are input fields for 'Template Name' and 'Description'. Below these are tabs for 'Basic Configuration', 'Tunnel', 'NAT', 'ACL', 'ARP', and 'Advanced'. The 'Basic Configuration' tab is active, showing fields for 'Shutdown' (Yes/No), 'Interface Name', and 'Description'.

7. From the **VPN Interface Cellular** drop-down, click **Create Template**. The VPN Interface Cellular template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Cellular parameters.
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 first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field.

### Configure Basic Cellular Interface Functionality

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

**Table 90:**

Parameter Name	Description
Shutdown*	Click <b>No</b> to enable the interface.
Technology	Cellular technology. The default is <b>lte</b> . Other values are <b>auto</b> and <b>cdma</b> . For ZTP to work, the technology must be <b>auto</b> .
Interface Name*	Enter the name of the interface. It must be <b>cellular0</b> .
Profile ID*	Enter the identification number of the cellular profile. This is the profile identifier that you configure in the Cellular-Profile template. <i>Range:</i> 1 through 15
Description	Enter a description of the cellular interface.
IPv4 Configuration	To configure a static address, click <b>Static</b> and enter an IPv4 address.  To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click <b>Dynamic</b> . You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.
IPv6 Configuration	To configure a static address for an interface in VPN 0, click <b>Static</b> and enter an IPv6 address.  To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click <b>Dynamic</b> . You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.
DHCP Helper	Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.
Block Non-Source IP	Click <b>Yes</b> to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.
Bandwidth Upstream	For transmitted traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps
Bandwidth Downstream	For received traffic, set the bandwidth above which to generate notifications. <i>Range:</i> 1 through $(2^{32} / 2) - 1$ kbps

Parameter Name	Description
IP MTU*	Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value.

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

*CLI equivalent:*

### Create a Tunnel Interface

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

To configure a tunnel interface, select the Tunnel tab, set Tunnel Interface to On, and configure the following parameters. Parameters marked with an asterisk are required to configure a cellular interface.

**Table 91:**

Parameter Name	Description
Tunnel Interface*	Click On to create a tunnel interface.
Color*	Select a color for the TLOC. The color typically used for cellular interface tunnels is <b>lte</b> .
Control Connection	The default is On, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click No to have a tunnel not establish a TLOC.
Maximum Control Connections	Set the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. <i>Range:</i> 0 through 8 Default: 2
vBond As STUN Server	Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.
Exclude Control Group List	Set the identifiers of one or more vSmart controller groups that this tunnel is not allowed to establish control connections with. <i>Range:</i> 0 through 100
vManage Connection Preference	Set the preference for using the tunnel to exchange control traffic with the vManage NMS. <i>Range:</i> 0 through 9 Default: 5
Low-Bandwidth Link	Click On to set the tunnel interface as a low-bandwidth link. Default: Off

Parameter Name	Description
Allow Service	Click On or Off for each service to allow or disallow the service on the cellular interface.

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

**Table 92:**

Parameter Name	Description
GRE	Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec	Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference	Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. <i>Range:</i> 0 through 4294967295 <i>Default:</i> 0
IPsec Weight	Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. <i>Range:</i> 1 through 255 <i>Default:</i> 1
Carrier	Select the carrier name or private network identifier to associate with the tunnel. <i>Values:</i> carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default <i>Default:</i> default
Bind Loopback Tunnel	Enter the name of a physical interface to bind to a loopback interface. The interface name has the format <b>ge slot/port</b> .
Last-Resort Circuit	Use the tunnel interface as the circuit of last resort
NAT Refresh Interval	Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 1 through 60 seconds <i>Default:</i> 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <i>Range:</i> 100 through 10000 milliseconds <i>Default:</i> 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. <i>Range:</i> 12 through 60 seconds <i>Default:</i> 12 seconds

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

*CLI equivalent:*

### Configure the Cellular Interface as a NAT Device

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

**Table 93: Configure the Cellular Interface as a NAT Device**

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

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

**Table 94:**

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

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

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

*CLI equivalent:*

### Apply Access Lists

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

**Table 95: Access Lists Parameters**

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

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

*CLI equivalent:*

### 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 96:**

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**.

*CLI equivalent:*

### Configure Other Interface Properties

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

**Table 97: Cellular Interfaces Advanced Parameters**

Parameter Name	Description
PMTU Discovery	Click <b>On</b> to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS	Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
Clear-Don't-Fragment	Click <b>On</b> to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS	Select a queue number to use for incoming traffic. <i>Range:</i> 0 through 7
ARP Timeout	Specify how long it takes for a dynamically learned ARP entry to time out. <i>Range:</i> 0 through 2678400 seconds (744 hours) <i>Default:</i> 1200 seconds (20 minutes)
Autonegotiate	Click <b>Off</b> to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension	Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.
Tracker	Enter the name of a tracker to track the status of transport interfaces that connect to the internet.
ICMP Redirect	Click <b>Disable</b> to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.

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

*CLI equivalent:*

### Release Information

Introduced in vManage NMS in Release 16.1. In Release 16.2, add circuit of last resort and its associated hold time. In Release 16.3, add support for IPv6. In Release 17.2.2, add support for tracker interface status. In Release 18.2, add support for disabling ICMP redirect messages.



## Configure Cellular Interfaces Using CLI

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

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

## Low-bandwidth Link Optimization

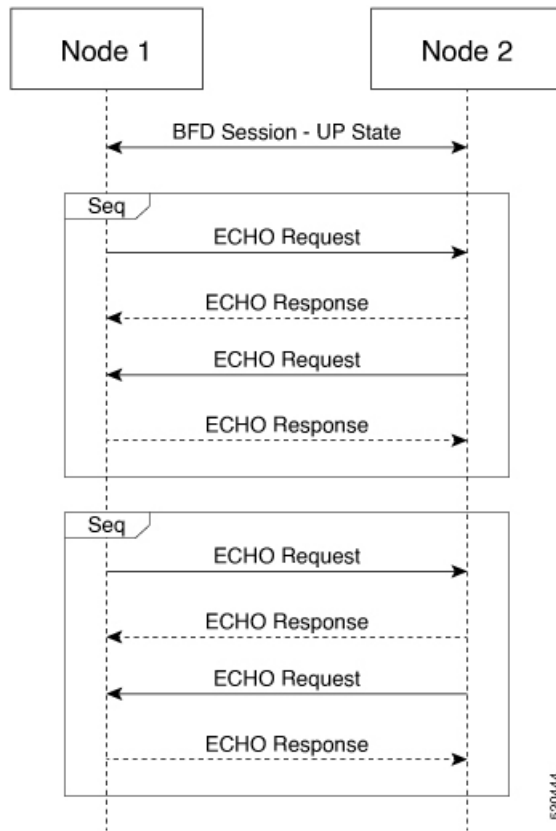
For low-bandwidth links, such as LTE cellular links, that are part of the overlay network, SD-WAN can reduce the amount of bandwidth used for control plane traffic. This can be helpful to reduce charges for cellular traffic, and to leave more bandwidth available for data traffic.

### BFD Fault Detection Uses Bandwidth

Bidirectional Forwarding Detection (BFD) is a network protocol that detects faults in the ability to forward traffic between two nodes in a network. The fault detection that BFD provides is a valuable component of routing management.

BFD operates by establishing sessions between nodes in a network that carry data traffic. These sessions use a handshake procedure to monitor connectivity. This produces a significant amount of control plane traffic.

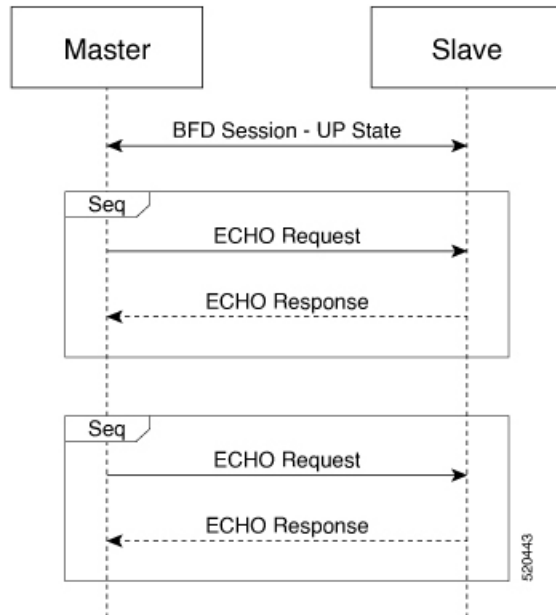
In the BFD “asynchronous mode” handshake procedure, the two nodes in a BFD session send ECHO requests to each other periodically. If no response is received after a request, a node considers the link to be down and reports this. Parameters such as transmission timer (Hello interval) and detection timer govern this mode.



### Low Bandwidth Link Option Reduces Traffic

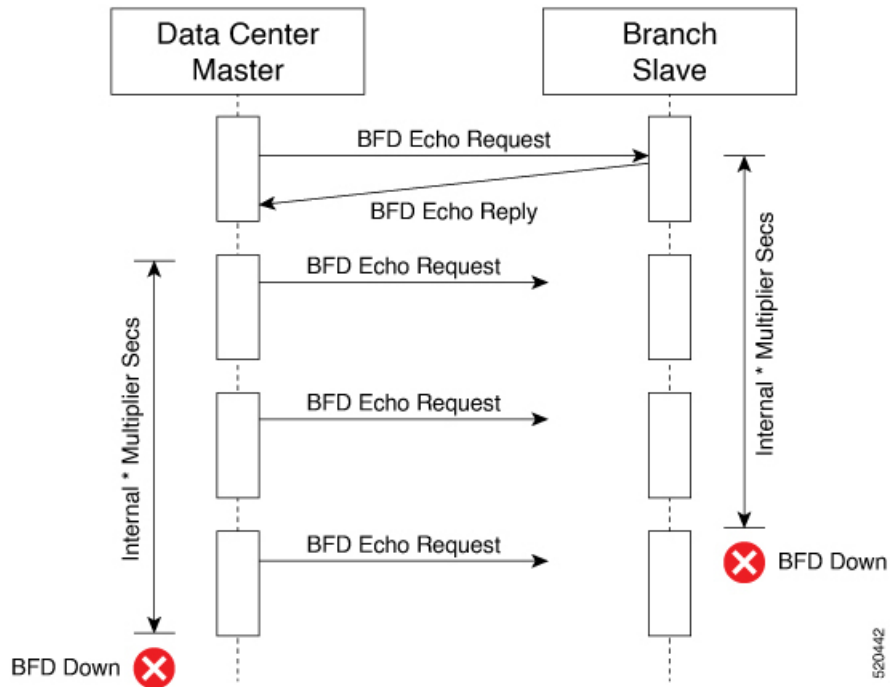
For low-bandwidth links, it is worthwhile to reduce this control traffic, while preserving BFD functionality. Using the low-bandwidth-link option reduces the BFD handshake traffic by almost half.

With this option enabled, BFD designates one node within a BFD session as primary node and the other node as subordinate node. The primary node continues to send ECHO requests and listen for responses, as usual. The subordinate node does not send ECHO requests, but sends responses to requests.

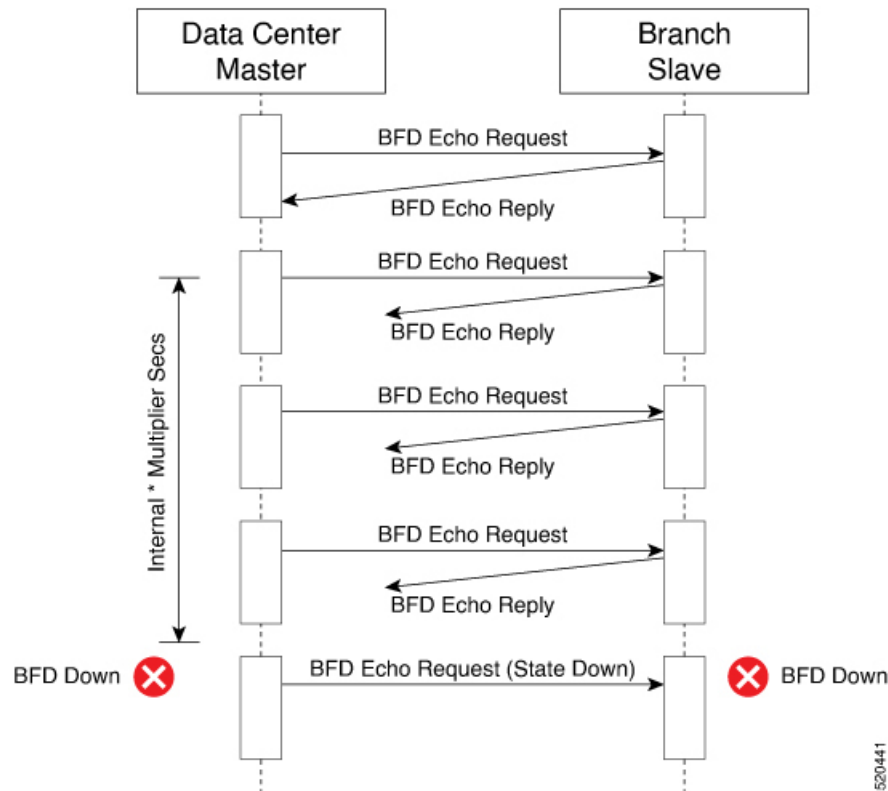


If the primary node sends an ECHO request and does not receive a response, the reason may be that either one of the following:

- Transmission of the request failed.



- Transmission of the response failed.



The primary node does not need to distinguish between these possibilities. If the primary node does not receive a response within a specified detection time, it determines that the link between the nodes is down and sends a State Down message to the subordinate node.

### Connection Statistics in Low-bandwidth-link Mode

With the low bandwidth link option, SD-WAN uses a streamlined logic to measure packet loss, latency, and jitter.

Statistic	Mechanism in low-bandwidth-link mode
Packet loss	<p>BFD uses two mechanisms together to track packet loss.</p> <ul style="list-style-type: none"> <li>When the primary node fails to receive a response to an ECHO request, it sends a “Last Lost” message in its next ECHO request. When the subordinate node receives this, it increments its count of lost packets.</li> <li>When the subordinate node fails to receive an ECHO request for longer than a configured interval, it concludes that the ECHO request was lost, and increments its count of lost packets.</li> </ul> <p>Combining these two enables SD-WAN to measure packet loss.</p>
Latency	The primary node measures the round-trip latency between sending an ECHO request and receiving a response.
Jitter	The primary node measures the variability of latency over time.

Using this primary/subordinate hierarchical model, and the logic described above, SD-WAN can collect connection statistics using less control plane traffic.

### Interoperability: Cisco vEdge and Cisco XE SD-WAN Devices

A network may include Cisco vEdge and Cisco XE SD-WAN devices. Low-bandwidth-link mode operates on both classes of devices, and the two types of devices can operate together in a BFD session.

### Configuring Low-Bandwidth Link

It is possible to use the low-bandwidth link option when configuring any interface that allows tunneling. When configuring interfaces using vManage, the low-bandwidth link appears as an option in the Tunnel section of WAN feature templates, such as VPN Interface Cellular or VPN Interface PPP.

## WiFi Radio

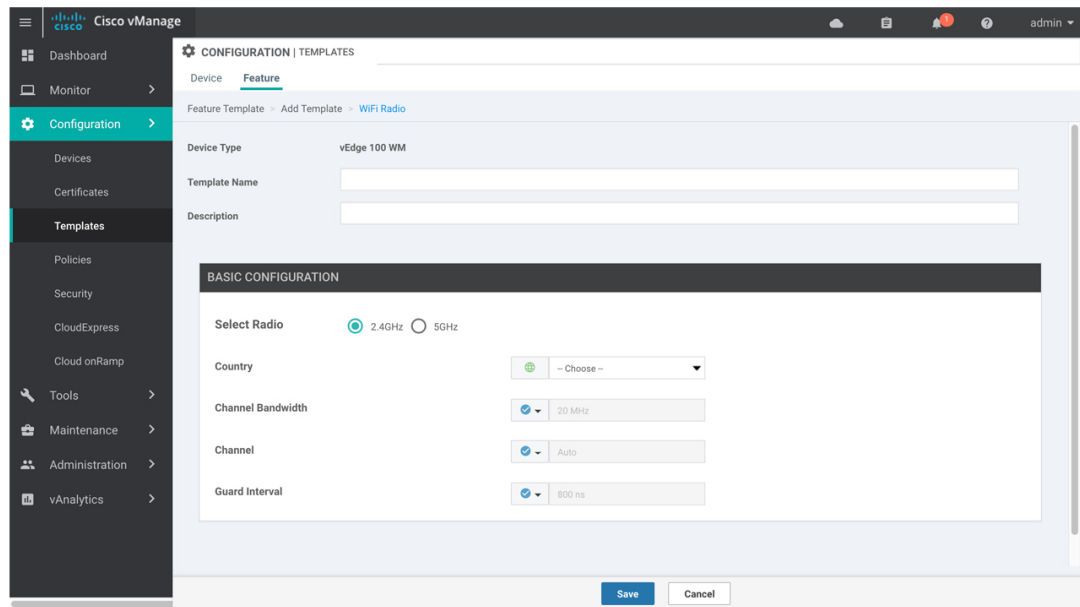
Use the WiFi Radio template for all devices that support wireless LANs (WLANs).

To configure WLAN radio parameters using Cisco vManage templates:

1. Create a WiFi Radio template to configure WLAN radio parameters, as described in this article.
2. Create a Wifi SSID template to configure an SSID and related parameters.

### Create WLAN Feature Template

1. In Cisco vManage, select the **Configuration** > **Templattesscreen**.
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 device model that supports wireless LANs (WLANs).
5. Click the **WLAN** tab, or scroll to the WLAN section.
6. From the **WiFi Radio** drop-down, click **Create Template**. The **WiFi Radio** template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining WiFi Radio parameters.



369440

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.

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

### Configure the WLAN Radio Frequency

To configure the WLAN radio frequency, in the **Basic Configuration** tab, configure the following parameters. Parameters marked with an asterisk are required to configure the radio.

**Table 98:**

Parameter Name	Description
Select Radio*	Select the radio band. It can be 2.4 GHz or 5 GHz.
Country*	Select the country where the router is installed.
Channel Bandwidth	Select the IEEE 802.11n and 802.11ac channel bandwidth. For a 5-GHz radio band, the default value is 80 MHz, and for 2.4 GHz, the default is 20 MHz.
Channel	Select the radio channel. The default is "auto", which automatically selects the best channel. For 5-GHz radio bands, you can configure dynamic frequency selection (DFS) channels.
Guard Interval	Select the guard interval. For a 5-GHz radio band, the default value is the short guard interval (SGI) of 400 ns, and for 2.4 GHz, the default is 800 ns.

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

### Release Information

Introduced in vManage NMS Release 16.3.

## WiFi SSID

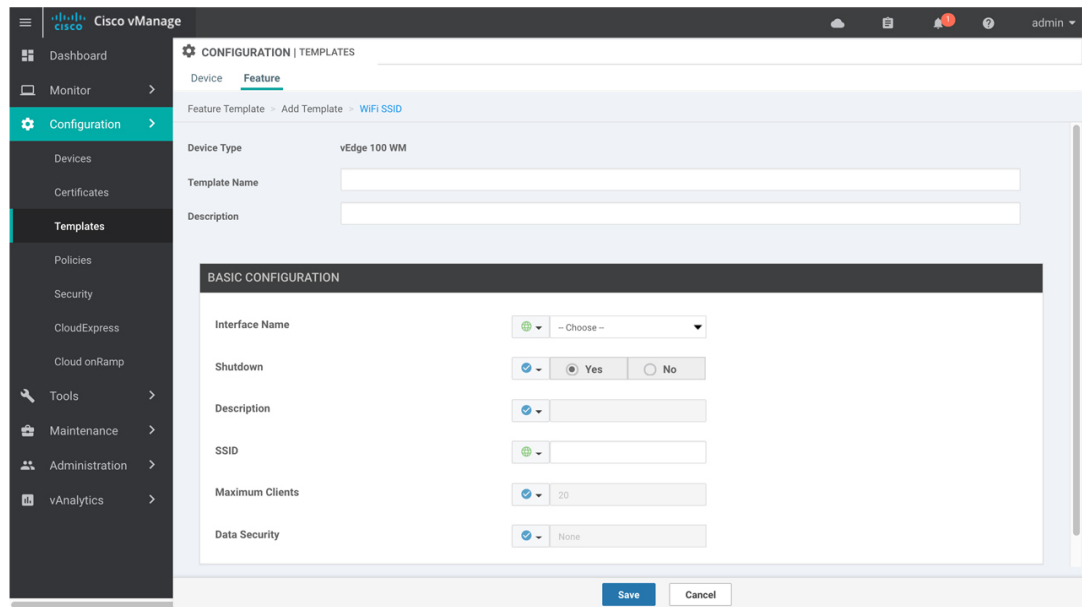
You can use the WiFi SSID template for all devices that support wireless LANs (WLANs)

To configure SSIDs on the WLAN radio using vManage templates:

1. Create a WiFi SSID template to configure the VAP interfaces to use as SSIDs, as described in this article.
2. Create a WiFi Radio template to configure WLAN radio parameters.
3. Create a Bridge template to assign the VAP interface to a bridging domain.
4. Create a device template that incorporates the WiFi Radio feature template and the Wifi SSID feature template.

### Navigate to the Template Screen and Name the Template

1. In Cisco vManage, select the Configuration ► Templates screen.
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 a device that supports wireless LANs (WLANs).
5. Click the WLAN tab located directly beneath the Description field, or scroll to the WLAN section.
6. Under Additional WiFi Radio Templates, located to the right of the screen, click **WiFi SSID**.



369441

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

### WLAN SSID Configuration

To configure SSIDs on a device, configure the following parameters in the **Basic Configuration** tab. Parameters marked with an asterisk are required to configure the SSIDs.

**Table 99:**

Parameter Name	Description
Interface Name*	Select the VAP interface name.
Shutdown*	Click <b>No</b> to enable the interface.
Description (optional)	Enter a description for the interface.



Parameter Name	Description
SSID*	<p>Enter the name of the SSID. It can be a string from 4 through 32 characters. The SSID must be unique.</p> <p>You can configure up to four SSIDs.</p> <p>Each SSID is called a virtual access point (VAP) interface. To a client, each VAP interfaces appears as a different access point (AP) with its own SSID. To provide access to different networks, assign each VAP to a different VLAN.</p>
Maximum Clients	<p>Enter the maximum number of clients allowed to connect to the WLAN. <i>Range:</i> 1 through 50 <i>Default:</i> 25</p>
Data Security	<p>Select the security type to enable user authentication or enterprise WPA security.</p> <p>For user authentication, select from WPA Personal, WPA/WPA2 Personal, or WPA2 Personal, and then enter a clear text or an AES-encrypted key.</p> <p>For enterprise security, select from WPA Enterprise, WPA/WPA2 Enterprise, or WPA2 Enterprise, and then enter a RADIUS server tag.</p>
RADIUS Server	<p>If you select one of the enterprise security methods based on using a RADIUS authentication server, enter the RADIUS server tag.</p>
WPA Personal Key	<p>If you select one of the personal security methods based on preshared keys, enter either a clear text or an AES-encrypted password.</p>
Management Security	<p>If you select one of the WPA2 security methods, select the encryption of management frames to be none, optional, or required.</p>

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

### Release Information

Introduced in Cisco vManage Release 16.3.





## CHAPTER 6

# IPv6 Functionality

This chapter describes the options for enabling IPv6 functionality for Cisco SD-WAN templates and policies. Use the information in this chapter if your deployment uses IPv6.

### Configure IPv6 Functionality for an Interface or Subinterface Template

To configure IPv6 functionality for an interface or subinterface template, perform the following steps.

Cisco SD-WAN supports dual stack: you can configure IPv4 and IPv6 in the same deployment. You can configure up to three global IPv6 addresses per interface.

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button and configure the parameters that the following table describes.

Parameter Name	Description
Static	This radio button is selected by default because IPv6 addresses are static.
IPv6 Address	Enter the IPv6 address of the interface or subinterface.

*CLI equivalent:*

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

### Configure IPv6 Functionality for an OMP Template

To configure IPv6 functionality for an Overlay Management Protocol (OMP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **OMP** from the list of templates.

4. In the Basic Configuration area, click the **IPv6** button in the ADVERTISE area and configure the parameters that the following table describes.

Parameter Name	Description
Connected	Click <b>Off</b> to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.
Static	Click <b>Off</b> to disable advertising static routes to OMP. By default static routes are advertised to OMP.
BGP	Click <b>On</b> to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.

*CLI equivalent:*

First enable Service VRF for IPv6:

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

Next enable OMP.

OMP supports global IPv6 configuration. In addition, per VRF level configuration is allowed. Per VRF level configuration overrides global configuration.

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
  advertise bgp
  advertise connected

  address-family ipv6 vrf 1
  advertise static
```

Global configuration is the default configuration, so IPv6 is enabled by default for OMP. To disable IPv6 OMP route redistribution for a particular VRF, configure the redistribution protocol to no as follows:

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
  advertise bgp
  advertise connected

  address-family ipv6 vrf 1
  no advertise connected
  no advertise static
  no advertise bgp
```

### Configure IPv6 Functionality for a BGP Template

To configure IPv6 functionality for a Border Gateway Protocol (BGP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **BGP** from the list of templates.
4. In the Unicast Address Family area, click the **IPv6** button and configure the parameters that the following table describes.

Tab	Parameter Name	Description
	Maximum Paths	Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing. <i>Range:</i> 0 to 32
	Address Family	Enter the BGP IPv6 unicast address family.
RE-DISTRIBUTE		Click the <b>Redistribute</b> tab, and then click <b>Add New Redistribute</b> .
	Protocol	Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following: <ul style="list-style-type: none"> <li>• For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.</li> <li>• 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.</li> </ul>
	Route Policy	Enter the name of the route policy to apply to redistributed routes.
		Click <b>Add</b> to save the redistribution information.
NETWORK		Click the <b>Network</b> tab, and then click <b>Add New Network</b> .
	Network Prefix	Enter a network prefix, in the format of <i>prefix/length</i> , to be advertised by BGP.
		Click <b>Add</b> to save the network prefix.
AGGREGATE ADDRESS		Click the <b>Aggregate Address</b> tab, and then click <b>Add New Aggregate Address</b> .
	Aggregate Prefix	Enter the prefix of the addresses to aggregate for all BGP sessions, in the format <i>prefix/length</i> .
	AS Set Path	Click <b>On</b> to generate set path information for the aggregated prefixes.
	Summary Only	Click <b>On</b> to filter out more specific routes from BGP updates.
		Click <b>Add</b> to save the aggregate address.

1. In the Neighbor area, click the **IPv6** button, create a new neighbor or edit an existing one, and then configure the parameters that the following table describes.

Parameters marked with an asterisk are required.

Parameter Name	Description
IPv6 Address*	Specify the IPv6 address of the BGP neighbor.
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Address Family	Select <b>Global</b> from the drop-down list, click <b>On</b> and select the address family. Enter the address family information.
Shutdown	To shut down a BGP neighbor when you push the template, select <b>Global</b> from the drop-down list and then click <b>Yes</b> . <i>Default: Off</i>

*CLI equivalent:*

```
config-transaction
router bgp 1
  bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

### Configure IPv6 Functionality for a VRRP Template

To configure IPv6 functionality for a Virtual Router Redundancy Protocol (VRRP) template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the VRRP area, click the **IPv6** button and then click **New VRRP**.
5. Configure the parameters that the following table describes.

Parameter Name	Description
Group ID	Enter a virtual router ID, which represents a group of routers. Range: 1 through 255
Priority	Enter the priority level of the router within a VRRP group. <ul style="list-style-type: none"> <li>• <i>Range:</i> 1 through 254</li> <li>• <i>Default:</i> 100</li> </ul>

Parameter Name	Description
Timer	Not used.
Track OMP	Select On to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router. <i>Default: Off</i>
Track Prefix List	Enter a value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy.
Link Local IPv6 Address	Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Global IPv6 Address	Enter a virtual global unicast IPv6 address, which represents the global address of the group. The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. For example, 2001::2/124.  You can configure up to 3 global IPv6 addresses.

*CLI equivalent:*

```

config-transaction
interface GigabitEthernet1

    vrrp 10 address-family ipv6
        priority 20
        track omp shutdown
        address FE80::10:100:1 primary
        address 2001:10:100::1/64

Prefix-list tracking
track 1 ipv6 route 1:1::1/128
    reachability
    ipv6 vrf 1

track 2 ipv6 route 2:2::2/128
    reachability
    ipv6 vrf 2

track 20 list boolean or
    object 1
    object 2

vrrp 10 address-family ipv6
    track 20 shutdown

```

**Configure IPv6 Functionality for an SNMP Template**

To configure IPv6 functionality for an SNMP template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **SNMP** from the list of templates.

4. In the SNMP Version area, click the **SNMP Version** button ► **TRAP TARGET SERVER** and create or edit an SNMP trap target.

1. Configure the parameters that the following table describes.

Parameter Name	Description
VPN ID	Enter the number of the VPN to use to reach the trap server. <i>Range:</i> 0 through 65530
IP Address	Enter the IP address of the SNMP server.
UDP Port	Enter the UDP port number for connecting to the SNMP server. <i>Range:</i> 1 though 65535
Trap Group Name	Select the name of a trap group that was configured under the Group tab.
User Name	Select the name of a community that was configured under the Community tab.
Source Interface	Enter the interface to use to send traps to the SNMP server that is receiving the trap information.



**Note** Make sure that you have already configured the SNMP community and trap target group.

*CLI equivalent:*

The following example permits any SNMP to access all objects with read-only permission using the community string named public. The device also will send Border Gateway Protocol(BGP) traps IPv6 host 3ffe:b00:c18:1::3/127 using SNMP v1. The community string named public will be sent with the traps.

```
Device# config-transaction
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

In the following example, the SNMP context A is associated with the views in SNMPv2c group GROUP1 and the IPv6 named access list public2:

```
Device# config-transaction
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list comm AVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify access
ipv6 public2
```

The following example configures the IPv6 host as the notification server:

```
Device> enable
Device# config-transaction
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group publicv2c access ipv6 public2
Device(config)# snmp-server hosthost1.com2c vrf trap-vrf
Device(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6
```



```
public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```

### Configure IPv6 Functionality for a DHCP Relay Agent Template

To configure IPv6 functionality for a DHCP Relay Agent template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button.
5. Click **Add** next to DHCP Helper.
6. Configure the parameters that the following table describes.

*Table 100:*

Parameter Name	Description
DHCPv6 Helper #	IP address of the DHCP helper
DHCPv6 Helper VPN	VPN ID of the VPN source interface for the DHCP helper.

*CLI equivalent:*

```
device-configuration
interface GigabitEthernet8
  vrf forwarding 2
  no ip address
  ipv6 address 2001:A14:99::F/64
  ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

### Configure IPv6 Functionality for an ACL Template or a QoS Template

To configure IPv6 functionality for an ACL and QoS template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► **Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the ACL/QoS area, configure the parameters that the following table describes.

Parameter Name	Description
Ingress ACL – IPv6	Click <b>on</b> to enable the IPv6 ingress access list.
IPv6 Ingress Access List	Enter the name of the IPv6 ingress access list.
Egress ACL – IPv6	Click <b>on</b> to enable the IPv6 egress access list.

Parameter Name	Description
IPv6 Egress Access List	Enter the name of the IPv6 egress access list.

*CLI Equivalent for Configuring IPv6 Functionality for an ACL Template:*

```

Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)# sequence 11
Device(config-sequence-11)# match
Device(config-match)# source-ip 2001:380:1::64/128
Device(config-match)# destination-ip 2001:3c0:1::64/128
Device(config-match)# source-port 4000
Device(config-match)# destination-port 3000
Device(config-match)# traffic-class 6
Device(config-match)# next-header 6
Device(config-match)# packet-length 1000
Device(config-match)# action accept
Device(config-action)#

Device(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
Device(config-interface-GigabitEthernet6)#
Device(config-interface-GigabitEthernet6)#

Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv_ipv6_prefix
Device(config-access-list-ipv_ipv6_prefix)# sequence 11
Device(config-sequence-11)# match
Device(config-match)# source-data-prefix-list data-ipv6-prefix-list
Device(config-match)# destination-data-prefix-list source_ipv6_list
Device(config-match)# destination-ip 2001:3c0:1::64/128
Device(config-match)# source-port 4000
Device(config-match)# destination-port 3000
Device(config-match)# traffic-class 6
Device(config-match)# next-header 6
Device(config-match)# packet-length 1000
Device(config-match)# !
Device(config-match)# action accept

```

*CLI Equivalent for Configuring IPv6 Functionality for a QoS Template:*

```

Device(config)# class-map match-any class0
Device(config-cmap)# match qos-group 0
Device(config-cmap)# class-map match-any class1
Device(config-cmap)# match qos-group 1
Device(config-cmap)# !
Device(config-cmap)# policy-map qos_map_for_data_policy
Device(config-pmap)# class class0
Device(config-pmap-c)# bandwidth percent 10
Device(config-pmap-c)# random-detect
Device(config-pmap-c)# class class1
Device(config-pmap-c)# bandwidth percent 10
Device(config-pmap-c)# random-detect
Device(config-pmap-c)#
Device(config-pmap-c)# policy
Device(config-policy)# no app-visibility
Device(config-policy)# class-map
Device(config-class-map)# class class0 queue 0
Device(config-class-map)# class class1 queue 1

```

```

Device(config-class-map)# !
Device(config-class-map)# ipv6
Device(config-ipv6)# access-list fwd_class_data_policy
Device(config-access-list-fwd_class_data_policy)# sequence 5
Device(config-sequence-5)# match
Device(config-match)# traffic-class 0
Device(config-match)# !
Device(config-match)# action accept
Device(config-action)# count fwd_class_data_policycnt_5
Device(config-action)# class class0
Device(config-action)# !
Device(config-action)# !
Device(config-action)# sequence 6
Device(config-sequence-6)# match
Device(config-match)# traffic-class 1
Device(config-match)# !
Device(config-match)# action accept
Device(config-action)# count fwd_class_data_policycnt_6
Device(config-action)# class class1
Device(config-action)# !
Device(config-action)# !
Device(config-action)# !
Device(config-action)# default-action drop

class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
bandwidth percent 10
random-detect
class class1
bandwidth percent 10
random-detect

policy
no app-visibility
class-map
class class0 queue 0
class class1 queue 1
!
ipv6
access-list fwd_class_data_policy
sequence 5
match
traffic-class 0
!
action accept
count fwd_class_data_policycnt_5
class class0
!
sequence 6
match
traffic-class 1
!
action accept
count fwd_class_data_policycnt_6
class class1
!
default-action drop

```

### Configure IPv6 Functionality for a Logging Template

To configure IPv6 functionality for a Logging template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **Logging** from the list of templates.
4. In the Server area, click the **IPv6** button.
5. Configure the parameters that the following table describes.

Parameter Name	Description
IPv6 Hostname/IPv6 Address	Host name or IP address of the server to direct the logging information.
VPN ID	VPN ID of the VPN source interface.
Source Interface	Name of the source interface.
Priority	Choose the maximum severity of messages that are logged.

*CLI equivalent:*

```
config-transaction
Device(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```

### Configure IPv6 Functionality for a New Prefix List

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration ► Policies**.
2. From the Custom Options drop-down menu, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Prefix** from the list on the left and then select **New Prefix List**.
4. Select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

*CLI equivalent:*

```
config-transaction
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)# sequence 11
Device(config-sequence-11)# match
Device(config-match)# source-ip 2001:380:1::64/128
Device(config-match)# destination-ip 2001:3c0:1::64/128
```

### Configure IPv6 Functionality for a Data Prefix

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration ► Policies**.

2. From the Custom Options drop-down menu, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.
4. In the Internet Protocol area, select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

*CLI equivalent:*

```
Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64
```

### Configure IPv6 Functionality for a Centralized Policy

To configure a centralized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select **Configuration ► Policies**.
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select the **Traffic Data** tab.
4. Select Add Policy ► Create New.
5. Click the **Sequence Type** button and then select **Traffic Engineering**.
6. Click the **Sequence Rule** button.
7. From the Protocol drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.
8. Click the **Sequence Type** button and then select **QoS**.
9. Click the **Sequence Rule** button.
10. From the Protocol drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

*CLI equivalent:*

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                ipv6-prefix-list ipv6-1
                ipv6-prefix 1::1/128
```

### Configure IPv6 Functionality for a Localized Policy

To configure a localized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select **Configuration ► Policies**.
2. From the Custom Options drop-down menu, select **Access Control Lists** under Localized Policy.
3. Click the **Add Access Control List Policy** button and choose **Add IPv6 ACL Policy**. The policy you create will apply only to IPv6 address families.

*CLI equivalent:*

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
config-transaction
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```



## CHAPTER 7

# IP Directed Broadcast

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached are broadcast on that subnet.



**Note** The access control list (ACL) option for directed broadcast is not supported in vManage.

To enable the translation of a directed broadcast to physical broadcasts, use the `ip directed-broadcast` command. To disable this function, use the `no` form of this command. By default, `ip directed-broadcast` is disabled and all IP directed broadcasts are dropped.

### **ip directed-broadcast** and **no ip directed-broadcast**

#### **Example**

This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

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







## CHAPTER 8

# CLI Templates for Cisco XE SD-WAN Routers

The CLI Templates for Cisco XE SD-WAN Routers features allows you to configure intent-based CLI templates for Cisco XE SD-WAN routers using vManage. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, vManage enables pushing vEdge syntax-based commands to Cisco XE SD-WAN Routers in Cisco IOS XE Syntax.

Using vManage CLI templates significantly reduces the effort to configure feature templates.

### Benefits of CLI Templates

- You can reuse any Cisco vEdge-specific vManage feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, vManage displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SDWAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

### Configuring CLI Templates in vManage

1. In vManage, select Configuration ► Templates.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select CLI Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. 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.

- 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.
- The configuration of the CLI template must be intent-based. You can upload a configuration file using the Select a File field or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```

system

  host-name {{hostname}}
  system-ip {{system_ip}}
  domain-id 1

  site-id {{site_id}}
  port-offset      1
  admin-tech-on-failure
  organization-name "XYZ"
  logging
  disk
  enable
!!

```

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

- To save the feature template, click Add.



**Note** See the Attach Devices to a Device Template section in this topic to know more about attaching a device to a template and reusing a template for multiple devices of the same device model.

## Sample Configurations for CLI Template

### System Level Configuration

**Table 101: System Level Parameters**

CLI Template Configuration	Configuration on the Device
<pre> system  host-name pm4  system-ip 172.16.255.14  overlay-id 1  site-id 400  control-session-pps 300  admin-tech-on-failure  sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346 </pre>	<pre> system  host-name  pm4 system-ip  172.16.255.14 overlay-id  1 site-id 400 control-session-pps 300 admin-tech-on-failure sp-organization-name "XYZ Inc Regression" organization-name "XYZ Inc Regression" console-baud-rate 11520 vbond 10.0.12.26 port 12346 </pre>

**AAA Configuration - Authentication, authorization, and accounting (AAA) with RADIUS and TACACS+**

**Table 102: AAA Configuration**

CLI Template Configuration	Configuration on the Device
<pre> aaa auth- order local radius tacacs usergroup basic  task system read write task interface read write !  usergroup netadmin !  usergroup operator task system read task interface read task policy read task routing read task security read ! user admin password  \$6\$nbblkA==\$ae/DO78l/wluPUohhBU2L6h/ Q.PLkurGvxjRlS9OWB9iTTfWsgNQcABV6F MW57vuEHvo3zp3qdYVinLmMIu/p/ secret \$9\$3/IL3/UF2F2F3E\$J9NBeklWrc9EmHk6F5AidMOfQD.QPAmDkz.c  ! ! radius  server 10.99.144.200 source-interface GigabitEthernet0/0/1 exit server 10.99.144.201  source-interface GigabitEthernet0/1/0 exit ! tacacs  server 10.0.1.1 auth-port 50  vpn 0  source-interface GigabitEthernet0/0/1  key 1  secret-key \$8\$Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrPcg=  exit ! ! </pre>	<pre> aaa group server tacacs+ server-10.0.1.1 server-private 10.0.1.1 timeout 5 key \$8\$vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=  ip tacacs source-interface GigabitEthernet0/0/1 ! aaa group server radius server-10.99.144.200  server-private 10.99.144.200 auth-port 1812 timeout 5 retransmit 3 ip radius source-interface GigabitEthernet0/0/1 !  aaa group server radius server-10.99.144.201  server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit 3 ip radius source-interface GigabitEthernet0/1/0 ! aaa authentication login default local group radius group tacacs+ aaa authorization exec default local group radius group tacacs+ a aa session-id common --- added by default  username admin privilege 15 secret 9 \$9\$3/IL3/UF2F2F3E\$J9NBeklWrc9EmHk6F5AidMOfQD.QPAmDkz.c </pre>

**Logging configuration - Configures logging to either the local hard drive or a remote host****Table 103: Logging Configuration**

CLI Template Configuration	Configuration on the Device
<pre>logging   disk     enable     file size 12     file rotate 6   !   server 192.168.13.1     vpn          0     source-interface Loopback1     priority      alert   exit   !</pre>	<pre>logging   disk     enable   !   ! logging persistent size 75497472 filesize 12582912   logging buffered 512000 --- added by default  logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent</pre>

**Switch Port and VLAN configuration****Table 104: Switch Port Configuration**

CLI Template Configuration	Configuration on the Device
<pre>interface GigabitEthernet0/1/4   switchport   mode trunk   access vlan vlan 10   access vlan name "DHCP Vlan"   trunk allowed vlan 10   !   no shutdown  vpn 10   name "DHCP VPN"   interface Vlan10     description "Vlan 10 Mgmt interface"     ip address 10.29.35.1/24     no shutdown   !   !</pre>	<pre>interface GigabitEthernet0/1/4   switchport ios-sw:mode trunk   switchport ios-sw:trunk allowed vlan 10   no shutdown   no ip address   exit  interface Vlan10   description Vlan 10 Mgmt interface   no shutdown   arp timeout 1200   vrf forwarding 10   ip address 10.29.35.1 255.255.255.0   ip mtu 1500   exit</pre>

## Cellular Configuration

**Table 105: Cellular Configuration - Configures cellular controllers and cellular interfaces**

CLI Template Configuration	Configuration on the Device
<pre> vpn 0  interface Cellular0/2/0    description "Cellular interface"    no shutdown  !   controller cellular 0/2/0    lte sim max-retry 1    lte failovertimer 7    profile id 1 apn Broadband  ! </pre>	<pre> interface Cellular0/2/0  description Cellular interface  no shutdown  ip address negotiated  ip mtu 1428  mtu          1500  exit   controller Cellular 0/2/0    lte sim max-retry 1    lte failovertimer 7    profile id 1 apn Broadband authentication  none pdn-type ipv4 </pre>

**BGP, OSPF, and EIGRP - Configures BGP, OSPF, and EIGRP Routing Protocols under Transport or Service VPN**

*Table 106: BGP, OSPF, and EIGRP Configuration*

CLI Template Configuration	Configuration on the Device
----------------------------	-----------------------------

CLI Template Configuration	Configuration on the Device
<pre> vpn1   bgp 2     shutdown     distance external 30     distance internal 250     distance local 10     address-family ipv4-unicast       network 10.0.100.0/24       redistribute static route-policy     route_map       redistribute connected route-policy     route_map       !       neighbor 10.0.100.1       no shutdown       remote-as 3       timers         keepalive 12         holdtime 20         connect-retry 300         advertisement-interval 123       !       update-source GigabitEthernet0/0/1       ebgp-multihop 1       password       \$8\$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=       address-family ipv4-unicast  vpn 1   router   ospf     router-id 172.16.255.15     compatible rfc1583     timers spf 200 1000 10000     redistribute connected route-policy   route_map     max-metric router-lsa administrative     area 23     stub     interface GigabitEthernet0/0/1       cost 23       authentication type message-digest       authentication authentication-key key1      exit   exit   !  vpn 1   router   eigrp 1     af-interface GigabitEthernet0/0/2     no split-horizon     exit-af-interface   !   address-family ipv4 network 10.1.10.1/32   address-family ipv4 topology base   redistribute omp   exit-af-topology </pre>	

CLI Template Configuration	Configuration on the Device
	<pre> router bgp 2   bgp log-neighbor-changes   distance bgp 30 250 10   address-family ipv4 unicast vrf 1     neighbor 10.0.100.1 remote-as 3     neighbor 10.0.100.1 activate     neighbor 10.0.100.1 ebgp-multihop 1     neighbor 10.0.100.1 maximum-prefix 2147483647 100     neighbor 10.0.100.1 password 0 password     neighbor 10.0.100.1 send-community both     neighbor 10.0.100.1 timers 12 20     neighbor 10.0.100.1 update-source GigabitEthernet0/0/1   network 10.0.100.0 mask 255.255.255.0   redistribute connected   redistribute static route-map route_map   exit-address-family ! timers bgp 60 180  router ospf 1 vrf 1   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-area 110   distance ospf intra-area 110   redistribute connected subnets route-map route_map ! 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 ! router eigrp eigrp-name   address-family ipv4 vrf 1 autonomous-system 1   af-interface GigabitEthernet0/0/2   hello-interval 5   hold-time 15   no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0   topology base   redistribute omp   exit-af-topology ! exit-address-family </pre>



CLI Template Configuration	Configuration on the Device
	! !

**VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces**

*Table 107: VPN, Interface, and Tunnel Configuration*

CLI Template Configuration	Configuration on the Device
<pre> vpn 0  interface GigabitEthernet0/2/0   ip address 10.1.14.14/24   tunnel-interface   encapsulation ipsec   color lte   no allow-service bgp   allow-service dhcp   allow-service dns   allow-service icmp   no allow-service sshd   no allow-service netconf   no allow-service ntp   no allow-service ospf   no allow-service stun   allow-service https   !   autonegotiate   no shutdown   !   ip route 0.0.0.0/0 10.1.14.13  vpn 512  interface GigabitEthernet0   ip dhcp-client  ipv6 dhcp-client autonegotiate  no shutdown  ! ! </pre>	<pre> ip route 0.0.0.0 0.0.0.0 10.1.14.13 1  interface GigabitEthernet0/2/0  no shutdown  arp timeout 1200 - added by default  ip address 10.1.14.14 255.255.255.0  ip redirects --&gt; added by default  ip mtu 1500  mtu 1500  negotiation auto --&gt; added by default  exit  interface Tunnel120 ---&gt; based on the interface 0/2/0  no shutdown  ip unnumbered GigabitEthernet0/2/0  no ip redirects  ipv6 unnumbered GigabitEthernet0/2/0  no ipv6 redirects  tunnel source GigabitEthernet0/2/0  tunnel mode sdwan  sdwan  interface GigabitEthernet0/2/0   tunnel-interface   encapsulation ipsec weight 1   color lte   no last-resort-circuit   vmanage-connection-preference 5   no allow-service all   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  interface GigabitEthernet0  no shutdown  arp timeout 1200  vrf forwarding Mgmt-intf  ip address dhcp client-id GigabitEthernet0 ip  redirects  ip dhcp client default-router distance 1 ip  mtu 1500  mtu 1500  negotiation auto </pre>

### Network Address Translation (NAT) over Direct Internet Access (DIA)

Table 108: NAT over DIA

CLI Template Configuration	Configuration on the Device
<pre> vpn 201  interface GigabitEthernet0/0/2.2901   description giga21   ip address 10.201.201.1/24   mtu 1496   no shutdown   vrrp 100    track-omp     ipv4 10.201.201.3   !   !   !   dhcp-server    address-pool 10.201.201.0/24    exclude 10.201.201.1-10.201.201.10 10.201.201.20-10.201.201.22    offer-time 600    lease-time 86400    admin-state up    options     default-gateway 10.201.201.1     dns-servers 10.99.139.201     tftp-servers 10.99.139.201   !   !   !  ip route 0.0.0.0/0 vpn 0   ! vpn 0  interface GigabitEthernet0/0/0   ip address 172.16.10.1/24   nat    udp-timeout 3    tcp-timeout 40    respond-to-ping   !   ! </pre>	<pre> interface GigabitEthernet0/0/2.2901  no shutdown  encapsulation dot1Q 2901  vrf forwarding 201  ip address 10.201.201.1 255.255.255.0  ip mtu 1496  vrrp 100 address-family ipv4   vrrpv2    address 10.201.201.3    priority 100   track omp shutdown  exit  exit  ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901  option 150 ip 10.99.139.201  vrf 201  lease 1 0 0  default-router 10.201.201.1  dns-server 10.99.139.201  network 10.201.201.0 255.255.255.0  exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote  ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload  ip nat translation tcp-timeout 40  ip nat translation udp-timeout 3  ip nat route vrf 201 0.0.0.0 0.0.0.0 global  interface GigabitEthernet1/0/2  no shutdown  arp timeout 1200  ip address 10.1.15.15 255.255.255.0  ip nat outside  ip redirects  ip mtu 1500  mtu 1500  negotiation auto </pre>

## NAT64 Configuration

**Table 109: NAT64 Configuration**

<pre> vpn 1  nat64   v4 pool pool1 start-address 10.1.1.10   v4 pool pool1 end-address 10.1.1.100  !  interface GigabitEthernet3   ip address 10.1.19.15/24   nat64   !   autonegotiate   no shutdown  !         </pre>	<pre> interface GigabitEthernet3  no shutdown  arp timeout 1200  vrf forwarding 1  ip address 10.1.19.15 255.255.255.0  negotiation auto  nat64 enable  nat64 prefix stateful 2001::F/64 vrf 1   nat64 v4 pool pool1 10.1.1.10 10.1.1.100  nat64 v6v4 list global-list pool pool1 vrf  1  nat64 translation timeout tcp 60  nat64 translation timeout udp 1         </pre>
---	--

## Multilink and T1/E1 - Configures T1/E1 Controller and Serial, Multilink Interfaces

**Table 110: Configuring Multilink**

CLI Template Configuration	Configuration on the Device
<pre> card type t1 0 2  controller T1 0/2/0   framing esf   clock source internal   linecode b8zs   cablelength long 0db   channel-group 1 timeslots 15   channel-group 2 timeslots 12   channel-group 3 timeslots 10   channel-group 4 timeslots 10  !  interface Multilink1   no shutdown   encapsulation ppp   ip address 10.1.10.30 255.255.255.0   ppp pap sent-username admin password admin   ppp authentication pap   ppp multilink   ppp multilink links minimum 1   ppp multilink fragment disable   ppp multilink group 1  exit  interface Serial0/2/0:1   no shutdown   encapsulation ppp   bandwidth 1536   no ip address   load-interval 30   ppp pap sent-username admin password admin   ppp authentication pap   ppp multilink   ppp multilink group 1  exit         </pre>	<pre> interface Multilink1  ip address 10.1.10.30/24 shutdown  controller T1 0/2/0   linecode b8zs   channel-group 1   channel-group 3  !  ppp pap sent-username admin password admin  ppp authentication pap  ppp multilink  ppp multilink group 1         </pre>

**Local QoS Policy**

*Table 111: Local QoS Policy*

CLI Template Configuration	Configuration on the Device
----------------------------	-----------------------------

CLI Template Configuration	Configuration on the Device
<pre> vpn 1  interface GigabitEthernet0/0/1    ip address 10.2.54.15/24    no shutdown    access-list MyACL in    ! policy  class-map  class best-effort queue 3  class bulk-data queue 2  class critical-data queue 1  class voice queue 0  ! access-list MyACL  sequence 10  match   dscp 46   !  action accept   class voice   !  !  sequence 20  match   source-ip      10.1.1.0/24   destination-ip 192.168.10.0/24   !  action accept   class bulk-data   set    dscp 32   !  !  !  sequence 30  match   destination-ip 192.168.20.0/24   !  action accept   class critical-data   set    dscp 22   !  !  !  sequence 40  action accept   class best-effort   set    dscp 0   !  !  !  default-action accept  ! qos-scheduler be-scheduler  class      best-effort  bandwidth-percent 20  buffer-percent 20  drops      red-drop  ! qos-scheduler bulk-scheduler </pre>	<pre> interface GigabitEthernet0/0/1  access-list MyACL in  exit class-map match-any best-effort  match qos-group 3  ! class-map match-any bulk-data  match qos-group 2  ! class-map match-any critical-data  match qos-group 1  ! class-map match-any voice  match qos-group 0  ! policy-map MyQoSMap  class best-effort   random-detect   bandwidth percent 20  !  class bulk-data   random-detect   bandwidth percent 20  !  class critical-data   random-detect   bandwidth percent 40  !  class voice   priority percent 20  !  ! policy  no app-visibility  no flow-visibility  no implicit-acl-logging  log-frequency      1000  class-map  class best-effort queue 3  class bulk-data queue 2  class critical-data queue 1  class voice queue 0  ! access-list MyACL  sequence 10  match   dscp 46   !  action accept   class voice   !  !  !  sequence 20  match   source-ip      10.1.1.0/24   destination-ip 192.168.10.0/24   !  action accept   class bulk-data   set    dscp 32   !  ! </pre>

CLI Template Configuration	Configuration on the Device
<pre> class          bulk-data bandwidth-percent 20 buffer-percent 20 drops          red-drop ! qos-scheduler critical-scheduler class          critical-data bandwidth-percent 40 buffer-percent 40 drops          red-drop ! qos-scheduler voice-scheduler class          voice bandwidth-percent 20 buffer-percent 20 scheduling    llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! ! </pre>	<pre> ! ! sequence 30 match   destination-ip 192.168.20.0/24 ! action accept class critical-data set   dscp 22 ! ! ! sequence 40 action accept class best-effort set   dscp 0 ! ! ! default-action accept ! ! ! ! </pre>

## Security Policy (ZBFW, IPS/IDS, URL-Filtering) Configuration

**Table 112: Security Policy (ZBFW, IPS/IDS, URL-Filtering)**

CLI Template Configuration	Configuration on the Device
<pre> policy   zone internet     vpn 0     !   zone zone1     vpn 1     !   zone zone2     vpn 2     !   zone-pair ZP_zone1_internet_fw_policy     source-zone      zone1     destination-zone internet     zone-policy      fw_policy     !   zone-pair ZP_zone1_zone2_fw_policy     source-zone      zone1     destination-zone zone2     zone-policy      fw_policy     !   zone-based-policy fw_policy     sequence 1     match       source-data-prefix-list subnet1       !     action inspect     !     !     default-action pass     !   zone-to-nozone-internet deny   lists     data-prefix-list subnet1     ip-prefix 10.0.10.0/24     !     !   url-filtering url_filter     web-category-action block     web-categories      games     block-threshold     moderate-risk     block text     "&lt;![CDATA[&amp;lt;h3&amp;gt;Access" to the requested     page has been denied]]&gt;"     target-vpns         1     !   intrusion-prevention intrusion_policy     security-level     connectivity     inspection-mode     protection     log-level          err     target-vpns        1     !   failure-mode         open   !   !   ! </pre>	

CLI Template Configuration	Configuration on the Device
	<pre> ip access-list extended fw_policy-seq-1-acl_     11 permit object-group fw_policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl 10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_     match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy     class fw_policy-seq-1-cm_         inspect ! class class-default     pass ! ! object-group service fw_policy-seq-1-service-og_     ip ! parameter-map type inspect-global     alert on     log dropped-packets     multi-tenancy     vpn zone security ! parameter-map type umbrella global     token A5EA676087BF66A42DC4F722C2AFD10D00256274     dnscrypt     vrf 1         dns-resolver                umbrella         match-local-domain-to-bypass ! ! zone security internet     vpn 0 ! zone security zone1     vpn 1 ! zone security zone2     vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet     service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2     service-policy type inspect fw_policy ! app-hosting appid utd app-resource package-profile cloud-low app-vnic gateway0 virtualportgroup 0 </pre>



CLI Template Configuration	Configuration on the Device
	<pre> guest-interface 0   guest-ipaddress 192.168.1.2 netmask   255.255.255.252 !   app-vnic gateway1 virtualportgroup 1 guest-interface 1   guest-ipaddress 192.0.2.2 netmask   255.255.255.252 !   start !   utd multi-tenancy   utd engine standard multi-tenancy   web-filter block page profile block-url_filter   text &lt;!\[CDATA[&amp;lt;h3&amp;gt;Access to the   requested page has been   denied&amp;lt;/h3&amp;gt;&amp;lt;p&amp;gt;Please contact your   Network Administrator&amp;lt;/p&amp;gt;]]&gt; !   web-filter url profile url_filter   categories block   games !   block page-profile block-url_filter   log level error   reputation   block-threshold moderate-risk ! ! threat-inspection profile intrusion_policy    threat protection   policy connectivity   logging level err !   utd global !   policy utd-policy-vrf-1   all-interfaces   vrf 1   threat-inspection profile intrusion_policy    web-filter url profile url_filter exit ! </pre>

## Configuring NTP

**Table 113: Configuring NTP**

CLI Template Configuration	Configuration on the Device
<pre>ntp   server 10.29.43.1     source-interface GigabitEthernet1     version 4   exit ! !</pre>	<pre>ntp server 198.51.241.229 source GigabitEthernet1 version 4</pre>

## IPv6 Configuration

**Table 114: IPv6 Configuration**

CLI Template Configuration	Configuration on the Device
<pre>vpn 1   interface GigabitEthernet3     ipv6 address 2671:123A::1/128     shutdown   !   !</pre>	<pre>interface GigabitEthernet3   shutdown   arp timeout 1200   vrf forwarding 1   no ip address   ip redirects   ip mtu 1500   ipv6 address 2671:123A::1/128   ipv6 redirects   mtu 1500   negotiation auto   exit vrf definition 1   rd 1:1   address-family ipv4     exit-address-family   !   address-family ipv6     exit-address-family   !   !</pre>