CISCO VALIDATED DESIGN

Cisco SD-WAN Deployment Guide

October 2018

CISCO VALIDATED DESIGN

Table of Contents

Introduction

The Cisco® SD-WAN solution is an enterprise-grade WAN architecture overlay that enables digital and cloud transformation for enterprises. It fully integrates routing, security, centralized policy, and orchestration into large-scale networks. It is multi-tenant, cloud-delivered, highly-automated, secure, scalable, and application-aware with rich analytics. The Cisco SD-WAN technology addresses the problems and challenges of common WAN deployments.

This guide describes a Cisco SD-WAN network implementation showcasing some deployment models and features commonly used by organizations. The guide is not meant to exhaustively cover all options. It does highlight best practices and assists with a successful configuration and deployment of a Cisco SD-WAN network.

The implementation includes one data center with two Cisco vEdge 5000 routers and five remote sites as a mix of Cisco vEdge 1000 and 100 routers. The data center brownfield deployment described enables connectivity to the non-SD-WAN sites through the data center during the migration from WAN to SD-WAN. Greenfield remote site deployments are described, although the configuration concepts are also useful in brownfield deployments.

Prerequisites to starting deployment:

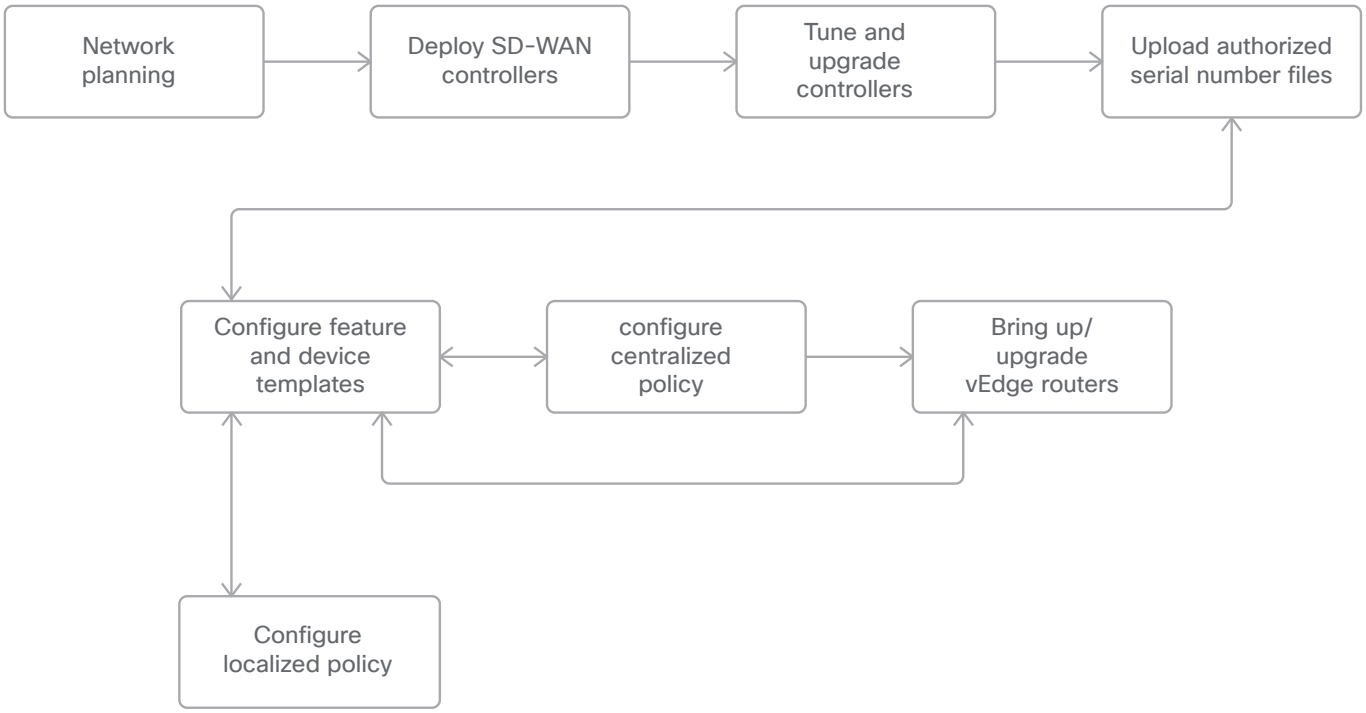
- Cisco vEdge routers are installed and ready to configure.
- Devices adjacent to the Cisco vEdge routers are configured.
- SD-WAN controllers are set up and deployed with the Cisco cloud-managed service.
- The Cisco SD-WAN solution and its associated concepts are understood, although no deployment experience is required. See the SD-WAN Design Guide for background information on the SD-WAN solution.

Refer to Appendix A for the hardware models and software versions used in this deployment guide. Refer to Appendix D for portions of the supporting network device configurations. Refer to Appendices E and F for summaries of the configurations for the vEdge devices.

Deployment overview

In order to have a fully functional overlay, there are a number of steps that need to be taken. The following image illustrates one example workflow.

Figure 1. Deployment flow chart



1. Network planning – Plan out device placement, system IP addresses, and site IDs; plan vEdge device configurations and policies and code versions; and plan out supporting device configurations, including any firewall ports that need opening to accommodate vEdge communication. Put together a detailed migration plan.
2. Deploy SD-WAN controllers – The vManage, vSmart controllers, and the vBond orchestrators should be deployed, certificates should be installed, and the controllers should be authenticated to each other. This paper assumes a cloud-managed service deployment, so this step is already covered.
3. Tune and upgrade controllers – The SD-WAN controller status can be verified and optionally tuned for common, best-practice configurations. The controllers can be upgraded if need be.
4. Upload the authorized serial number file – The authorized serial number file, which contains the serial and chassis numbers for all of the vEdge routers that are authorized to be in the network, should be uploaded to vManage. Once uploaded in vManage, the file is distributed to the vBond and vSmart controllers.
5. Configure feature and device templates – Configure feature templates and device templates and attach them to the vEdge devices, supplying variables to parameter values as necessary. vManage builds the full configurations and pushes them out to the vEdge devices. It is recommended to deploy the data centers before deploying the branches.

6. Configure localized policy – Configure any localized policy and attach the policy to the targeted device templates. Note that if the device template is already attached to vEdge devices, you need to attach a localized policy first, before making any policy references within the feature templates.
7. Configure centralized policy – Configure any centralized policies with vManage, which will be downloaded to the vSmart controllers in the network.
8. Bring up/upgrade vEdge routers – Bring up the vEdge routers in order to establish control connections to the vBond, vSmart, and vManage devices. This is accomplished either through a bootstrap configuration or through the Zero-Touch Provisioning (ZTP) process. In addition, upgrade the vEdge routers if necessary, which can be performed through the vManage GUI or automatically during the ZTP process.

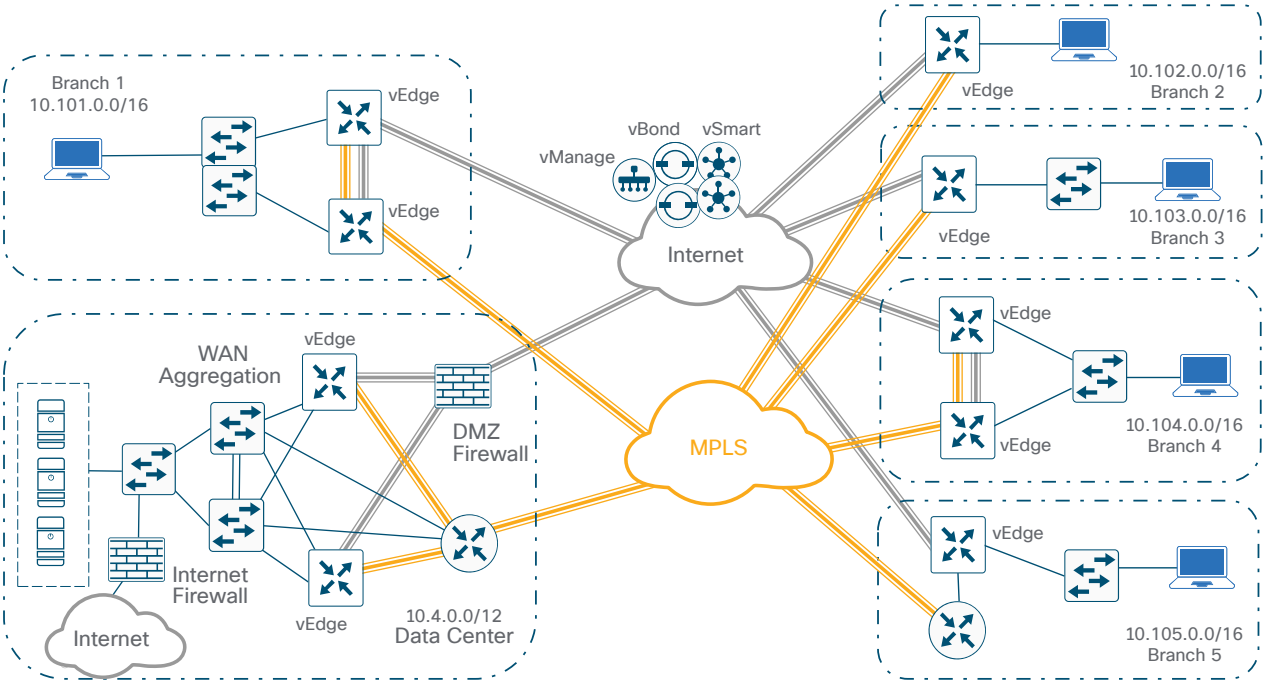
Note that the step ordering is fairly flexible with a few exceptions:

- Network planning and the SD-WAN controller deployment should come first
- When targeting a new code version, the vManage device should be upgraded first, followed by the vSmart and vBond controllers, followed by the vEdge routers.
- The authorized serial number file needs to be uploaded before any vEdge routers can be successfully brought online.
- Device templates must be attached to vEdge routers in the vManage GUI before bringing them online successfully via the ZTP process.
- Localized policy is attached to a device template. If the device template is already attached to a vEdge device, the localized policy must be attached before any policy components (route-policies, prefix-lists, etc.) can be referenced within the device templates.

Deployment example

The following figure is a high-level overview of the example network in this deployment guide.

Figure 2. Example SD-WAN network



In this topology, there is one data center and five remote sites. The transports shown are one MPLS and one Internet service provider. The SD-WAN controllers are deployed using Cisco's cloud-managed service and reachable via the Internet transport. There is one vManage, one vSmart controller, and one vBond orchestrator on the U.S. West Coast, and there is one vSmart controller and one vBond orchestrator on the U.S. East Coast.

Each vEdge router attempts to make a connection to the controllers over each transport. The vEdge router will initially connect to a vBond and will then connect to the two vSmart controllers over each transport. Only one vManage connection is made from the site, and it will depend on which transport first connected to it, but this preference is configurable. The vEdge routers connect directly to the controllers over the Internet transport. The vEdge routers connect to the controllers over the MPLS transport by being routed over the IPSec tunnels to the data center and following the default route out of the Internet firewall to the Internet transport.

Data center details

Transport side

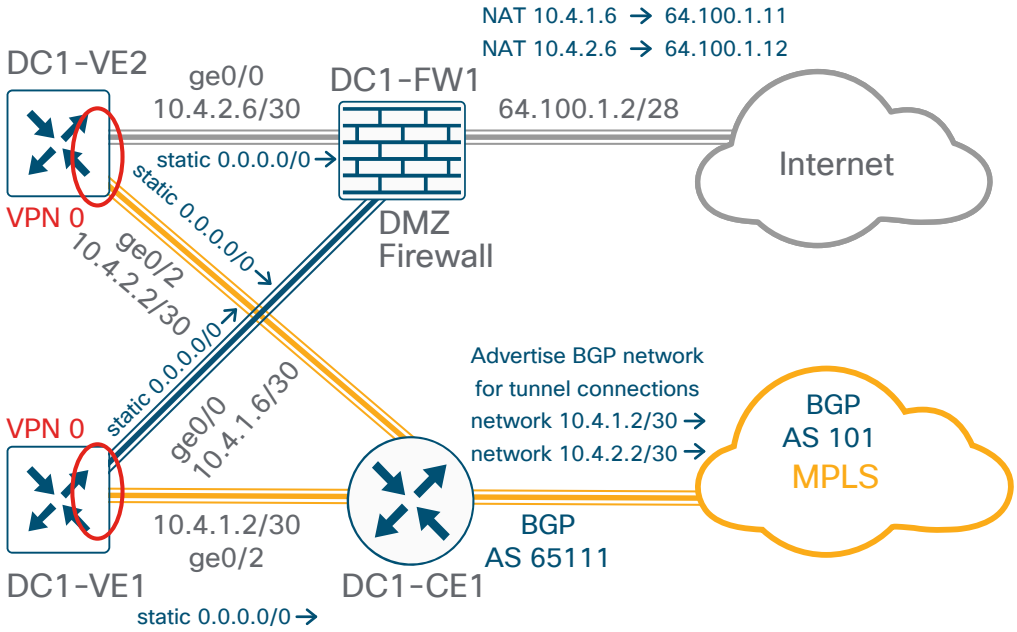
The transport VPN, VPN 0, contains interface ge0/0 for the Internet transport and ge0/2 for the MPLS transport on each vEdge router.

Interface ge0/0 of each vEdge router is connected to a DMZ switch which connects to a Cisco Adaptive Security Appliance (ASA) 5500 using a DMZ interface. Each vEdge router Internet-facing interface will be assigned an IP address that needs to be Internet-routable since it will be the endpoint for the VPN tunnel connection over the Internet. This can be accomplished by either assigning a routable address directly to the vEdge router or assigning a non-routable RFC-1918 address directly to the vEdge router and using Network Address Translation

(NAT) on the ASA 5500 to translate this private IP address into a routable IP address. This design assumes that a static NAT is configured for each vEdge Internet tunnel endpoint address on the Cisco ASA 5500. This is equivalent to full-cone NAT, or one-to-one NAT, which maps an internal address/port pair to an external address/port pair and allows an outside host to initiate traffic to the inside of the network. It is recommended that the data center or hub sites use one-to-one NAT to prevent issues with connections to other vEdge routers. The vEdge router will use a static default route in VPN 0 to route the tunnel endpoint out to the Internet transport.

Interface ge0/2 on each vEdge router is connected to the Customer Edge (CE) router, which connects to the service provider's MPLS Provider Edge (PE) router and peers with it via an external Border Gateway Protocol (eBGP) connection. The private address that is assigned for the vEdge MPLS tunnel endpoint will be advertised from the CE router by advertising the subnets connected to the vEdge routers via BGP into the provider cloud so the tunnel endpoint can be reachable to other vEdge routers sitting on the MPLS transport. The vEdge will use a static default route in VPN 0 to route the tunnel endpoint out to the MPLS transport.

Figure 3. Data center network transport side



Service side

The service VPN, VPN 1, contains interfaces ge0/4 and ge0/5 for the connections to the WAN aggregation switches. Interface ge0/4 of each vEdge connects to data center WAN aggregation switch 1 in the network, while interface ge0/5 connects to data center WAN aggregation switch 2. Each vEdge peers to each switch via eBGP using the interface addresses, so the switches use BGP next-hop-self to ensure all routing next hops are reachable from each vEdge.

Figure 4. Data center network service side

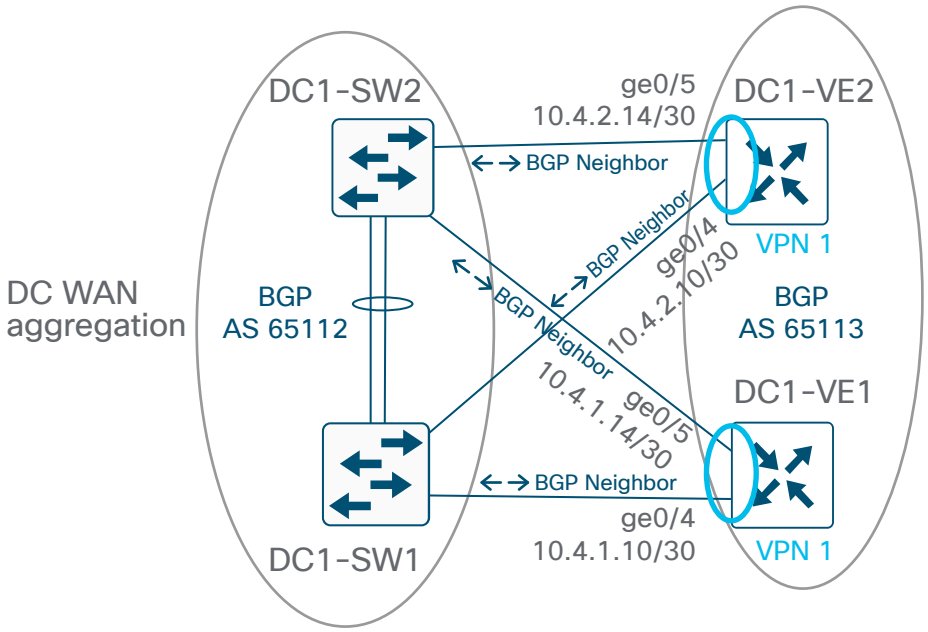


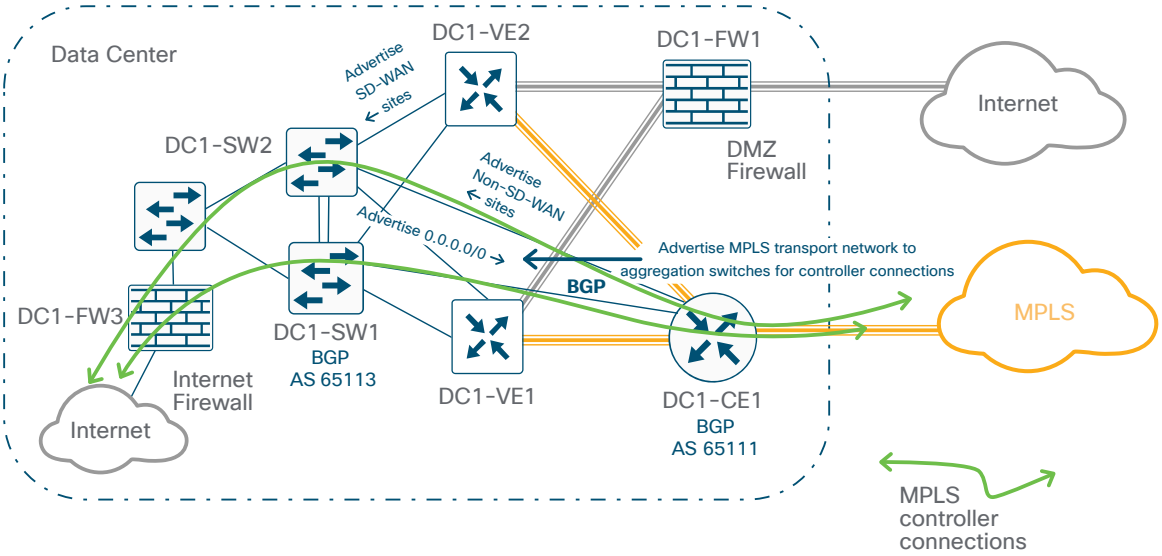
Table 1. Data center vEdge IP addresses

Hostname	ge0/0 Internet	ge0/2 MPLS	ge0/4 DC1-SW1	ge0/5 DC2-SW2
DC1-VE1	10.4.1.6/30	10.4.1.2/30	10.4.1.10/30	10.4.1.14/30
DC1-VE2	10.4.2.6/30	10.4.2.2/30`	10.4.2.10/30	10.4.2.14/30

MPLS routing

The CE router in the data center peers with the WAN aggregation switches via eBGP. The CE advertises the non-SD-WAN site networks while the vEdge routers advertise the SD-WAN site networks. For the MPLS controller connections, the aggregation switches advertise a default route to the CE router so the control connections from the MPLS transport can follow the route out to the Internet firewall in order to connect to the controllers. This Internet firewall, DC1-FW3, is configured for dynamic NAT with a pool of addresses so the vEdge control connections to the controllers are sourced from routable Internet addresses. The CE must also advertise the MPLS tunnel endpoints (including transport location [TLOC] extension subnets) to the aggregation switches so the controllers from the Internet transport can reach the vEdge routers sitting on the MPLS transport.

Figure 5. Data center MPLS routing



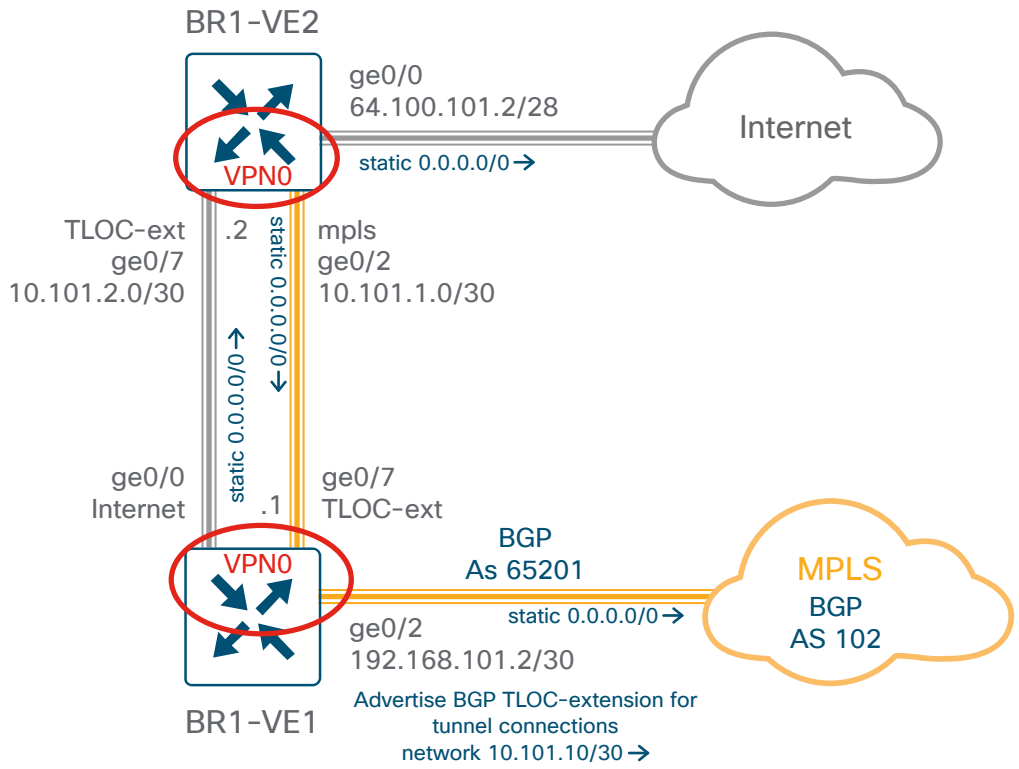
Branch details

Branch 1: Dual-vEdge/TLOC extension/layer 2 trunk LAN switch/VRRP site

Transport side

In Branch 1, two vEdge 1000 routers are depicted, each with a direct connection to one of the transport providers. This site has TLOC-extension links between the vEdge routers to give each vEdge router access to both transports. vEdge 1 runs BGP in the transport VPN to communicate the TLOC extension link subnet to the MPLS cloud, so vEdge 2 will have reachability to the controllers through the data center and to other vEdge routers on the MPLS transport to form IPSec tunnels. On both vEdge routers, static default routes pointing to the next-hop gateways are configured for tunnel establishment on the MPLS (ge0/2) and Internet (ge0/0) links on both vEdge routers. The TLOC-extension interface does not need any special routing configured since it routes tunnel and control traffic to the next hop, which is directly connected.

Figure 6. Branch 1 transport side



Service side

Each vEdge router connects to a stack of LAN switches via a trunk interface. Only one link on each vEdge is attached to a single LAN switch in the stack. This simplifies the design as there is no current support for channeling or spanning-tree, and if you configure a link from each vEdge router to each LAN switch, you would need to configure Integrated Routing and Bridging (IRB), which can add complexity.

The trunk links are each configured with two VLANs, vlan 10 (data) and 20 (voice), which translates into two different sub-interfaces each on the vEdge router side. The physical link, ge0/4, is configured in VPN 0, while each sub-interface is a part of the service VPN, VPN 1. With Virtual Router Redundancy Protocol (VRRP), the vEdge routers become the IP gateways for the hosts at the branch. VRRP is configured on each sub-interface with a .1 host address for the two subnets, 10.101.10.0/24 and 10.101.20.0/24.

Figure 7. Branch 1 service side

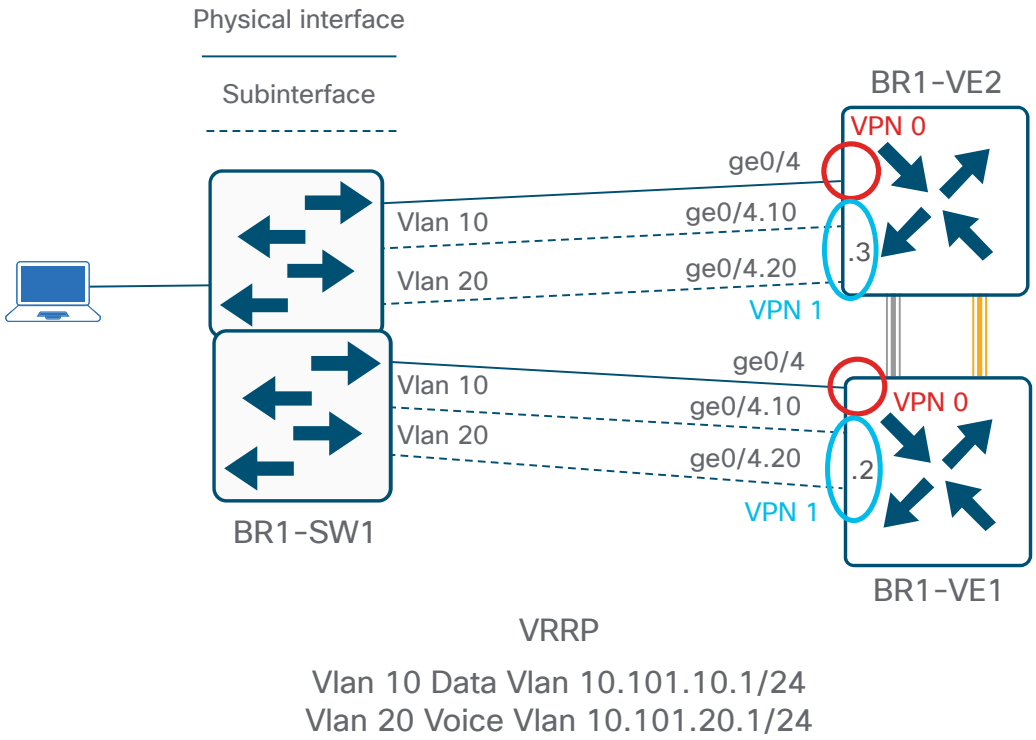


Table 2. Branch 1 vEdge IP addresses

Hostname	ge0/0 Internet	ge0/2 MPLS	ge0/7 TLOC Extension	ge0/4 BR1-SW1 Vlan 10	ge0/4 BR1-SW1 Vlan 20
BR1-VE1	10.101.2.1/30	192.168.101.2/30	10.101.1.1/30	10.101.10.2/24	10.101.20.2/24
BR1-VE2	64.100.101.2/28	10.101.1.2/30	10.101.2.2/30	10.101.10.3/24	10.101.20.3/24

Branch 2: Single vEdge/Internet DHCP address/no LAN switch

Transport side

Branch 2 contains one vEdge 100wm router, which connects to both the MPLS and Internet transports. The Internet transport interface is configured for Dynamic Host Configuration Protocol (DHCP) in order to dynamically obtain an IP and gateway address. A static default route pointing to the next-hop gateway is configured for tunnel establishment on the MPLS transport (ge0/2).

Service side

Branch 2 has no switch. A host is connected to interfaces ge0/0 and ge0/3.

Figure 8. Branch 2 transport and service side

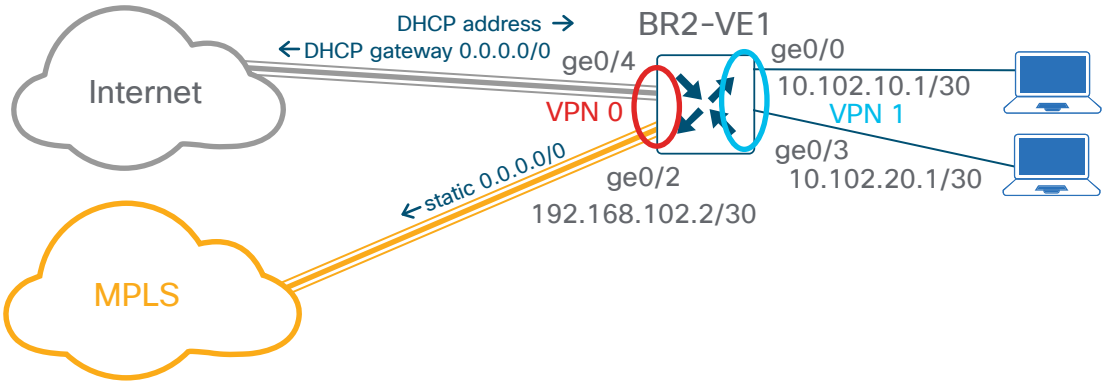


Table 3. Branch 2 vEdge IP addresses

Hostname	ge0/4 Internet	ge0/2 MPLS	ge0/0	ge0/3
BR2-VE1	DHCP (64.100.102.x/28)	192.168.102.2/30	10.102.10.1/30	10.102.20.1/30

Branch 3: Single vEdge/layer 2 trunk LAN switch site

Transport side

Branch 3 contains one vEdge 100b router which connects to both the MPLS and Internet transports. A static default route pointing to the next-hop gateway is configured for tunnel establishment on the Internet (ge0/4) and MPLS (ge0/2) transports.

Service side

The vEdge router on Branch 3 is trunked to a layer 2 switch. The trunk link is configured with two VLANs, vlan 10 (data) and 20 (voice), which translates into two different sub-interfaces each on the vEdge router side. The physical link, ge0/0, is configured in VPN 0, while each sub-interface is a part of the service VPN, VPN 1.

Figure 9. Branch 3 transport and service side

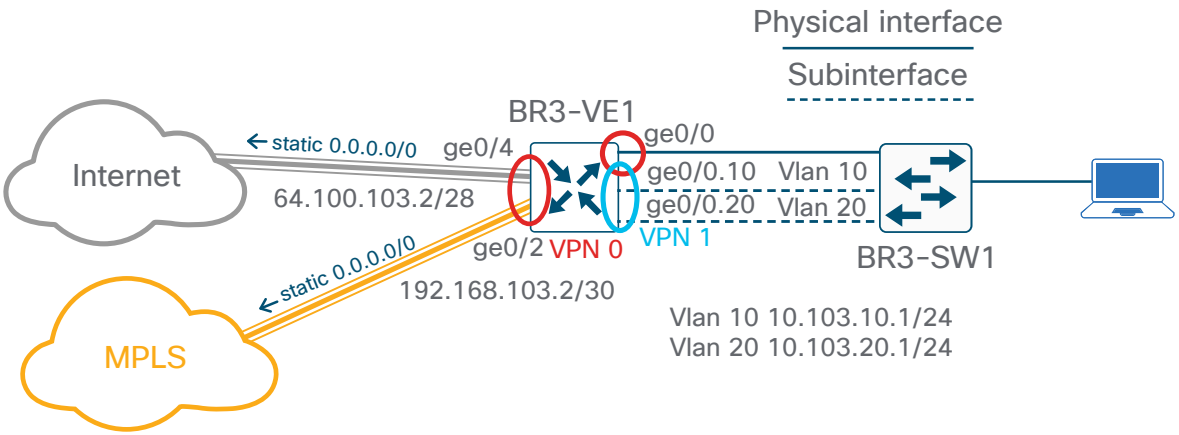


Table 4. Branch 3 vEdge IP addresses

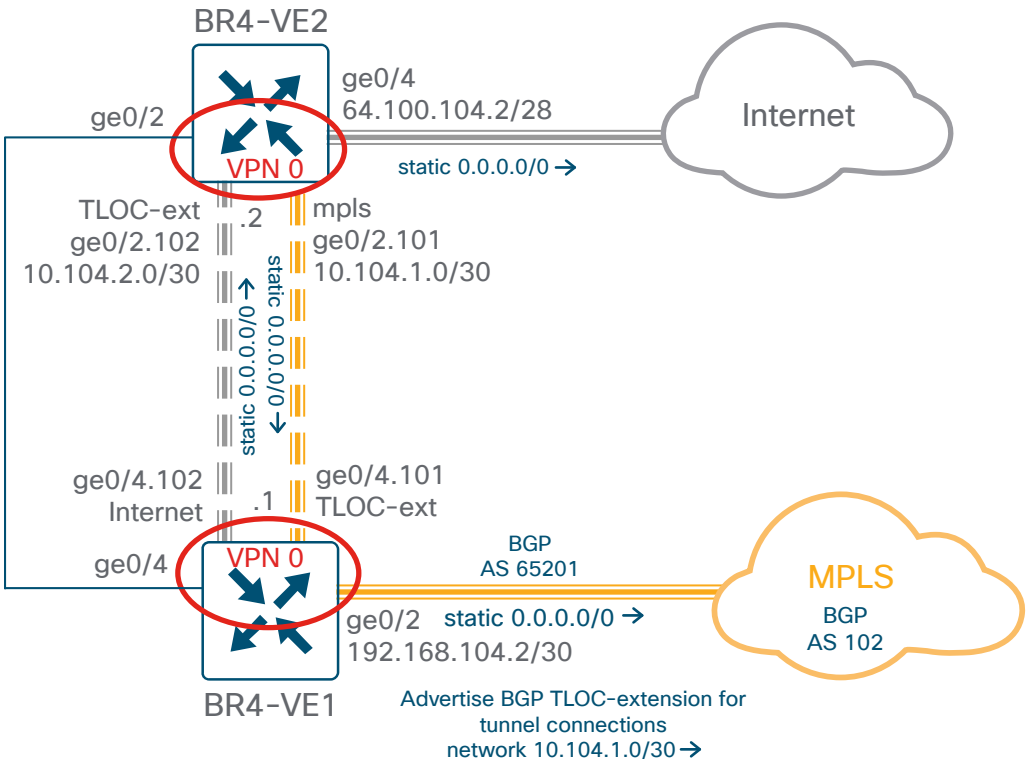
Hostname	ge0/4 Internet	ge0/2 MPLS	ge0/0 LAN-SW1 Vlan 10	ge0/0 LAN-SW2 Vlan 20
BR3-VE1	64.100.103.2/28	192.168.103.2/30	10.103.10.1/24	10.103.20.1/24

Branch 4: Sub-interface TLOC-extension/layer 3 OSPF routing site

Transport side

In Branch 4, two vEdge 100b routers are depicted, each with a direct connection to one of the transport providers. This site has a TLOC-extension link between the vEdge routers to give each vEdge router access to both transports. The TLOC-extension link utilizes sub-interfaces. vEdge 1 runs BGP in the transport VPN to communicate the TLOC extension link subnet to the MPLS cloud, so vEdge2 will have reachability to the controllers through the data center and to other vEdge routers on the MPLS transport to form IPSec tunnels. On both vEdge routers, static default routes pointing to the next-hop gateways are configured for tunnel establishment on the MPLS (ge0/2) and Internet (ge0/0) links. The TLOC-extension sub-interface does not need any special routing configured since it routes tunnel and control traffic to the next hop, which is directly connected. The physical links, ge0/4 on vEdge 1 and ge0/2 on vEdge 2, as well as the sub-interfaces, are configured in VPN 0.

Figure 10. Branch 4 transport side



Service side

Branch 4 has two vEdge routers connected to a layer 3 switch and running Open Shortest Path First (OSPF) between them. All devices are in area 0. The vEdge router interfaces are configured for OSPF network point to point on each interface to the layer 3 switch.

Figure 11. Branch 4 service side

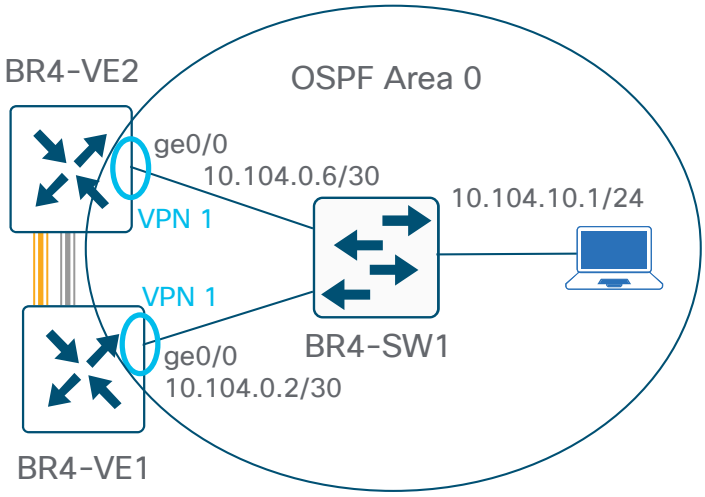


Table 5. Branch 4 vEdge1 IP addresses

Hostname	ge0/4.102 Internet	ge0/2 MPLS	ge0/4.101 TLOC Extension	ge0/0 LAN-SW1
BR4-VE1	10.104.2.1/30	192.168.104.2/30	10.104.1.1/30	10.104.0.2/30

Table 6. Branch 4 vEdge2 IP addresses

Hostname	ge0/4 Internet	ge0/2.101 MPLS	ge0/2.102 TLOC Extension	ge0/0 LAN-SW1
BR4-VE2	64.100.104.2/28	10.104.1.2/30	10.104.2.2/30	10.104.0.6/30

Branch 5: CE router/layer 3 switch/static LAN routing site

Transport side

Branch 5 has a single vEdge 100b directly connected to the Internet transport and is also connected to a CE router, which has a connection to the MPLS transport. A static default route pointing to the next-hop gateway is configured for tunnel establishment on the Internet (ge0/4) and MPLS (ge0/2) transports. BGP configured on the CE router advertises the vEdge MPLS subnet so the vEdge router can have reachability to the other vEdge routers on the MPLS transport and connectivity to the controllers through the data center.

Service side

The vEdge router at branch 5 connects to a layer 3 switch and there is static routing between the LAN switch and the vEdge router.

Figure 12. Branch 5 transport and service side

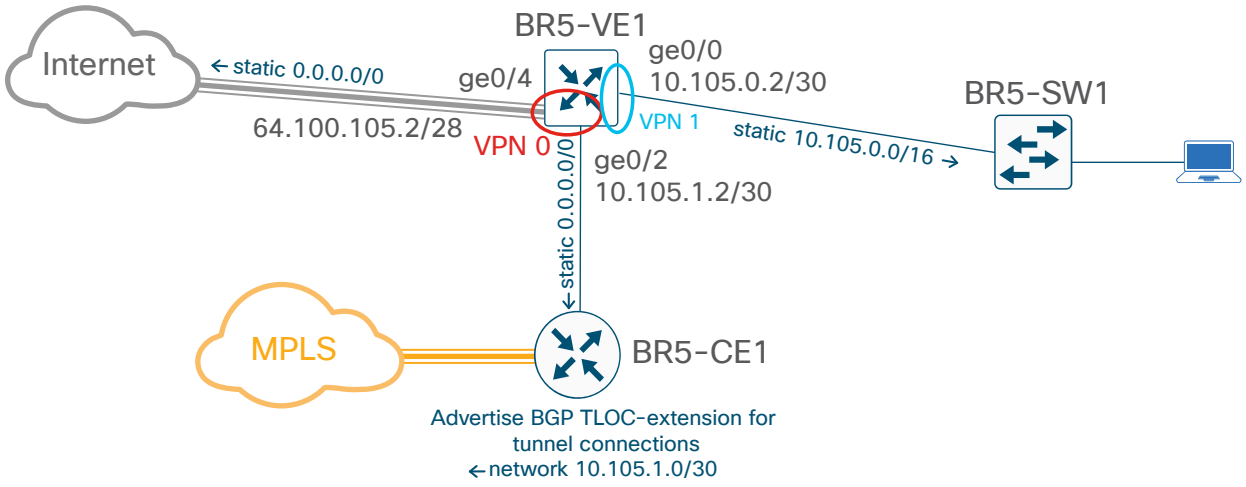


Table 7. Branch 5 vEdge IP addresses

Hostname	ge0/4 Internet	ge0/2 MPLS	ge0/0 LAN-SW1
BR5-VE1	64.100.105.2/28	10.105.1.2/30	10.105.0.2/30

Additional details

Port numbering

The following table is the port numbering scheme chosen for this deployment guide. The Internet column reflects the ZTP ports on the various vEdge models.

Table 8. Port numbering scheme

vEdge Model	Internet	MPLS	MPLS	TLOC Extension
vEdge 5000	ge0/0	ge0/2	ge0/4, ge0/5	-
vEdge 1000	ge0/0	ge0/2	ge0/4, ge0/5	ge0/7
vEdge 100	ge0/4	ge0/2	ge0/0	ge0/3

System IP address and site ID

In this example network, the system IP address in the range 10.255.240.0/12 is specific to North America, the third octet reflects the region (U.S. West or East) and the fourth octet reflects the branch number.

The site IDs for this example network are similar to the scheme specified in the SD-WAN Design Guide, except that six digits are used instead of nine. The number of the branch is built into the site type digits instead of using three extra digits for that purpose.

Table 9. Six-digit site ID example

vEdge Model	Representation	Examples
1	Country/continent	1=North America, 2=Europe, 3=APAC
2	Region	1=US West, 2=US East, 3=Canada West, 4=Canada East
3-6	Site type	0000-0099=Hub locations, 1000-1999=Type 1 sites, 2000-2999=Type 2 sites, 3000-3999 = Type 3 sites, 4000-4999=Type 4 sites, 5000-9999 = future use

Table 10. Example network site type descriptions

Site type	Description
Site type 1 (1000-1999)	Low bandwidth sites, where there is no full mesh of traffic. Traffic must go through the hub instead (branches 2 and 5)
Site type 2 (2000-2999)	Sites that offer guest Direct Internet Access (DIA) (branches 1 and 4) (not implemented in this guide)
Site type 3 (3000-3999)	Sites that require voice on MPLS while all other traffic takes the Internet transport (branch 3) (not implemented in this guide)
Site type 4 (4000-4999)	Sites that require corporate traffic use a central firewall to talk to other sites directly (not implemented in this guide)

The following table provides a summary of the site IDs and system IP addresses for this example network.

Table 11. Example network site IDs and system IP addresses

Hostname	Location	Site ID	System IP
DC1-VE1	Datacenter 1/West	110001	10.255.241.101
DC1-VE2	Datacenter 1/West	110001	10.255.241.102
BR1-VE1	Branch 1/West	112001	10.255.241.11
BR1-VE2	Branch 1/West	112002	10.255.241.12
BR2-VE1	Branch 2/West	111002	10.255.241.21
BR3-VE1	Branch 3/West	113003	10.255.241.31
BR4-VE1	Branch 4/East	122004	10.255.242.41
BR4-VE2	Branch 4/East	122004	10.255.242.42
BR5-VE1	Branch 5/East	121005	10.255.242.51

Color

In the example network, the MPLS color is used for the MPLS transport. MPLS control traffic is using NAT to reach the controllers on the Internet through the data center, but because MPLS is a private color, the vEdge routers use the private address (or pre-NAT address) to set up tunnels through the MPLS transport.

Biz-internet, a public color, is the color used for the Internet transport which means the vEdge routers will use the post-NAT address if available to set up tunnels to other vEdge routers through the Internet transport.

Additional design parameters

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the WAN. These parameters are listed in the following table.

Table 12. Universal design parameters

Network service	IP address
Domain name	cisco.local
Active Directory, DHCP server	10.4.48.10
DNS server	10.4.48.10 (internal), 64.100.100.125, 64.100.100.126
Logging server	10.4.48.13
Cisco Identity Services Engine (ISE)	10.4.48.15
Network Time Protocol (NTP) server	10.4.48.17 (internal), time.nist.gov
Cisco Unified Communications Manager	10.4.48.19

Deployment details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Tech tip

The procedures in this section provide examples for most settings. The actual settings and values that you use are determined by your current network configuration.

The deployment details will cover:

- Tuning controller configurations. Verify that the controllers are up and modify their configurations for best practices. Upload the authorized serial file.
- Preparing for software upgrades and upgrading the controllers.
- Deploying the data center vEdge routers. This covers the bootstrapping of vEdge routers to get them connected to the controllers, code upgrades, device and feature template configurations, and localized policy.
- Deploying the remote site vEdge routers. This covers the ZTP process in getting the vEdge routers connected to the controllers, code upgrades, device and feature template configurations, and localized policy.
- Deploying a centralized policy.
- Deploying an application-aware routing policy.
- Configuring traffic symmetry.
- Deploying Quality of Service (QoS).

Process

Tuning controller configurations

1. Verify controllers are up and ready
2. Determine controller configuration mode
3. Tune configuration settings (optional on all controllers)
4. Upload the authorized vEdge serial file

The controllers in this deployment consist of a vManage, two vSmart controllers, and two vBond orchestrators. The vManage and vBond orchestrators are in Command-Line Interface (CLI) mode while the vSmart controllers are in vManage mode using CLI-based templates. The vManage and vBond orchestrators can be modified directly with CLI, while the vSmart controllers must be configured using vManage.

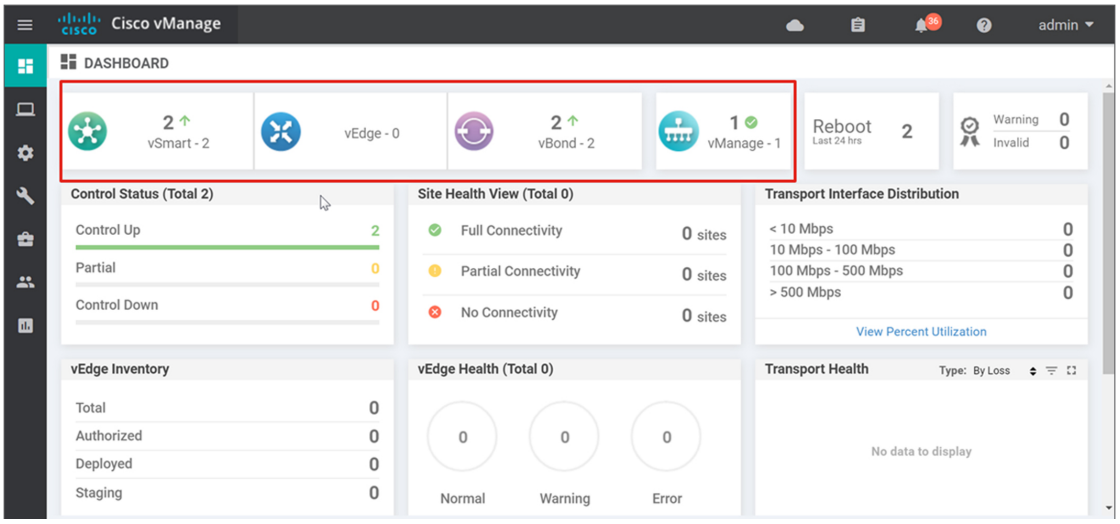
The following section instructs how to view the controller reachability, how to modify the controller configurations, and how to upload the vEdge serial file.

Procedure 1 Verify controllers are up and ready

Step 1: Access the vManage web instance by using a web browser.
For example: https://vmanage1.cisco.com:8443/

Step 2: Log in with username and password credentials.

Step 3: The vManage dashboard will be displayed. At the top, a status indicating reachability will be displayed for any vSmart controllers, vEdge routers, and vBond orchestrators that are installed and have been added to vManage. Verify the controllers are all showing up before moving on. The number of controllers will be shown with a green up arrow (indicating reachable), or a red down arrow (indicating unreachable).

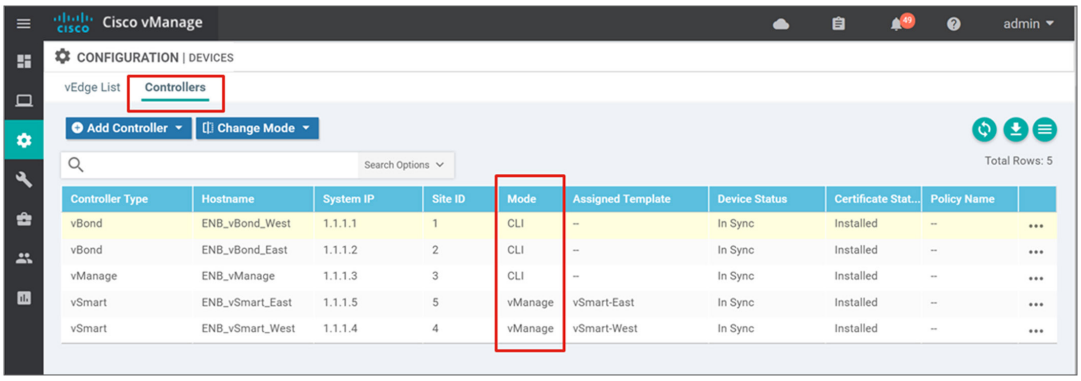


Procedure 2 Determine controller configuration mode

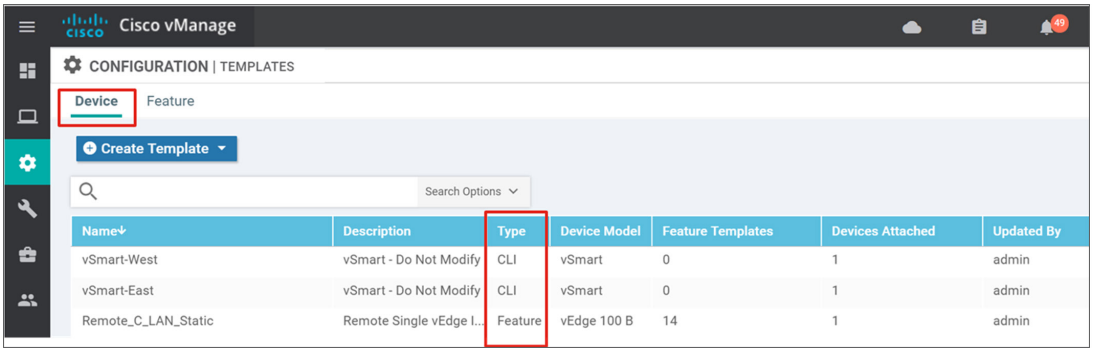
To determine the controller configuration mode:

Step 1: Go to **Configuration>Devices** and select the **Controllers** tab.

Step 2: Check the **Mode** column. The vManage and vBond controllers are in CLI mode, while the vSmart controllers are in vManage mode.



Step 3: To see what template type the vSmart controllers are using, go to **Configuration>Templates** and ensure the **Device** tab is selected. The column shows that the vSmart controllers are using **CLI** templates as opposed to feature templates.



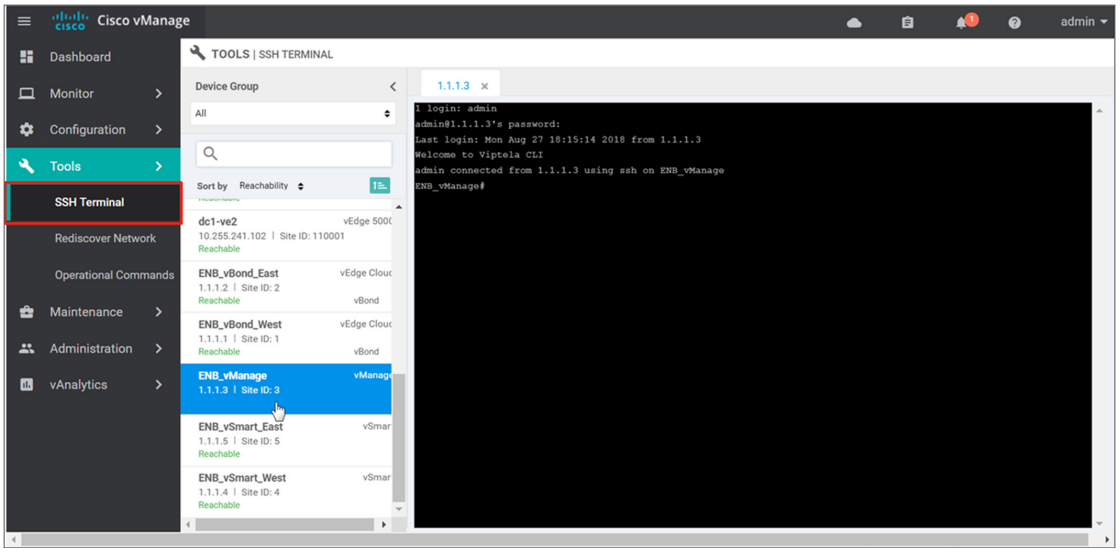
Procedure 3 Tune configuration settings (optional on all controllers)

Some settings you may want to modify:

- Admin password (all controllers). You may want to change the admin password for the controllers if you are using local authentication.
- Port hopping (all controllers). It is recommended to disable port hopping on controllers.
- TLS (vSmart controllers and vManage). If possible, run Transport Layer Security (TLS) as the security protocol between vEdge and the controllers and between controllers. This does not apply to vBond controllers. TLS is Transmission Control Protocol (TCP)-based and uses handshaking and acknowledgements.

- Enable **Send Backup Path** (vSmart controllers only). By default, Overlay Management Protocol (OMP) only advertises the best route or routes in the case of equal-cost paths. With the **Send Backup Path** command, OMP also advertises the next best route in addition to the best route. This can help improve convergence.
- **Send Path Limit** (vSmart controllers only). By default, the number of equal-cost routes that are advertised per prefix is four. It is recommended to increase this to the maximum of 16.

Step 1: To modify a controller in CLI mode, use Secure Shell (SSH) to connect to the desired controller. If you have the IP address, you can SSH directly, or you can SSH via vManage by going to **Tools > SSH Terminal** and selecting the device on the left side. An SSH window will come up in the main panel. Enter the current username and password.



Step 2: Change the admin password, disable port hopping, and enable TLS by entering the following:

```
config terminal
system
 no port-hop
 aaa
  user admin password admin
security
 control protocol tls
commit and-quit
```

Note that the password you enter is the clear-text version. It will be converted automatically to an encrypted string in the configuration.

Step 3: Repeat steps 1 and 2 for the vBond controllers. You will not be able to change the control protocol to TLS because only DTLS can be used.

Step 4: On vManage, go to **Configuration > Templates**, find the desired CLI template name (**vSmart-East**).

Step 5: Select **...** to the far right and select **Edit**

Step 6: Modify the CLI template by adding the following. When you insert configurations into CLI templates, you can place them in any order, but the configurations should be under the proper category headers (system, OMP, security). Otherwise, you may get errors when the configuration is pushed to the device. For example, port-hopping configurations belong under the system category. Here is a configuration snippet:

```
system
 no port-hop
 !
!
omp
 no shutdown
 send-path-limit  16
 graceful-restart
 send-backup-paths
 !
security
 control
  protocol tls
!
```

To adjust the AAA password in the CLI template, you need to configure the encrypted form of the password. An easy way to accomplish this password change is to create a variable instead. The value of the variable will be expected in clear text, then it will be automatically encrypted before being inserted into the configuration and pushed out to the device.

Step 7: In the CLI template, highlight the encrypted password and select **Create Variable**.

Step 8: A pop-up window asks for the variable name that is replacing the text. In the **Variable Name** text box, type in **admin_password** and select **Create Variable**.

Step 9: Select **Update**.

Step 10: Select **...** to the right of the device, then select **Edit Device Template** from the drop-down menu.

Step 11: Fill in the new admin password in the text box and then select **Update**.

Step 12: Select **Next** and then select **Configure Devices**. The configuration will be pushed out to the device. The status should be marked as success.

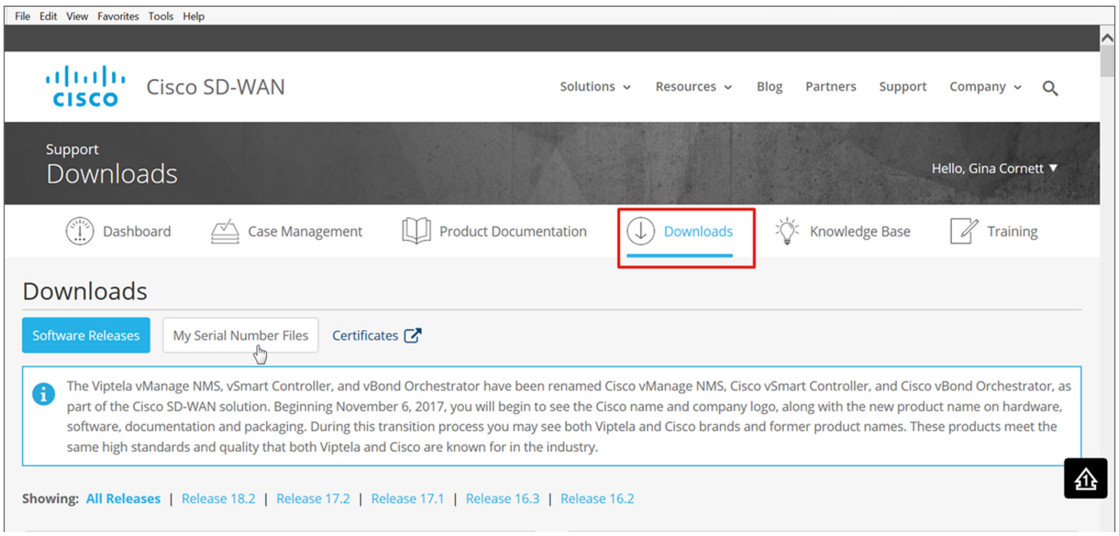
Step 13: Repeat steps 4 through 12 for the vSmart-West controller.

Procedure 4 Upload the authorized vEdge serial file

In order for the vEdge devices to come up and active in the overlay, you must have a valid authorized vEdge serial file uploaded to the vManage. This authorized serial number file lists the serial and chassis numbers for all the vEdge routers allowed in the network. vManage will send this file information to the controllers, and only devices that match serial numbers on the list will be validated and authenticated successfully by the controllers.

Step 1: Retrieve the authorized serial file on the Cisco SD-WAN support website. Go to https://sdwan-docs.cisco.com/Downloads. During this process, you may be redirected to log in, and if so, log in with your SD-WAN support username and password and navigate back to the Downloads page if needed.

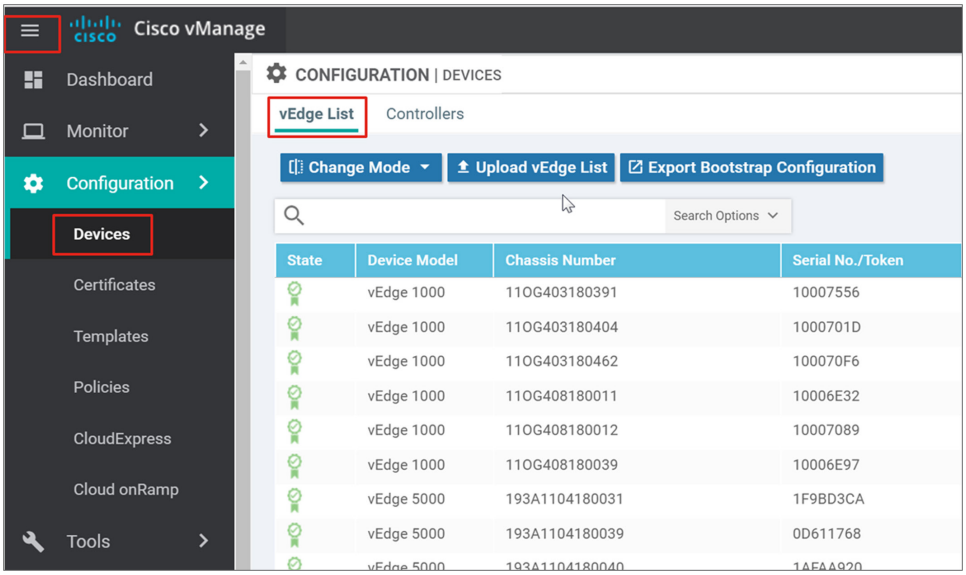
Step 2: Under the **Downloads** section, select the **My Serial Number** files box. Then download the serial file corresponding to the proper organization name.



Tech Tip

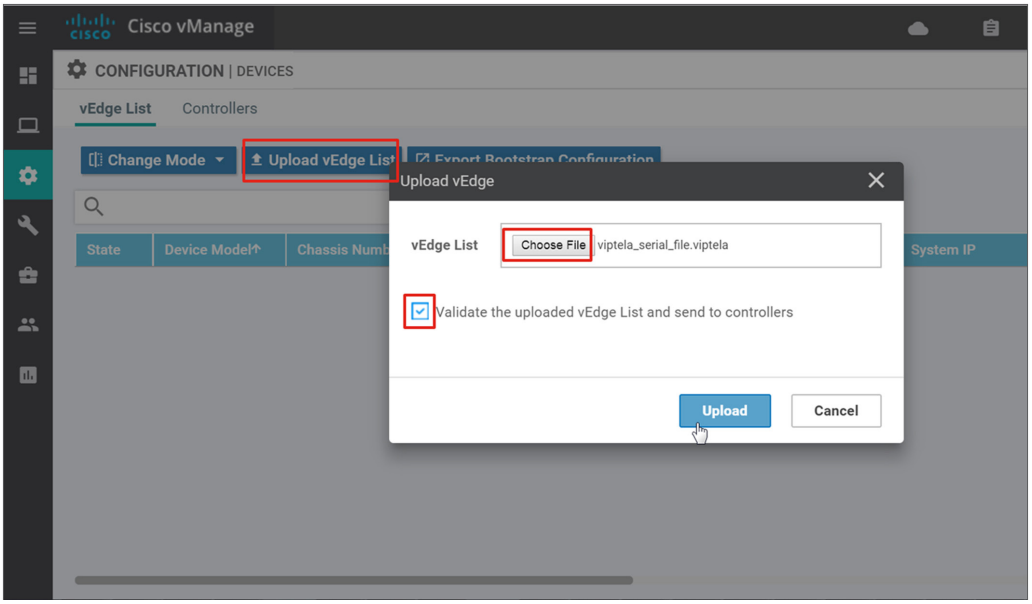
Serial Number Files are being migrated to the Cisco Network Plug and Play (PnP) website. Follow instructions that appear on My Serial Number Files page at https://sdwan-docs.cisco.com/Downloads. The PnP portal can be found at https://software.cisco.com.

Step 3: In the vManage GUI, go to **Configuration>Devices** on the left side, or alternatively, expand the left menu by selecting the three horizontal bars in the top left corner of the GUI, then select **Configuration>Devices**. Ensure the vEdge List tab is selected.



Step 4: Select the **Upload vEdge List** button. A pop-up window appears. Select **Choose File**. Browse for and select the serial file. Select **Open**.

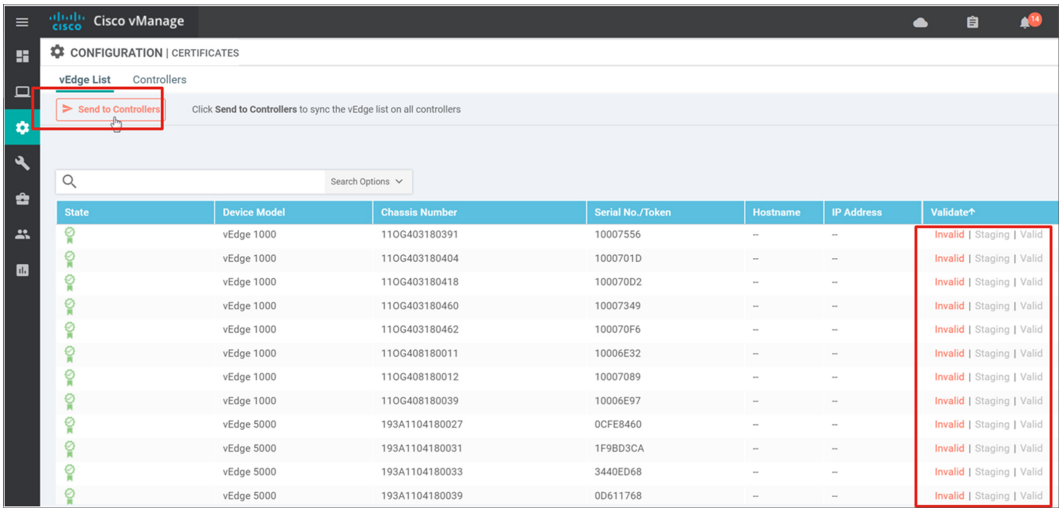
Step 5: Now that the file is selected, select the check box in order to validate the upload of the vEdge list and send it to the controllers. Select the **Upload** button. If you select the check box, this will put all the devices on the list into a valid state, meaning they can be brought up at any time on the network and start forwarding traffic. If you do not select **Validate**, all of the devices will show up as invalid, and you will need to change them to valid individually if you want to bring them up on the network and participate in the overlay.



Step 6: The box will ask if you are sure you want to upload the file. Select **OK**.

Step 7: A pop-up window appears to inform you that the vEdge list uploaded successfully and informs you of the number of vEdge routers that were uploaded successfully. Select **OK**. A page will indicate that the vEdge list has been successfully pushed out to the vBond and vSmart controllers.

Step 8: If you did not select the check box to validate the uploaded vEdge list to send to the controllers, you can go to **Configuration>Certificates**, ensure the **vEdge List** tab is selected, and select the **Send to Controllers** button in the top left section of the screen. This will distribute the list of authorized vEdge routers to all of the controllers. A page will indicate that the vEdge list has been successfully pushed out to the vBond and vSmart controllers. All devices will be in an invalid state.



Process

Preparing for software upgrades and upgrading the controllers

1. Prepare and configure vManage for software upgrades
2. Upgrade vManage (optional)
3. Upgrade the vBond and vSmart controllers

Software may be downloaded from https://sdwan-docs.cisco.com/Downloads.

When moving to a particular code version, it is important to upgrade code first on the vManage, then on the controllers (vSmart, vBond), and lastly, on the vEdge routers. Be certain vManage and the controllers are at the proper code version before bringing the vEdge routers onto the targeted code version. The vEdge routers can be upgraded once online or as a last part of the ZTP process, or even manually before deployment, if needed. The vEdge routers do not necessarily need to be at the same version of the controllers, but it's recommended as configurations supported in the vManage GUI may not be supported on a vEdge running a lower code version.

Some best practices when upgrading software:

1. Upgrade the vManage, then the vBond orchestrators, then half of the vSmart controllers. Let the controllers run stable for 24 hours. Then upgrade the remainder of the vSmart controllers.
2. Break up the vEdge routers into different upgrade groups. You can identify them with a tag in the device-groups field in the system template. Target a test site or multiple test sites, and put those vEdge routers into the first upgrade group. In dual vEdge sites, put each vEdge router into a different upgrade group and do not upgrade both of them at the same time. All vEdge routers in an upgrade group can be upgraded in parallel (up to 32 vEdge routers), however, take into account the ability for vManage or a remote file server to be able to handle the concurrent file transfers to the vEdge routers.

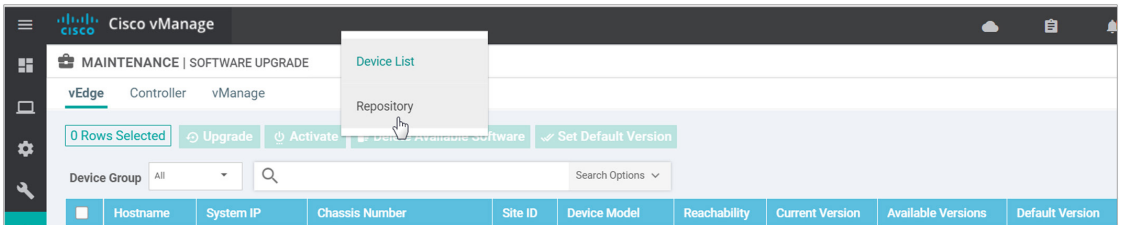
3. Upgrade the first upgrade group and let the code run stable for a predetermined amount of time, then proceed to upgrade the additional upgrade groups.

When upgrading using vManage, you can upgrade using a code image that is directly loaded onto vManage or a remote vManage, and you can also upgrade using a code image located on a remote file server.

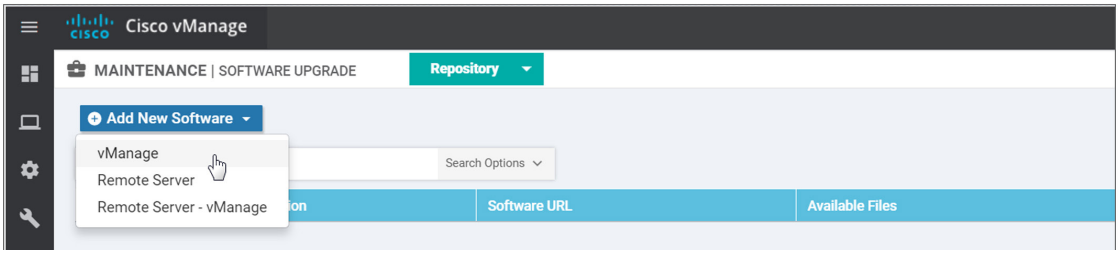
Procedure 1 Prepare and configure vManage for software upgrades

In this procedure, software for any controller and vEdge router is uploaded to vManage and a remote file server and the vManage software repository is configured and prepared for upgrading devices. The data center device upgrades will be performed with a remote server, while other devices will be upgraded using images stored on vManage.

Step 1: Go to **Maintenance > Software Upgrade**. The page will default to the **vEdge** tab and all of the vEdge routers the vManage knows about will be listed. Select **Device List** at the top of the page, and select **Repository** from the drop-down menu. The repository will store the image locally on vManage, or indicate where to retrieve it in the case of a remote file server or remote vManage.



Step 2: Select **Add New Software** and a drop-down menu allows you to select either **vManage**, **Remote Server**, or **Remote Server - vManage**.



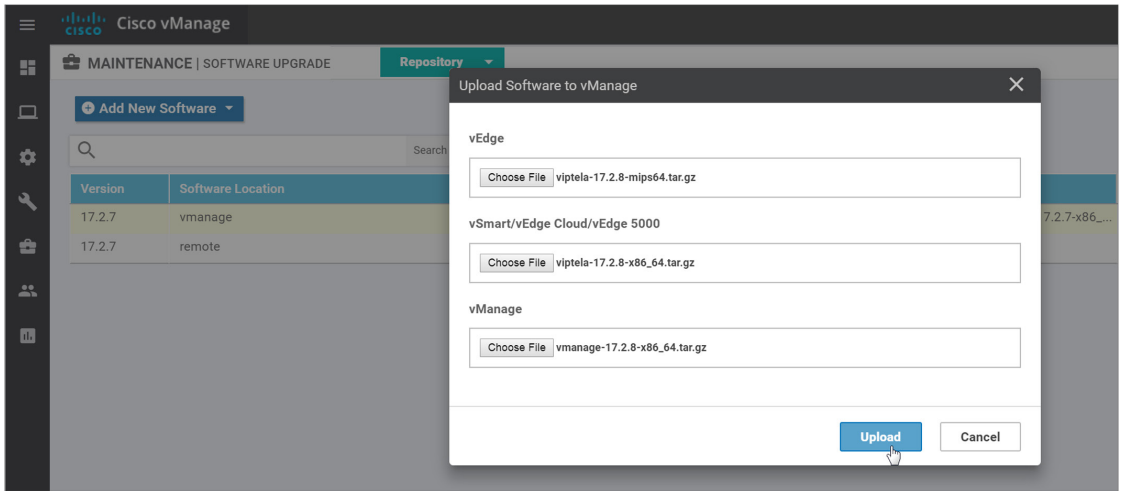
Step 3: Select **vManage**. A window will appear allowing you to upload three different types of files: vManage, vSmart/vEdge Cloud/vEdge 5000, and vEdge. The vEdge label applies to vEdge 100, 1000, and 2000 but not the vEdge 5000.

See the file naming conventions to determine which file is loaded into which section.

Table 13. SD-WAN file naming conventions

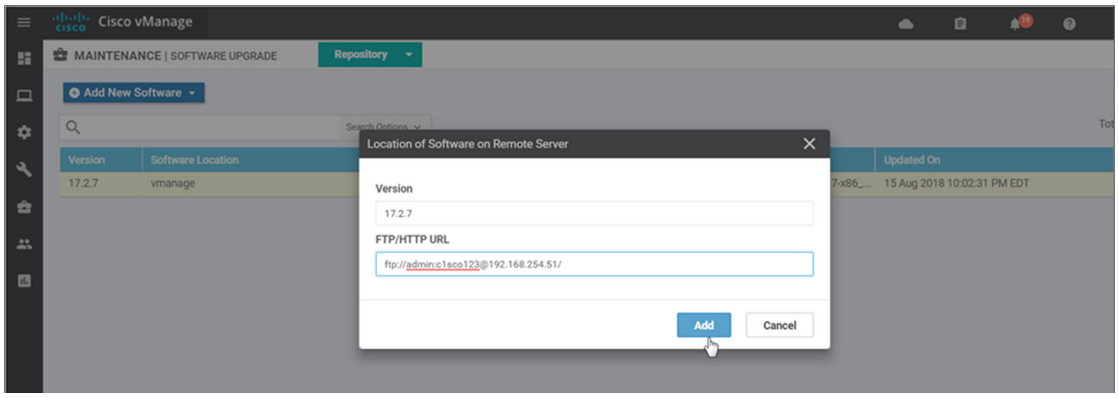
Device type	File name convention
vEdge (This includes vEdge100, 1000, and 2000)	viptela-17.2.8-mips64.tar.gz
vSmart/vEdge Cloud/vEdge 5000 (This also includes vBond)	viptela-17.2.8-x86_64.tar.gz
vManage	vmanage-17.2.8-x86_64.tar.gz

You will get a warning and an indication of the proper file type if you load the incorrect file type. Upload the desired files by selecting the **Choose File** button and choosing the desired software version and proper file type. You can load all three files or a subset of them.



Select **Upload**. A window will indicate the code is being loaded to the vManage. A message will indicate the images were uploaded successfully, and the version, software location (vManage), software URL, and available files will be added to the repository.

Step 4: To use a remote file server to upgrade devices, upload the desired files to the remote file server, then configure the URL information on the vManage. Select **Add New Software**, then select **Remote Server** from the drop-down menu. A window will pop up. Fill in the code version (17.2.7) and the FTP or HTTP URL of the file server, including authentication if needed (ftp://admin:c1sco123@192.168.254.51/). Select **Add**. The version, software location (remote), and software URL will be added to the repository list.



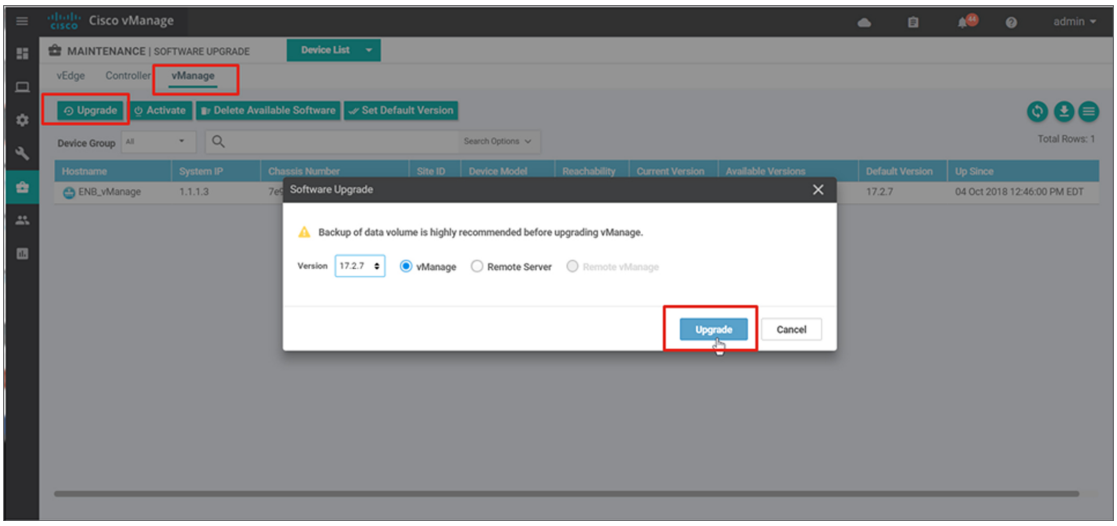
Procedure 2 Upgrade vManage (optional)

It is recommended to back up data before upgrading vManage.

Step 1: Go to **Maintenance > Software Upgrade**, then select the **vManage** tab.

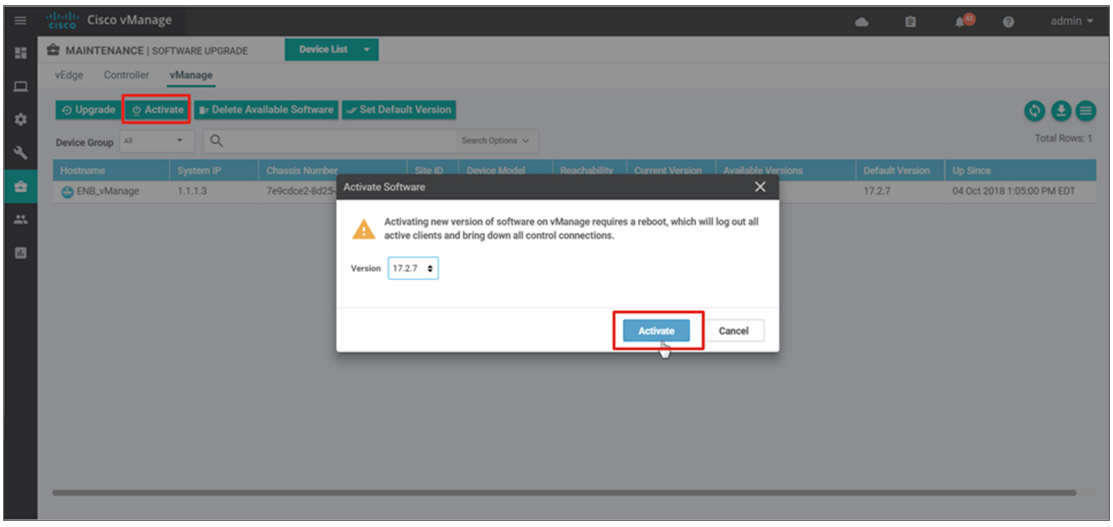
Step 2: Select the **Upgrade** button in the upper left part of the page. This will cause the software to install, but vManage will not reboot and load the new software until the **Activate** button is used.

Step 3: A window pops up. Choose the desired software from the drop-down box. Loading the image from vManage is the default. Select **Upgrade**.



Step 4: The software installation will indicate success. Go back to **Maintenance> Software Upgrade** and select the **vManage** tab. Then, select the **Activate** button.

Step 5: A window will pop up indicating that activating a new version of software on vManage requires a reboot, which will log out active clients and bring down control connections to vManage. Choose the software version from the drop-down box and select **Activate**.



Step 6: When the vManage comes back online, log back in and go to **Maintenance>Software Upgrade**, and select the **vManage** tab to verify the running version under the **Current Version** column.

Procedure 3 Upgrade the vBond and vSmart controllers

In this procedure, the controllers are upgraded directly from an image on the vManage.

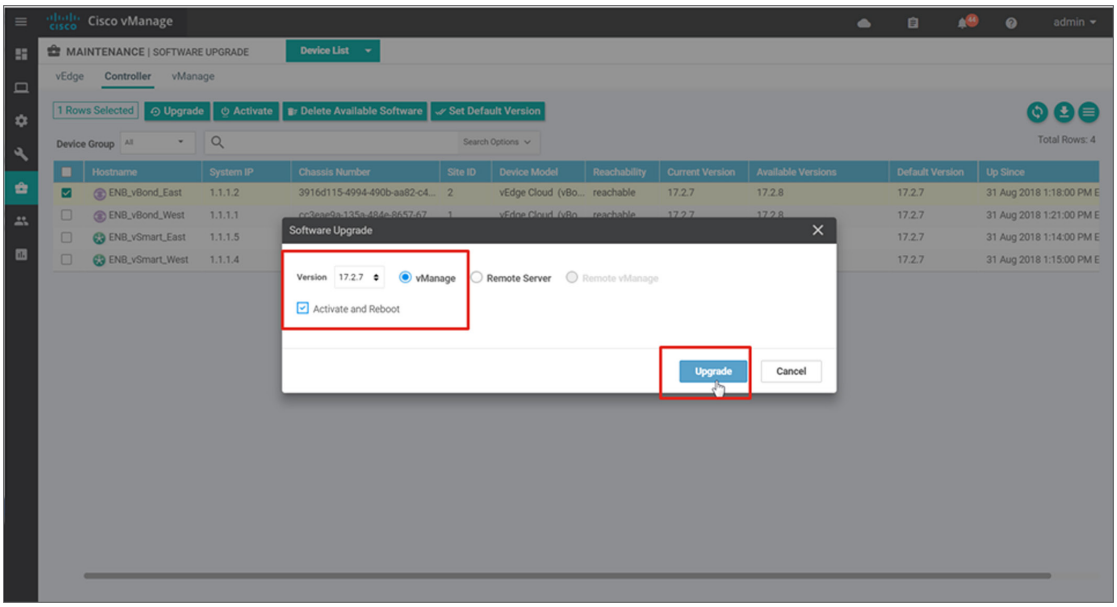
Step 1: Go to **Maintenance > Software Upgrade**, then select the **Controller** tab.

Step 2: Select the box next to a vBond controller you wish to upgrade and select the **Upgrade** button in the top left of the page.

Step 3: A window pops up. Choose the software version, and leave the vManage radio button selected.

Step 4: If you want to immediately activate and reboot after the installation, select the **Activate and Reboot** checkbox. If you do not select the checkbox, you will need to go back to the **Maintenance >Software Upgrade** and select the **Controller** tab to separately activate the software, which reboots the controller and runs the new software. Ensure the checkbox to **Activate and Reboot** is selected, and then select **Upgrade**.

Step 5: Repeat steps 1–4 in order to upgrade the rest of the controllers. You can select more than one at a time



Process

Deploying the data center vEdge routers

1. Verify the global vBond address
2. Put the vEdge routers in staging state (optional)
3. Configure the vEdge via CLI to connect to the controllers
4. Upgrade vEdge routers if necessary
5. Configure basic information section of feature template
6. Configure the transport VPN
7. Configure the Management VPN (optional)
8. Configure the Service VPN
9. Configure additional templates (optional)
10. Create a device template
11. Deploy the device templates to the vEdge routers
12. Create a localized policy
13. Attach localized policy to a device template
14. Add localized policy references in the feature templates
15. Bring vEdge devices out of staging mode

This section assumes the data center firewall, aggregation switches, and CE router have already been configured. Appendix D outlines the relevant code portions on these devices.

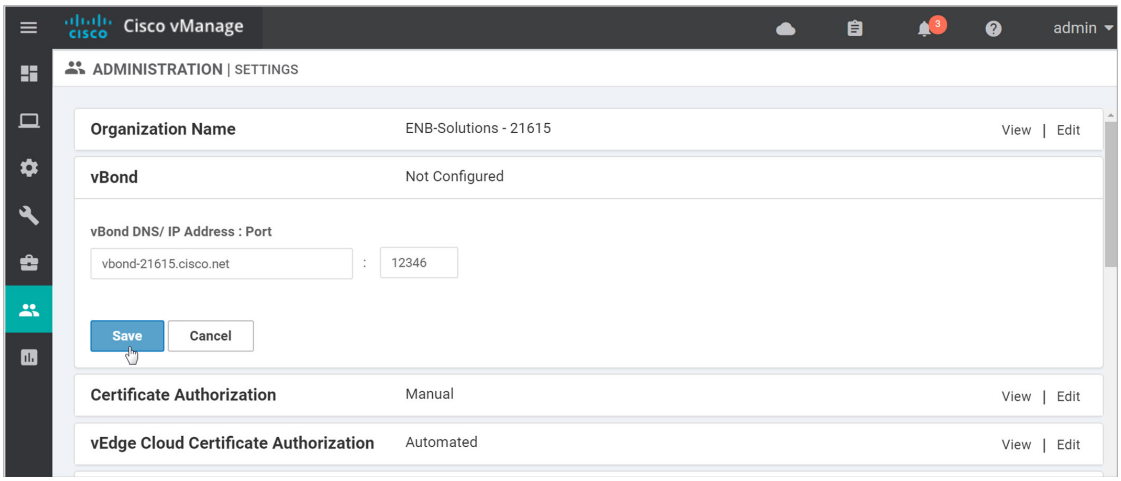
Even though ZTP can be performed, the vEdge routers in the data centers will be manually bootstrapped for connectivity to the vBond orchestrator.

Procedure 1 Verify the global vBond address

You cannot modify the vBond IP address or hostname through feature templates; the vBond orchestrator IP address or hostname listed under the vManage administration settings will be inserted into the configurations of the vEdge routers using feature templates. If this setting is not configured, you will be redirected to configure it when you attempt to configure your first device template.

Step 1: On the vManage GUI, go to **Administration > Settings**. The **vBond** configuration line should be populated with the vBond hostname and port number. If not, it will indicate *Not Configured*.

Step 2: To configure or modify this setting, on the right side of the vBond configuration line, select **Edit**, and enter the vBond IP or DNS address (**vbond-21615.cisco.net**). Select **Save**.



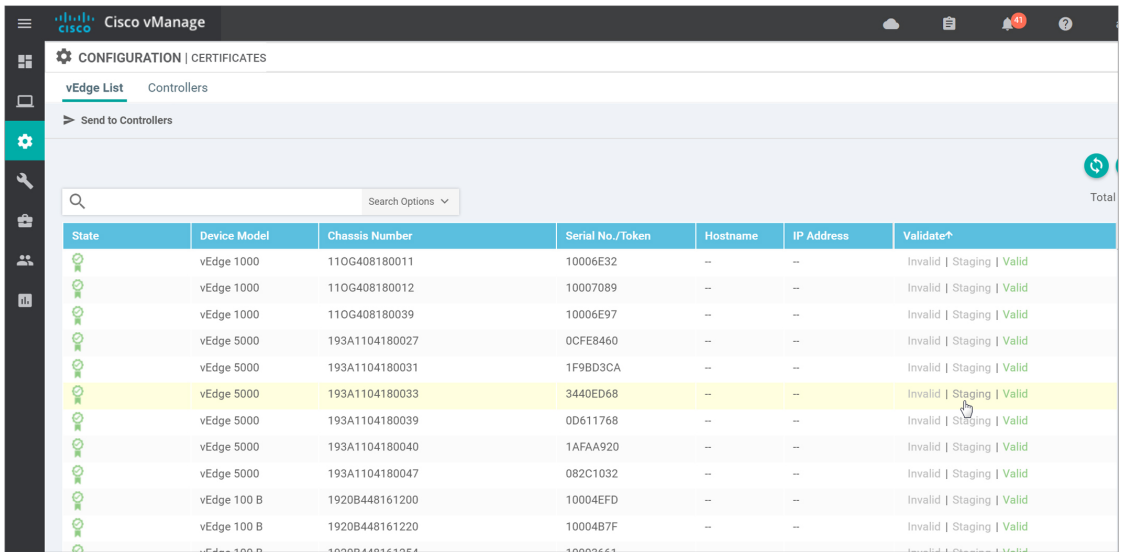
Procedure 2 Put the vEdge routers in staging state (optional)

Before bringing the vEdge routers up onto the network, we can optionally stage them first. This allows for us to bring them up with the control plane, but they will not join the overlay and forward traffic until we put them into a valid state. The vEdge routers will become OMP peers with the vSmart controllers, but no OMP routes will be sent, nor will any local routes be redistributed into OMP.

Step 1: From the vManage GUI, Go to **Configuration > Certificates**. Find the vEdge routers that belong to DC1. You can do this by matching the chassis serial number under the chassis number column by visually inspecting the vEdge router itself, or by executing a show hardware inventory on the vEdge router console:

```
vedge# show hardware inventory
hardware inventory Chassis 0
 version        1.1
 part-number    vEdge-5000
 serial-number  193A1104180033
 hw-description "vEdge-5000. CPLD rev: 0x0, PCB rev: A."
```

Step 2: To the right of the targeted vEdge router, select **Staging**. A pop-up window will ask if you are sure you want to stage. Select **Ok**.



Step 3: Repeat step 2 for the other vEdge router.

Step 4: Be certain to select the **Send to Controllers** button in the upper left portion of the screen when finished.

Procedure 3 Configure the vEdge via CLI to connect to the controllers

Step 1: Console to the vEdge device that will become dc1-ve1. You will get a login prompt. Type in the username and password. The vEdge configuration should be at factory defaults if this is the first time you've logged in. To go back to factory defaults (not common) or view a factory default configuration, see Appendix B.

Tech tip

The controllers in this network are running 17.2.7. If you are trying to bring up a vEdge 5000 onto the network that is on a code version lower than 17.2.5, you may have issues bringing up the control plane. It is recommended to manually upgrade the vEdge router to at least 17.2.5 or greater before attempting to bring the vEdge onto the network. See Appendix C for manual upgrade steps.

Step 2: Configure VPN 0 and the physical interface that will connect to the network to reach the vBond. The DNS server needs to be defined to resolve the vBond hostname and a default route needs to be defined to direct the control packets to the next hop. Copy and paste in the following CLI:

```
config t
vpn 0
 dns 64.100.100.125 primary
ip route 0.0.0.0/0 10.4.1.5
interface ge0/0
ip address 10.4.1.6/30
commit and-quit
```

Step 3: Test connectivity to the vBond orchestrator by issuing a ping to **vbond-21615.cisco.net** at the console. Ensure connectivity succeeds before proceeding.

```
vedge# ping vbond-21615.cisco.net
Ping in VPN 0
PING vbond-21615.cisco.net (64.100.100.51) 56(84) bytes of data.
64 bytes from 64.100.100.51: icmp_seq=1 ttl=63 time=0.380 ms
64 bytes from 64.100.100.51: icmp_seq=2 ttl=63 time=0.538 ms
64 bytes from 64.100.100.51: icmp_seq=3 ttl=63 time=0.499 ms
```

Step 4: Configure the necessary system parameters. This includes the **system-ip**, **site-id**, **organization name**, and **vbond** IP address or hostname. The **system host-name** is also defined to make the device more easily recognizable in vManage. Copy and paste in the following CLI:

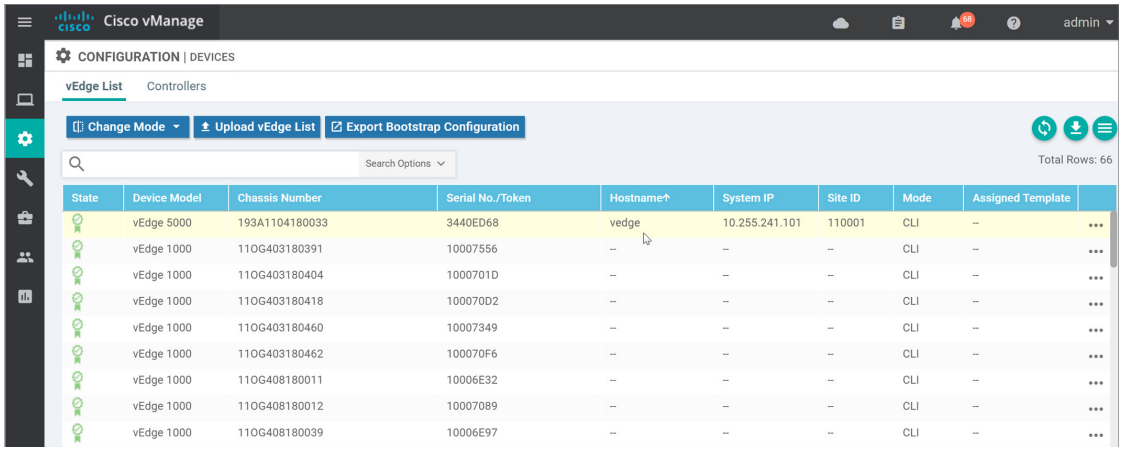
```
config t
system
host-name dc1-ve1
system-ip 10.255.241.101
site-id 112001
organization-name "ENB-Solutions - 21615"
vbond vbond-21615.cisco.net
commit and-quit
```

Step 5: Verify the control connections. A **show control summary** will initially show four connections–one to the vBond orchestrator, one to vManage and one to each of the vSmart controllers. Then the vBond connection will terminate and connections to vManage and the vSmart controllers remain up.

```
vedge# show control summary
control summary 0
 vbond_counts   0
 vmanage_counts 1
 vsmart_counts  2
```

The command**, show control connections,** will show additional details.

On vManage, the vEdge router shows up in the **Configuration > Devices** output.



Step 6: Repeat steps 2 through 5 for the second vEdge router using the following bootstrap configuration commands:

```
config t
vpn 0
 dns 64.100.100.125 primary
ip route 0.0.0.0/0 10.4.2.5
interface ge0/0
ip address 10.4.2.6/30
      system
       host-name dc1-ve2
       system-ip 10.255.241.102
 site-id 112001
 organization-name "ENB-Solutions - 21615"
 vbond vbond-21615.cisco.net
 commit and-quit
```

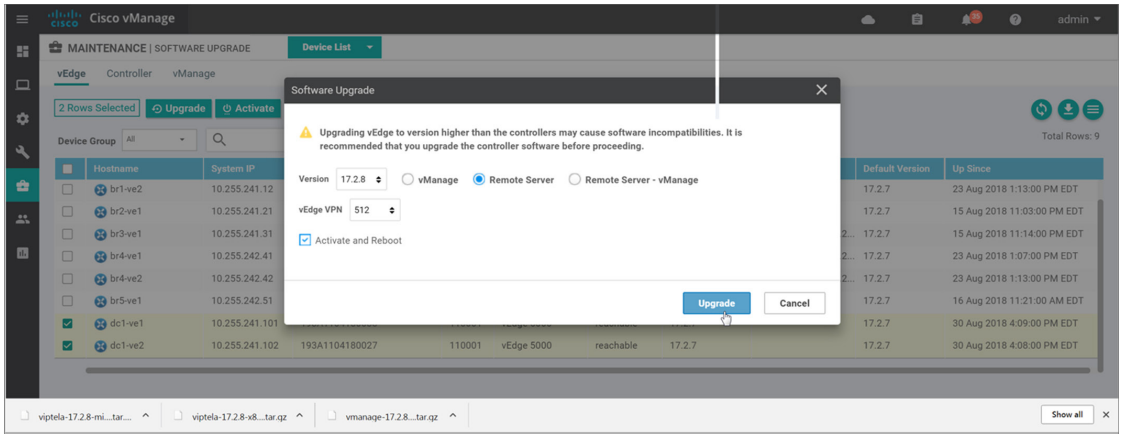
You can refresh the vManage page if needed to view the second vEdge when it appears in vManage.

Procedure 4 Upgrade vEdge routers if necessary

Step 1: Go to **Maintenance > Software Upgrade** to check the code versions (see **Current Version** column).

Step 2: If an upgrade is needed, select the check boxes next to the two vEdge routers and select **Upgrade**. A window pops up.

Step 3: Select the new code version from the drop-down box, and select the **Remote Server** radio button. Select the VPN where the vEdge can reach the remote server. In this case, it is VPN 512. Select the **Activate and Reboot** check box and select **Upgrade**. The vEdge devices will retrieve the software from the remote file server, install it, and then reboot in order to activate it.



Procedure 5 Configure basic information section of feature template

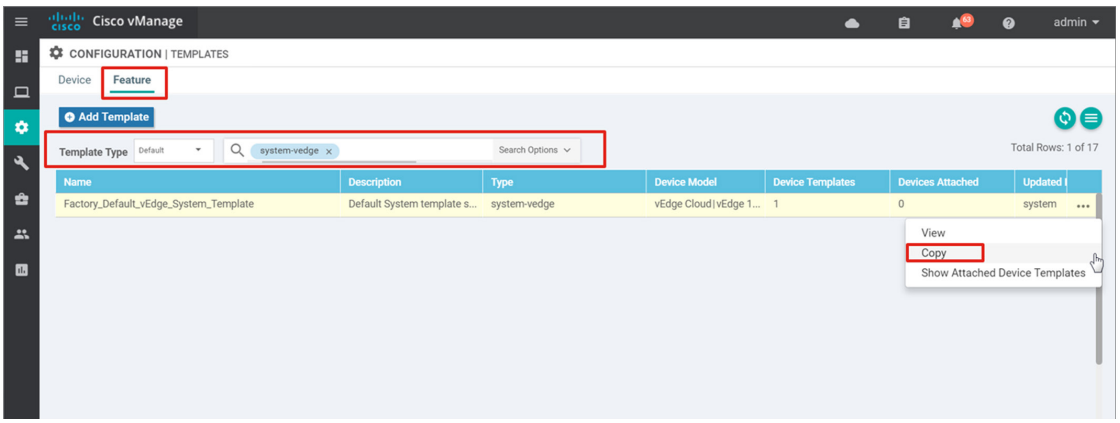
In this section, the feature templates that fall under the basic information section of the device template will be configured. This includes system settings, logging, Network Time Protocol (NTP), AAA, OMP, Bidirectional Forwarding Detection (BFD), and security feature templates.

System

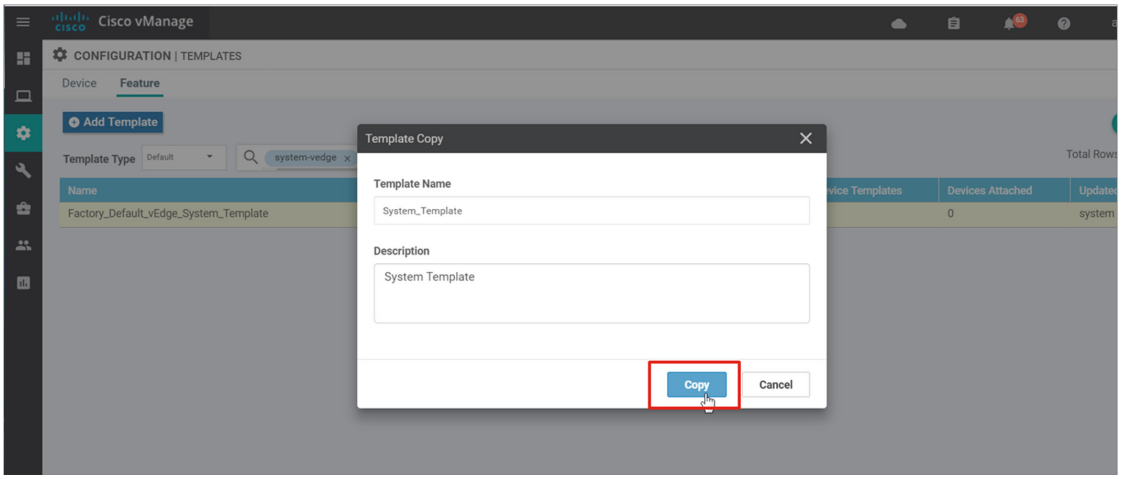
The following steps show a system template being created by copying the default system template for a vEdge device. You create variables for different parameters, including latitude and longitude, so that the feature template can be used across most vEdge devices. Latitude and longitude values allow us to view the vEdge location on the vManage map located at **Monitor > Geography** on the vManage GUI.

Step 1: From **the Configuration > Templates** page, ensure that the **Feature** tab is selected. Select **Default** from the drop-down box next to **Template Type** to view a list of all of the default feature templates.

Step 2: Type **system-vedge** into the search box and press return. One template is listed. Select **...** next to the template called *Factory_Default_vEdge_System_Template* and select **Copy**.

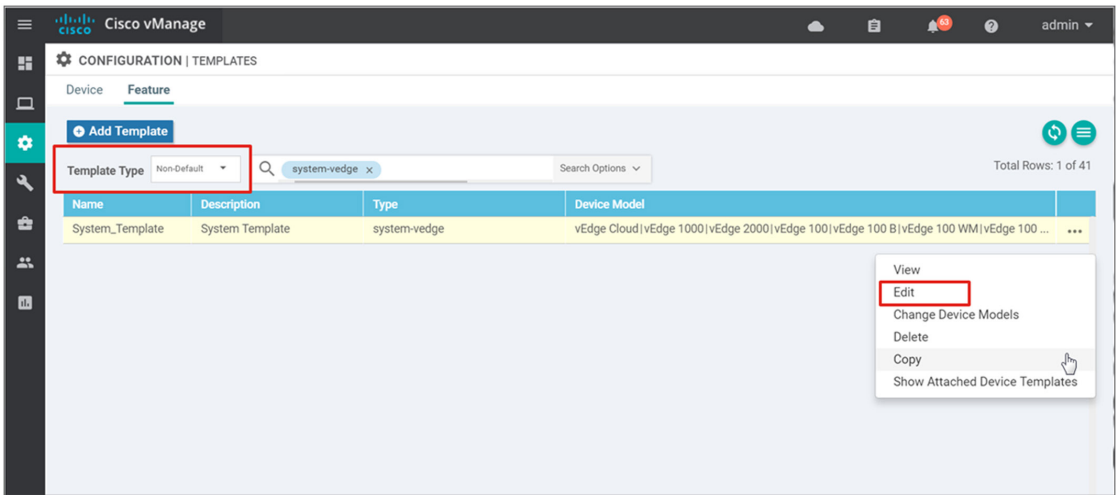


In the pop-up window, enter the template name **System_Template** and description **System Template** and select **Copy**.



Step 3: Back at the feature template main screen, select **Non-Default** from the **Template Type** drop-down box. The text, **system-vedge**, is still enabled in the text search box. The newly copied system feature template is listed.

Step 4: To the right of the feature template called *System_Template*, select **...** and select **Edit**.



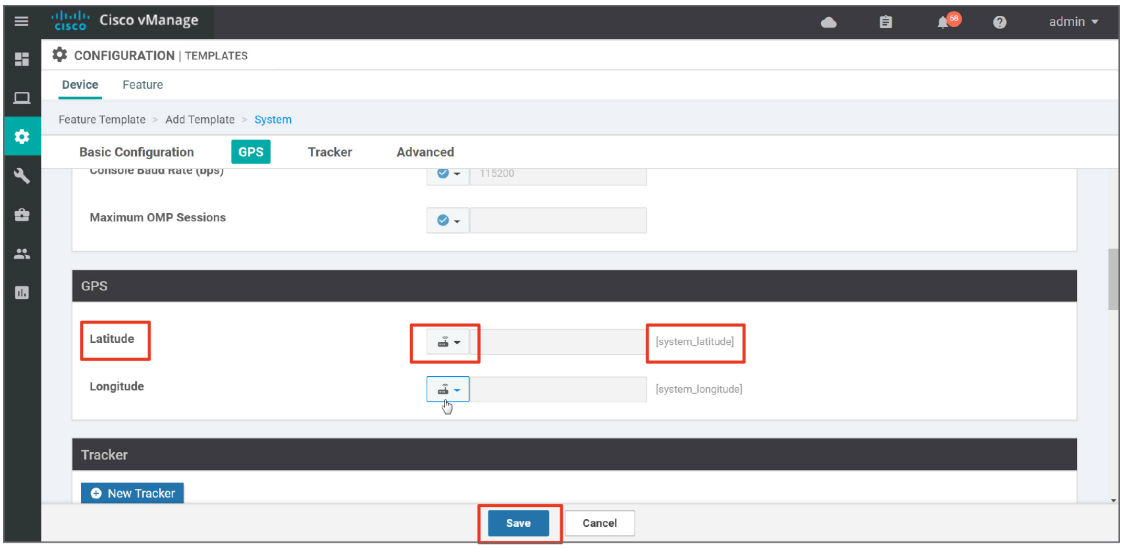
The system feature template configuration is displayed. The **Device Type** field is inherited by the template it is copied from, which is all device types in this case. By default, there are parameter variables already created for **Site ID, System IP,** and **Hostname** (**system_site_id, system_system_ip,** and **system_hostname**).

Step 5: Device groups can help organize and group common vEdge routers when using the vManage GUI for upgrading and monitoring. For example, you can organize vEdge routers according to type or location, and put them into various upgrade groups during upgrade procedures. Next to **Device Groups**, choose **Device Specific** from the drop-down box. Use the variable name **system_device_groups**.

Step 6: Next to latitude, choose **Device Specific** from the drop-down box. Keep the default variable name, **system_latitude** (or you can change the variable name by clicking the text box and typing a new variable name).

Step 7: Repeat step 5 for **Longitude (system_longitude), Port Hopping (system_port_hop), and Port Offset (system_port_offset).** Default configurations are used for everything else, such as **Timezone** (**UTC**) and **Console Baud Rate** (**115200**).

Step 8: Select **Update**.



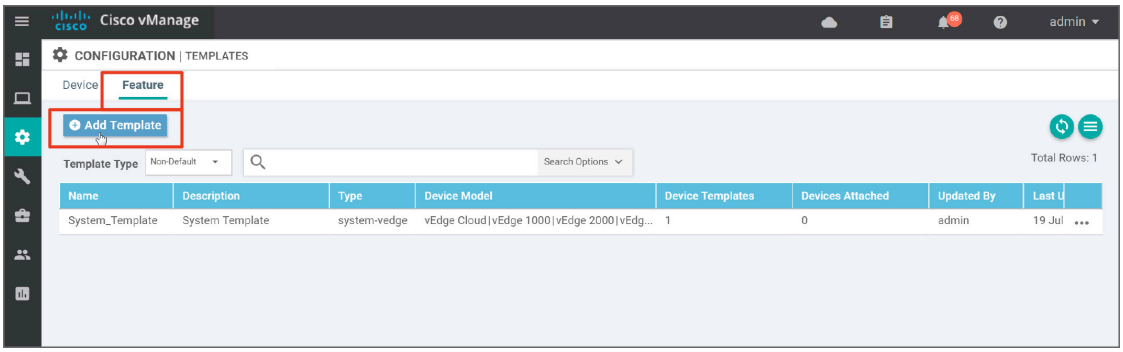
The following table summarizes the parameters configured in the system feature template:

Table 14. System feature template settings

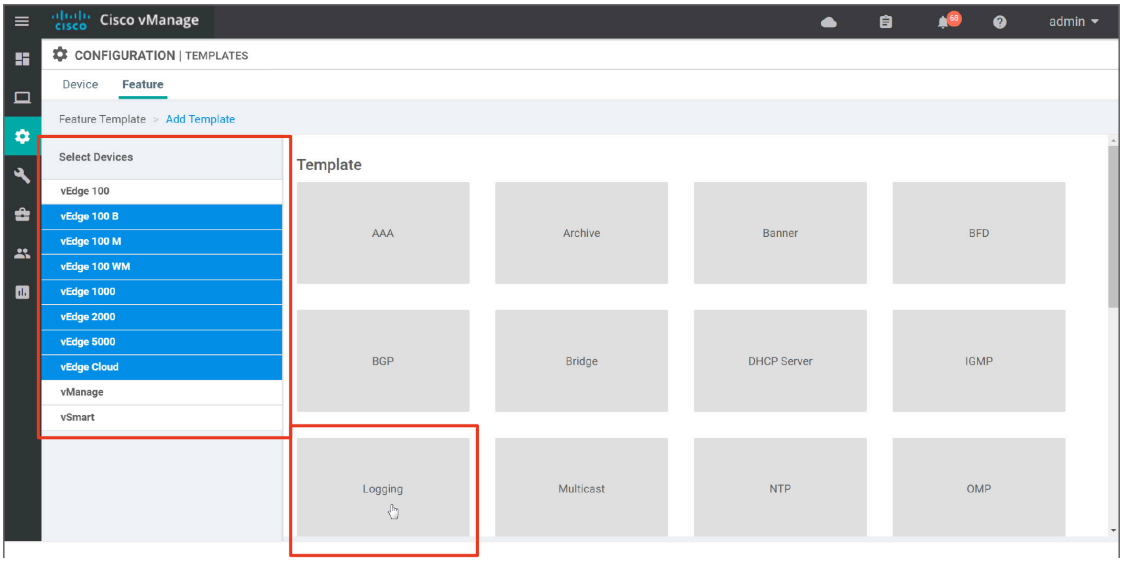
Section	Parameter	Type	Variable/value
Basic configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_hostname
	Device Groups	Device Specific	system_device_groups
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset

Logging

Step 9: To create a logging feature template, go to **Configuration > Templates** and select the **Feature** tab. Select the **Add Template** button.



Step 10: Select the devices this template will apply to from the left side. Click on the **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, and **vEdge Cloud** since we can apply this template to any device in the network. Select the **Logging** template block on the right.

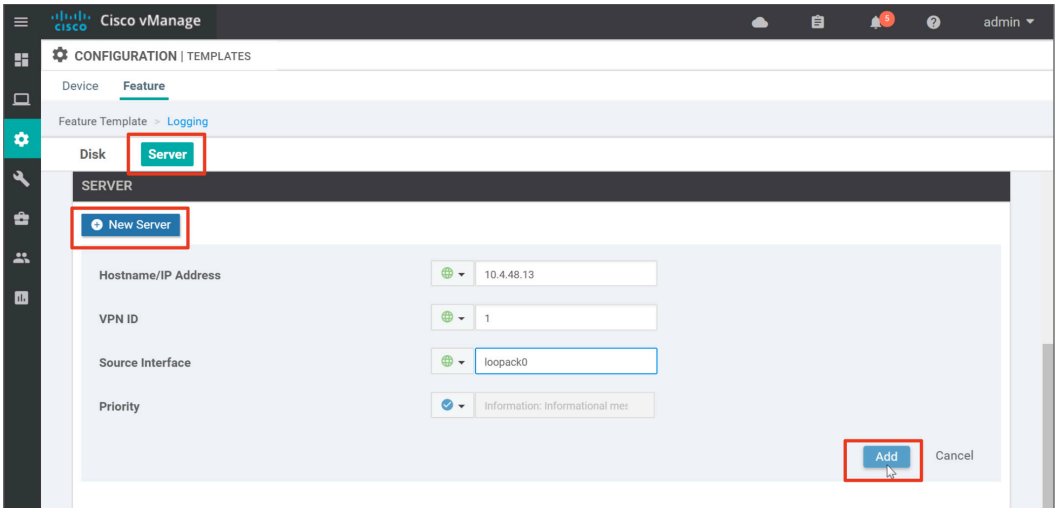


Step 11: The **Logging** template is presented. Fill in the **Template Name** (**Logging_Template**) and **Description** (**Logging Template**)

Step 12: Select **Server** in order to jump to the logging server section of the template. Select the **New Server** button. In the **Hostname/IP Address** box, type in the logging server hostname or IP address (**10.4.48.13** in this example). By default, this is a **Global** value, which means the value of **10.4.48.13** will be applied to all devices this template is applied to. Alternatively, this could have been defined as a **Device Specific** variable instead.

Step 13: For **VPN ID**, select **Global** from the drop-down box and type **1**, which references the service VPN number that will be created. The logging server, which sits in the data center, should be reachable from any site's local network. For remote sites, traffic will traverse over the tunnel to reach the data center.

Step 14: For **Source Interface**, select **Global** from the drop-down box and type **loopback0** into the text box. We want to source logging messages from loopback0, which will be the system IP for the device so we can better correlate the events on vManage.



Tech tip

Because loopback0 is referenced in this template as the source interface for logging messages, loopback0 must be defined somewhere within a referenced feature template. If loopback0 is not defined but is referenced within the logging template, the configuration push will fail when the device template is deployed to the devices.

Step 15: By default, events are also still logged to the local disk. For priority, informational messaging is the default. Select the **Add** button to add the logging server configuration to the feature template.

Tech tip

If you forget to select the **Add** button before you select the **Save** or **Update** button to save or update changes to the feature template, your logging server configurations will be lost and you will need to edit the template and re-configure.

Step 16: Select the **Save** button to complete template.

The following table summarizes the parameters configured in the logging feature template:

Table 15. Logging feature template settings

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	10.4.48.13
	VPN ID	Global	1
	Source Interface	Global	loopback0

Continue creating the NTP, AAA, OMP, BFD, and security templates.

Network Time Protocol (NTP)

In the NTP template, the devices will use an NTP server located on the Internet, **time.nst.gov** which is reachable through the transport VPN, VPN 0. Keeping correct time is important because certificates are used to authenticate and connect to the controllers. Connection to the vSmart controllers is needed before IPSec tunnels can be formed and connectivity to the data center restored from the branches. In order for NTP to work properly, a DNS server to resolve the NTP hostname will be required in the transport VPN. In addition, the NTP protocol needs to be allowed on the tunnel interface or NTP will not work in the transport VPN. DNS and allowed protocols are configured in the VPN interface templates configured later in this guide.

Step 17: Assuming that you are still on the feature templates page, select the **Add Template** button. Create the NTP template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

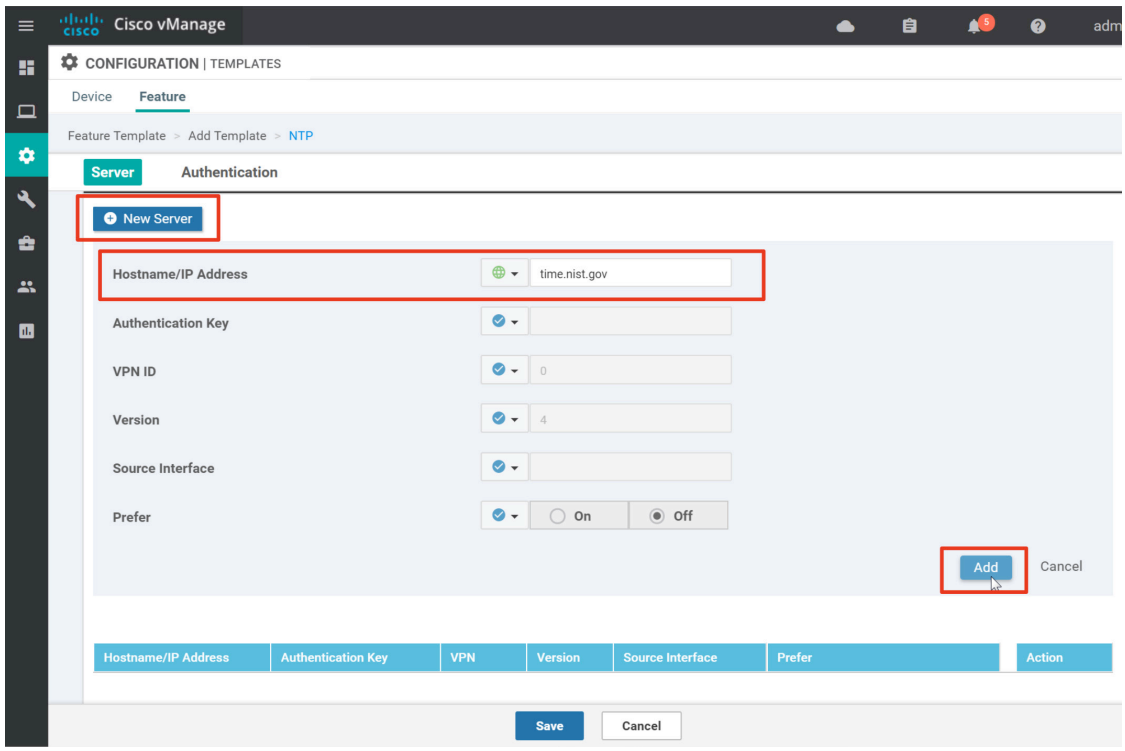
Template: NTP

Template Name: **NTP_Template**

Description: NTP Template

Step 18: In the **Server** section, select the **New Server** button, and type **time.nst.gov** in the **Hostname/IP Address** box. There is no authentication configured and the **VPN ID** by default is 0.

Step 19: Select **Add**. Add any additional servers as needed.



Tech tip

If you choose to use authentication, configure the **Authentication** part of the NTP feature template before you configure the **Server** section. If you try to configure the **Server** section first and are using an authentication key, you will get an invalid value indication (since it hasn't been created yet) and will not be able to add the server information while still referencing a non-existent authentication key.

Step 20: Select **Save** to complete the template.

The following table summarizes the parameters configured in the NTP feature template.

Table 16. NTP feature template settings

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	time.nst.gov

AAA

In the AAA feature template, local authentication is defined and the admin password will become a variable to simplify any future password changes as required.

Step 21: Assuming that you are still on the feature templates page, select the **Add Template** button. Create the AAA template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

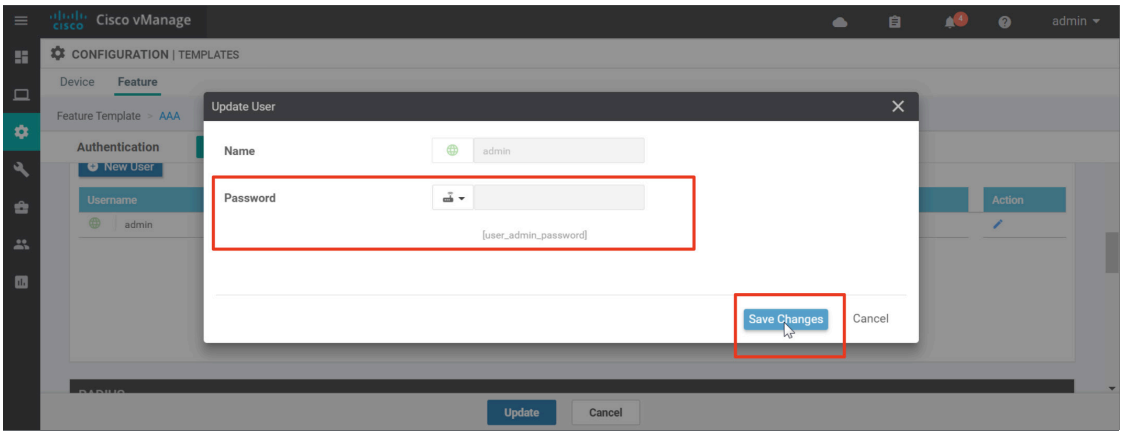
Template: AAA

Template Name: **AAA_Template**

Description: AAA Template

Step 22: Under the **Authentication Order** parameter, deselect **radius** and **tacacs** from the drop-down box (so only the **local** method is left). Click outside the box to close the drop-down menu.

Step 23: To change the **admin** password to a variable under the **Local** section, select the pencil under the **Action** column for the **Username admin**. A pop-up window will appear. Change the drop-down menu next to **Password** as **Device Specific**, and use the variable **user_admin_password** in the text box. Select the **Save Changes** button, which will close the pop-up window and save the changes made.



Step 24: Select **Save** to complete the template.

The following table summarizes the parameters configured in the AAA feature template.

Table 17. AAA feature template settings

Section	Parameter	Type	Variable/value
Authentication	Authentication order	Drop-down	local
Local	User/admin/ Password	Device Specific	user_admin_password

Overlay Management Protocol (OMP)

In the OMP feature template, the **Number of Paths Advertised per Prefix** and the **ECMP Limit** parameters will be changed from the default of four to the maximum number of 16. By default, connected and static routes and OSPF, with the exception of external OSPF routes, are redistributed into OMP. This will be disabled at the global level but will be enabled in the service VPN templates where needed.

Step 25: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button. Create the OMP template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: OMP

Template Name: **OMP_Template**

Description: OMP Template

Step 26: Configure the following parameters:

Table 18. OMP Feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Number of paths advertised per prefix	Global	16
Basic configuration	ECMP limit	Global	16
Advertise	Connected	Global	Off
	Static	Global	Off

Step 27: Select **Save** to complete the template.

Bidirectional Forwarding Detection (BFD)

In the BFD feature template, BFD is configured for each transport, the timers are adjusted, and path MTU discovery is disabled. For the timers, the multiplier is kept at six and the poll interval adjusted to 120000 milliseconds.

Step 28: Assuming that you are still on the feature templates page, select the **Add Template** button. Create the BFD template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: BFD

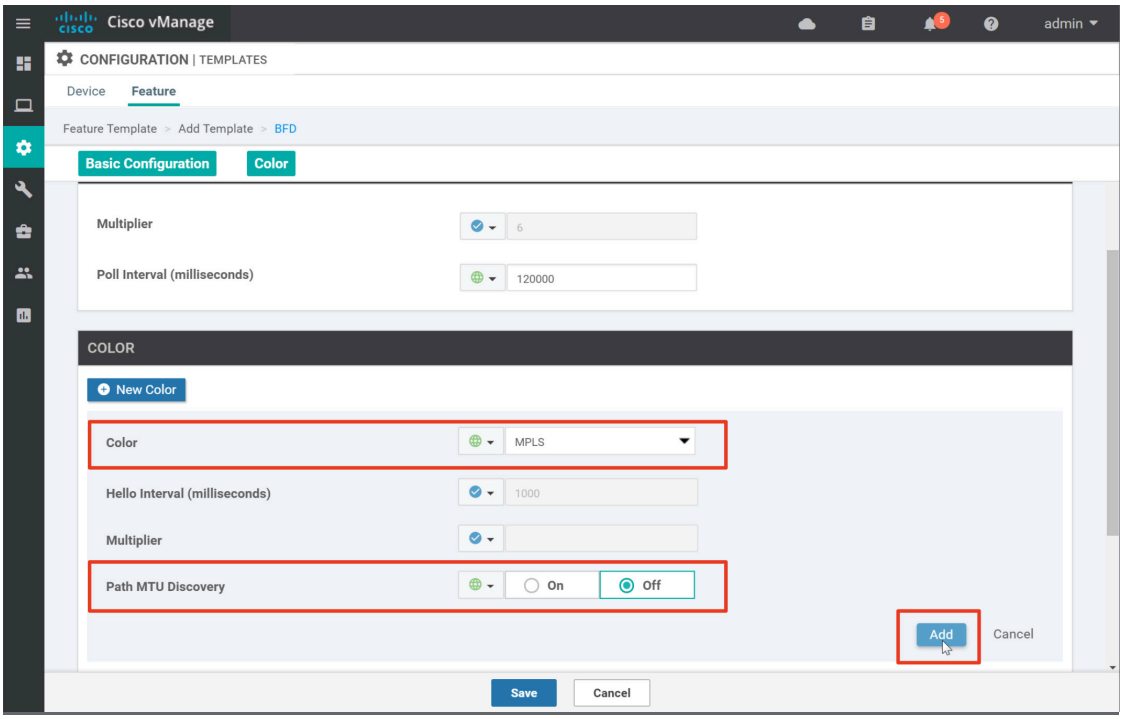
Template Name: **BFD_Template**

Description: BFD Template

Step 29: Under **Basic Configuration** next to **Poll Interval**, select **Global** and type in **120000** in the text box.

Step 30: For the **Color** section, select the **New Color** button, choose the transport color (MPLS) from the drop-down box, select **Global** and **Off** for **Path MTU Discovery**, then select **Add** to add the BFD transport configuration to the template.

Step 31: Repeat step 30 for the other transport (Biz Internet).



Step 32: Select **Save** to complete the template.

The following table summarizes the parameters configured in the BFD feature template.

Table 19. BFD feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Poll Interval	Global	120000
Color (MPLS)	Color	Drop-down	MPLS
	Path MTU	Global	Off
Color (Biz internet)	Color	Drop-down	Biz internet
	Path MTU	Global	Off

Security

In the security feature template, the anti-replay window is configured to the recommended value of 4096 Bytes.

Step 33: Assuming that you are still on the feature templates page, select the **Add Template** button. Create the security template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: Security

Template Name: **Security_Template**

Description: Security Template

Step 34: Configure the following parameters:

Table 20. Security feature template settings

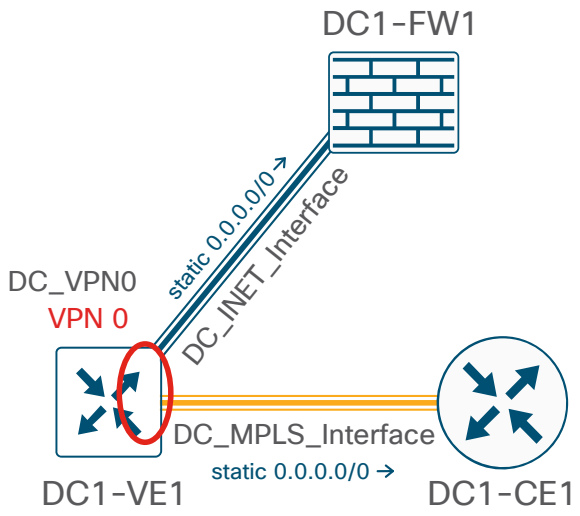
Section	Parameter	Type	Variable/value
Basic configuration	Replay window	Global/ drop-down	4096

Step 21: Select **Save** to complete the template.

Procedure 6 Configure the transport VPN

For the data center, the transport VPN, or VPN 0 feature template, needs to be created. In the VPN template, you configure Equal-Cost Multipath (ECMP) keying, DNS, and static routes. You then define the physical interfaces for each of the transports, the MPLS and Internet interfaces. In those templates, you configure interface names, IP addresses, and IPSec tunnel characteristics.

Figure 13. Data center vEdge transport templates



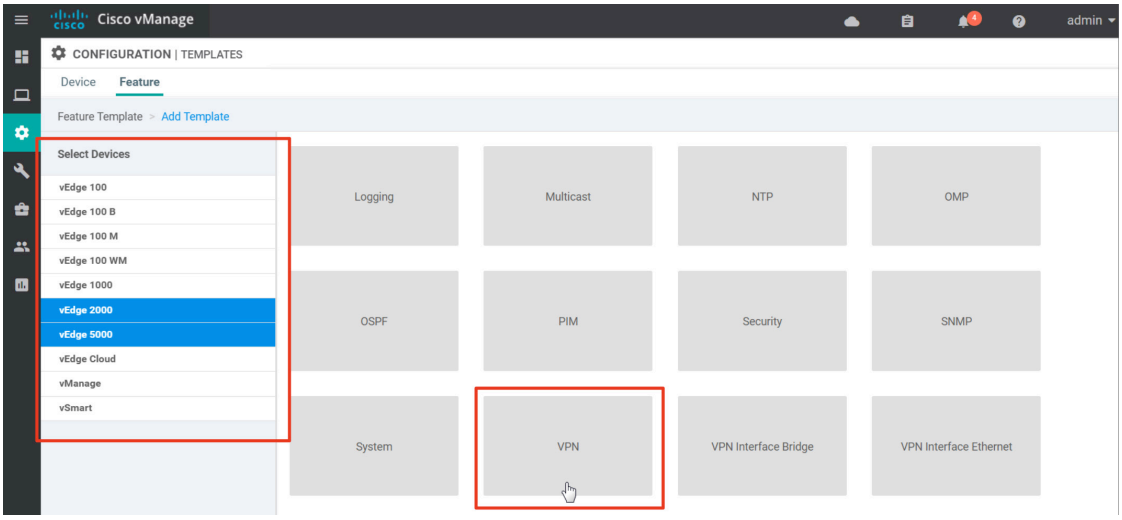
Transport VPN (VPN 0)

Step 1: In the vManage GUI, Select **Configuration > Templates**, and choose the **Feature** tab.

Step 2: Select the **Add template** button.

For the VPN-specific configurations, the data center templates stay separate from the branch templates, so a change in the branch template configurations do not inadvertently change the configurations at the data center.

Step 3: Under the **Select Devices** column, choose **vEdge 5000** and **vEdge 2000,** or additional vEdge device types that may reside at the data center. Select the **VPN** Template block to the right.



Step 4: Configure **Template name** and **Description**:

Template Name: **DC _VPN0**

Description: DC Transport VPN 0

Step 5: Under **Basic Configuration** next to **VPN**, configure **0** as the **VPN ID**.

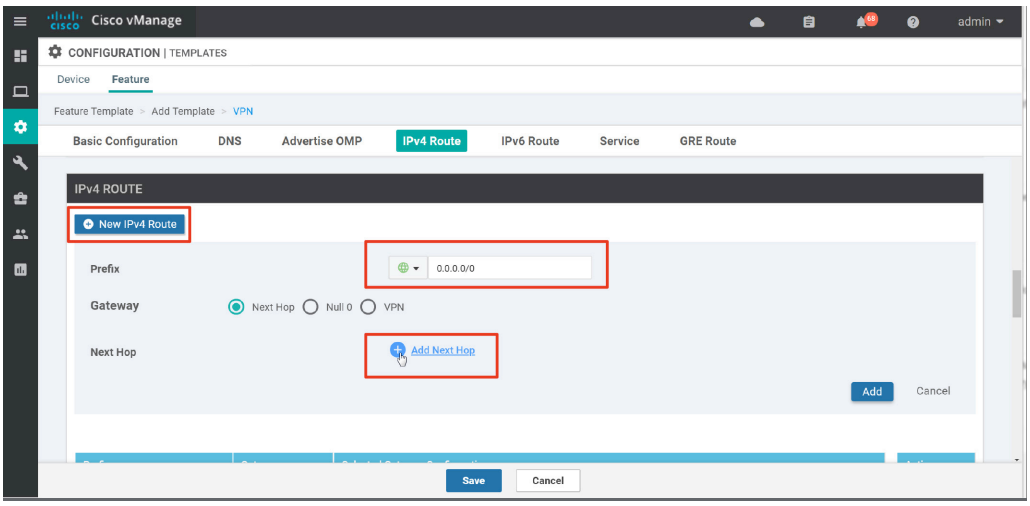
Step 6: Next to **Name**, select **Global** from the drop-down menu, and type **Transport VPN**, a description for the VPN.

Step 7: Next to **Enhance ECMP Keying**, select Global from the drop-down menu, and select **On**. Enabling this feature configures the ECMP hashing to use the layer 4 source and destination ports in addition to the source and destination IP address, protocol, and Differentiated Services Code Point (DSCP) field as the ECMP hash key. ECMP is used when there are equal-cost routing paths in the VPN and traffic uses a hash on key fields in the IP header to determine which path to take.

Step 8: Under **DNS** and next to **Primary DNS Address**, select **Global** from the drop-down menu and enter **64.100.100.125**. The **Secondary DNS Address** box appears. Select **Global** from the drop-down menu and enter **64.100.100.126** in the **Secondary DNS Address** text box.

Under the **IPv4 Route** template section, default routes are added for each interface. These routes are used in order for the tunnel endpoint to bring up tunnels with the neighboring sites. Multiple default routes can exist because the vEdge uses the physical tunnel endpoint source as well as the destination when making a routing decision.

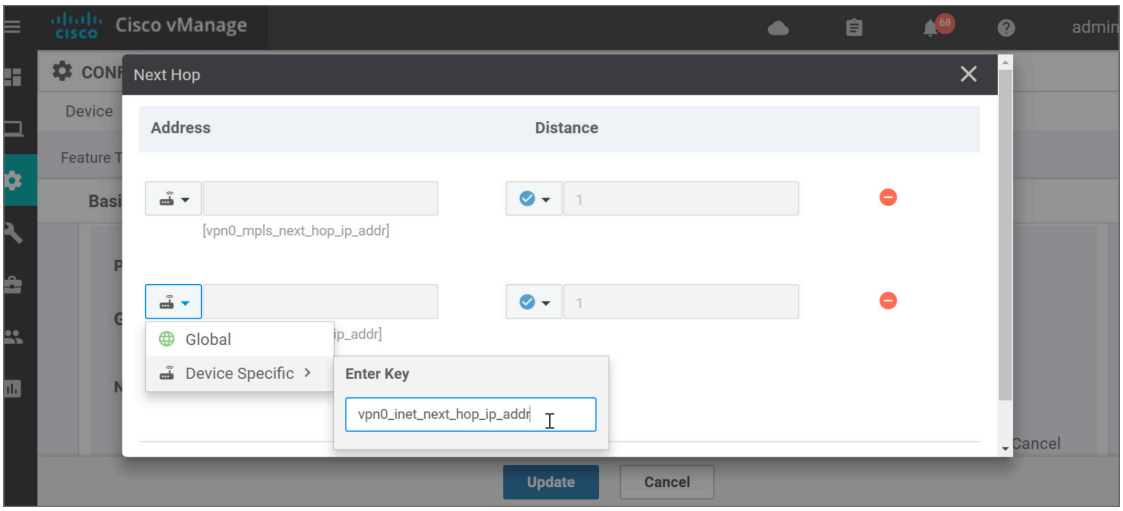
Step 9: Under the **IPv4 Route** section, select the **New IPv4 Route** button. Add **0.0.0.0/0** in the **Prefix** box and select **Add Next Hop**.



Step 10: A pop-up window appears that prompts you to add your first next hop. Select the **Add Next Hop** button.

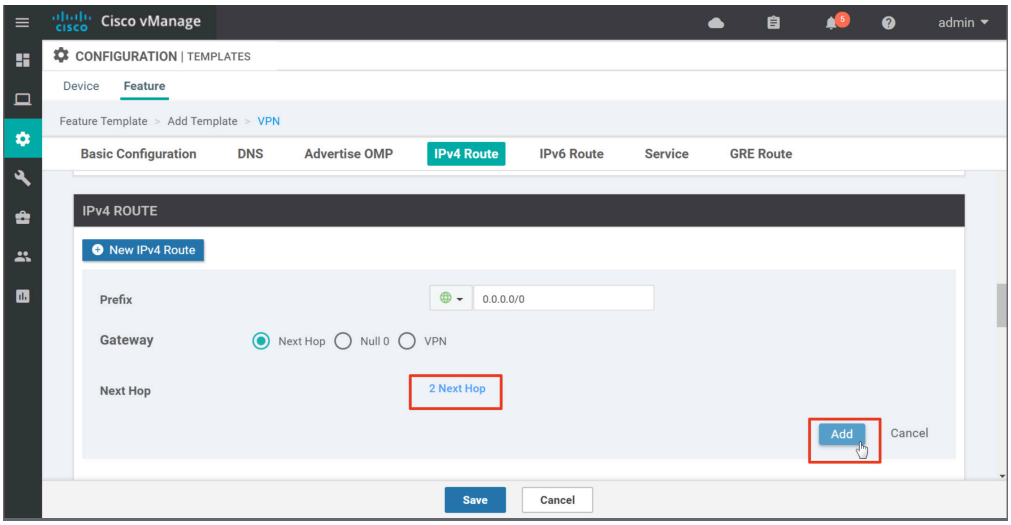
Step 11: Since this template applies to more than one vEdge, the next hop parameters are variables instead of global values. On the pop-up window, under **Address**, select **Device Specific** from the drop-down menu, and type in the next-hop IP address variable for the MPLS transport in the text box (**vpn0_mpls_next_hop_ip_addr**). Select **Add Next Hop** to add the second next hop.

Step 12: Under **Address** on the second next-hop entry, select **Device Specific** from the drop-down menu, and type in the next-hop IP address variable for the MPLS transport in the text box (**vpn0_inet_next_hop_ip_addr**).



Step 13: Select **Add** at the bottom of the popup. This stores both next hops for the prefix **0.0.0.0/0**. When you return to the feature template page, you will need to press **add** again in order to add the prefix **0.0.0.0/0** along with its next-hop information into the template.

Step 14: The **Next Hop** field will now indicate that there are **2 Next Hop** entries configured. Press **Add** to add the prefix **0.0.0.0/0** to the template.



Step 15: Select **Save** to create the template.

The following table summarizes the parameters configured in the VPN 0 feature template:

Table 21. VPN 0 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	64.100.100.125
	Secondary DNS Address	Global	64.100.100.126
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn0_mpls_next_hop_ip_addr
Basic configuration	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

Next, you configure the interfaces under the transport VPN.

VPN interface (MPLS)

Step 16: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button. Create the VPN Interface template using the following device types, template type, template name, and description:

Select Devices: vEdge 5000, vEdge 2000

Template: VPN Interface Ethernet

Template Name: **DC_ MPLS_Interface**

Description: DC MPLS Interface

Step 17: Under the **Basic Configuration** section next to **Shutdown**, select **Device Specific** and type in the variable name **vpn0_mpls_int_shutdown**. By defining the port status as a variable, the port can be turned up or down for any reason by just modifying the variable value and without having to modify the feature template.

Step 18: Under the **Basic Configuration** section next to **Interface Name**, select **Device Specific** and type in the variable name **vpn0_mpls_int_gex/x**. By defining the interface name as a variable, the interface can be modified for any reason through a variable instead of having to modify the feature template.

Step 19: Under **Basic Configuration** next to **Description**, select **Global** and type in **MPLS Interface** to describe the interface.

Step 20: Under **Basic Configuration** under **IPv4 Configuration** next to **IPv4 Address**, select **Device Specific** and type in the variable name **vpn0_mpls_int_ip_addr/maskbits.**

Step 21: Under **Basic Configuration**, next to **Bandwidth Upstream**, select **Device Specific** and type in the variable name **vpn0_mpls_int_bandwidth_up**. Next to **Bandwidth Downstream**, select **Device Specific** and type in the variable name **vpn0_mpls_int_bandwidth_down**. These two parameters cause vManage notifications, Simple Network Management Protocol (SNMP) traps, and logging messages to be sent when the bandwidth usage reaches 85% or greater than the configured bandwidth.

Step 22: Under **Tunnel** and next to **Tunnel Interface**, select **Global** and select **On**. When you select **On**, additional parameters for the tunnel are shown. Next to **Color**, select **Global** and select **mpls** from the drop-down text box. Next to **Restrict**, select **Global** and select **On**. Restrict means that only tunnels will be formed with other endpoints of the same color.

By default when the tunnel is enabled, the physical interface accepts DTLS/TLS and IPSec traffic in the case of vEdge. In addition, other services can be enabled and accepted into the physical interface unencrypted - this includes DNS, DHCP, and Internet Control Message Protocol (ICMP), by default. Other protocols include SSH, NETCONF, NTP, BGP, OSPF, and STUN. It is a best security practice to minimize the allowed protocols through. In the example network, for initial troubleshooting purposes, ICMP stays enabled and DHCP is turned off for the MPLS interface since the IP address on the interface is static. NTP and DNS are allowed through since the MPLS transport can route through the data center to reach the Internet.

Step 23: Under **Tunnel** and the **Allow Service** section, next to **DHCP**, select **Global** and select **Off**. Next to **NTP**, select **Global** and select **On**.

Step 24: Below the **Allow Service** section, select the **Advanced Options** text. The **Encapsulation** section is revealed. Next to **Preference**, select **Device Specific** and configure the variable as **vpn0_mpls_tunnel_ipsec_preference**. The IPSec tunnel preference allows you to prefer one tunnel over another depending on the preference value.

Step 25: Under the Advanced section next to **TCP MSS**, select **Global** and type **1350** in the text box. This configures the maximum segment size of the TCP packets.

Step 26: Under the **Advanced** section next to **Clear-Don't-Fragment**, select **Global** and select **On**. This clears the DF bit setting and allows packets larger than the Maximum Transmission Unit (MTU) of the interface to be fragmented.

Step 27: Press the **Save** button to create the template.

The following table summarizes the parameters configured in the feature template:

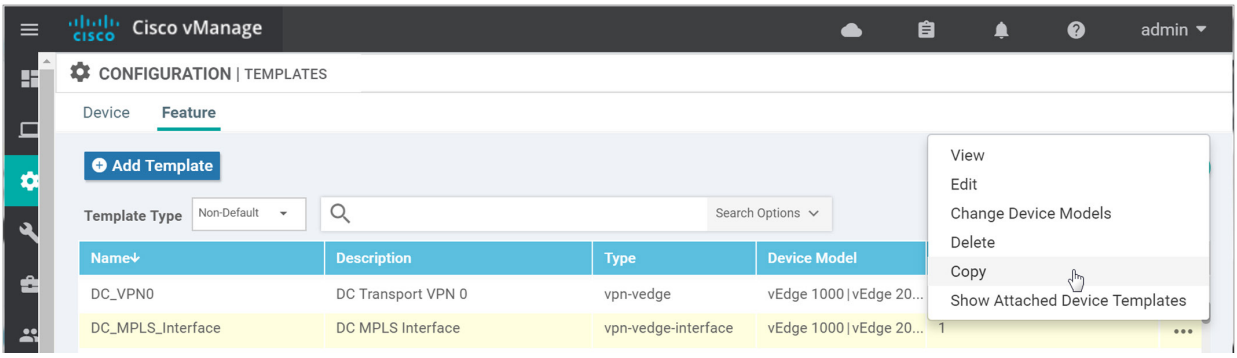
Table 22. VPN 0 VPN interface Ethernet feature template settings (MPLS)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x
	Description	Global	MPLS Interface
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
	Allow Service>DHCP	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Next, the Internet interface under the transport VPN is configured. The template should be very similar to the MPLS VPN interface template with the exception of variable names.

VPN interface (Internet)

Step 28: Assuming that you are still on the **Feature Templates** page, find the feature template just created (**DC_MPLS_Interface**) and select **...** to the far right. Select **Copy**.

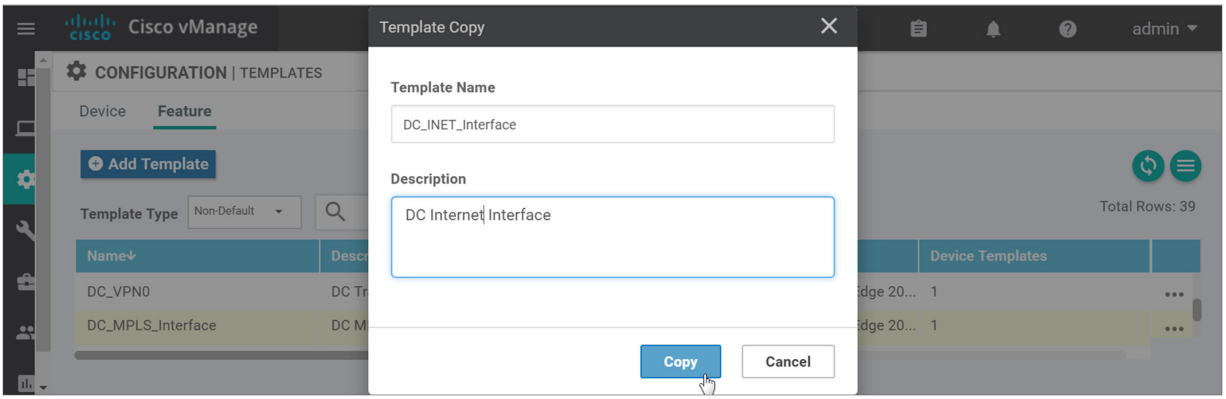


Step 29: On the pop-up window, define the template name and description as:

Template Name: **DC_INET_Interface**

Description: **DC Internet Interface**

Step 30: Select the **Copy** button. The feature template is created and is now in the list with the other created feature templates.



Step 31: Select **...** to the right of the newly-created feature template (**DC_INET_Interface**) and select **Edit** to modify the template.

Step 32: Modify the interface description, variables, and tunnel color.

The following table summarizes the parameters in the feature template.

Table 23. VPN 0 Interface Ethernet feature template settings (Internet)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x
	Description	Global	Internet Interface
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/maskbits
Basic configuration	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
	Restrict	Global	Off
	Allow Service>DHCP	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 33: Once configuration changes have been made, select the **Update** button to save the changes to the feature template.

Procedure 7 Configure the Management VPN (optional)

This configures the out-of-band management VPN. This VPN is always VPN 512, and this VPN cannot be used for any other purpose. This template can be applied to any vEdge router.

Step 1: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button. Create the VPN 512 template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: VPN

Template Name: **VPN512_Template**

Description: VPN 512 Out-of-Band Management

Step 2: Configure the parameters in the following table.

Table 24. Table-24. VPN512 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	512
	Name	Global	Management VPN
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn512_mgt_next_hop_ip_addr

Step 3: Select **Save** to create the feature template.

Next, the interface under the management VPN needs to be configured.

VPN interface (VPN512)

Step 4: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button.

Step 5: Create the VPN 512 interface template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: VPN Interface Ethernet

Template Name: **VPN512_Interface**

Description: VPN 512 Management Interface

Step 6: Configure the parameters in the following table.

Table 25. VPN 512 interface feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgt_int_mgmt0_or_gex/x
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_mgt_int_ip_addr/maskbits

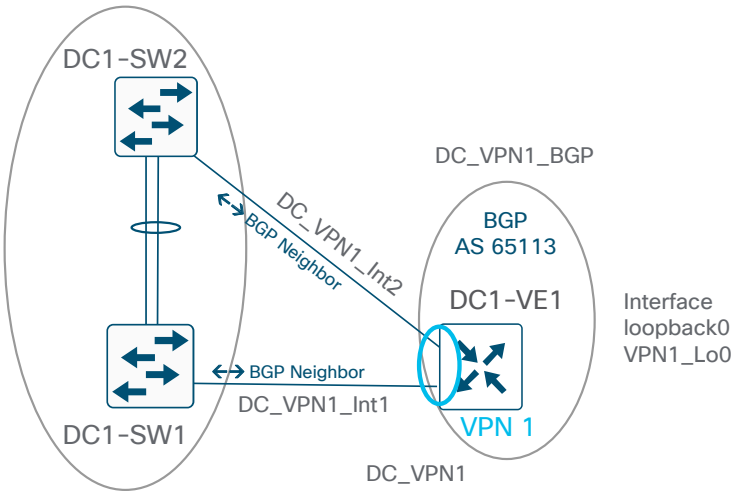
By defining the interface name as a variable, only one template is needed and can be applied to multiple types of vEdge devices because different model types use different management port interfaces. For example, the vEdge 1000, 2000, and 5000 routers all use the built-in mgmt0, while the vEdge 100 uses a normal Ethernet port, which is ge0/1 in the example network.

Step 7: Press the **Save** button to create the template.

Procedure 8 Configure the Service VPN

Next, configure the local service-side, or LAN-facing network. This network will connect into the WAN distribution/aggregation switches at the data center. This Service VPN needs three VPN Ethernet VPN templates, since you cannot reuse the same template twice within the same VPN, and there are two needed for the LAN interfaces and one needed for the loopback0 interface that is defined with the system IP address. A BGP template is also required to connect with the switches already running BGP at the data center.

Figure 14. Data center vEdge service templates



Service VPN 1

Step 8: Select **Configuration>Templates**, and select the **Feature** tab. Select the **Add Template** button.

Step 9: Create the VPN 1 template using the following device types, template, template name, and description:

Select Devices: **vEdge 2000**, **vEdge 5000**

Template: VPN Interface Ethernet

Template Name: **DC_VPN1**

Description: DC Service VPN 1

Step 10: Configure the parameters in the following table.

Table 26. Data center VPN 1 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN 1
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP	Global	On

With the **Advertise OMP** configuration, BGP routes are being redistributed into OMP so the remote sites will have reachability to the data center service-side routes.

Step 11: Select **Save** to create the template.

VPN interface Ethernet 1

Step 12: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button.

Step 13: Create the first VPN 1 interface template using the following device types, template type, template name, and description:

Select Devices: **vEdge 2000**, **vEdge 5000**

Template: VPN Interface Ethernet

Template Name: **DC_VPN1_Int1**

Description: DC Service VPN 1 Interface 1

Step 14: Configure the parameters in the following table.

Table 27. Data center VPN 1 interface feature template settings (Interface 1)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1 _lan_int1_gex/x
	Description	Device Specific	vpn1_lan_int1_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits

Step 15: Select **Save** to complete the template.

VPN interface Ethernet 2

Step 16: Assuming that you are still on the **Feature Templates** page, find the feature template just created (**DC_VPN1_Int1**) and select **...** to the far right. Select **Copy**.

Step 17: In the pop-up window, define the **Template Name** and **Description** as:

Template Name: **DC _VPN1_Int2**

Description: DC Service VPN 1 Interface 2

Step 18: Select the **Copy** button. The feature template is created and is now in the list with the other created feature templates.

Step 19: Choose **...** to the right of the newly-created feature template (**DC_VPN1_Int2**) and select **Edit** to modify the template.

Step 20: Modify the interface variables.

The following table summarizes the parameters in the feature template.

Table 28. Data center VPN 1 interface feature template settings (Interface 2)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1 _lan_int2_gex/x
	Description	Device Specific	vpn1_lan_int2_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits

Step 21: Once configuration changes have been made, select the **Update** button to save the changes in the feature template.

VPN interface Ethernet Loopback0

The loopback0 interface was created so logging, SNMP, and other management traffic could be sourced from the system IP address, making correlation with vManage easier. This template can be shared across all device types.

Step 22: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button.

Step 23: Create the loopback0 interface template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: VPN Interface Ethernet

Template Name: **VPN1_Lo0**

Description: Service VPN 1 Interface Loopback 0

Step 24: Configure the parameters listed in the following table.

Table 29. VPN 1 interface Ethernet feature template settings (Loopback 0)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Global	loopback0
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lo0_int_ip_addr/maskbits

Step 25: Select **Save** to complete the template.

Border Gateway Protocol (BGP)

Configure BGP in the Service VPN. In the configuration, OMP is redistributed into BGP so the data center can have reachability to the remote sites.

Step 26: Assuming that you are still on the **Feature Templates** page, select the **Add Template** button.

Step 27: Create the BGP template using the following device types, template type, template name, and description:

Select Devices: **vEdge 2000**, **vEdge 5000**

Template: BGP

Template Name: **DC_VPN1_BGP**

Description: DC VPN1 BGP Template

Step 28: Configure the parameters listed in the following table. To configure BGP neighbors, under the **Neighbor** section, select the **New Neighbor** button. Do this twice, once for each neighbor.

Table 30. BGP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	bgp _shutdown
	AS Number	Device Specific	bgp_as_num
	Router ID	Device Specific	bgp_router_id
	Propagate AS Path	Global	On
IPv4 Unicast Address Family	Maximum Paths	Global	2
	Address Family	Drop-down	Ipv4-unicast
	Re-Distribute/ Protocol	Drop-down	omp
	Network/Network Prefix	Device Specific	bgp_network_lo_addr/maskbits
Neighbor (1)	Address	Device Specific	bgp_neighbor1_address
	Description	Device Specific	bgp_neighbor1_description
	Remote AS	Device Specific	bgp_neighbor1_remote_as
	Address Family	Global	On
	Address Family	Global	ipv4-unicast
	Shutdown	Device Specific	bgp_neighbor1_shutdown
	Advanced Options/Password	Device Specific	bgp_neighbor1_password
	Advanced Options/Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9

Section	Parameter	Type	Variable/value
Neighbor (2)	Address	Device Specific	bgp_neighbor2_address
	Description	Device Specific	bgp_neighbor2_description
	Remote AS	Device Specific	bgp_neighbor2_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Shutdown	Device Specific	bgp_neighbor2_shutdown
	Advanced Options/Password	Device Specific	bgp_neighbor2_password
	Advanced Options/Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9

Step 29: Select **Save** to create the template.

Procedure 9 Configure additional templates (optional)

You can create a banner and SNMP feature template.

Banner

There are two types of banners: one that is displayed before the CLI username/login prompt (login banner) and one that is displayed after successfully logging in (message of the day, or MOTD, banner). Configure an MOTD banner.

Step 1: Select **Configuration>Templates**, and select the **Feature** tab. Select the **Add Template** button.

Step 2: Create the banner template using the following device types, template type, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: Banner

Template Name: **Banner_Template**

Description: Banner Template

Step 3: Configure the parameters listed in the following table.

Table 31. Banner feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	MOTD Banner	Global	This is a private network. It is for authorized use only.

Step 4: Select **Save** to create the template.

SNMP

Step 5: Select **Configuration>Templates**, and select the **Feature** tab. Select the **Add Template** button.

Step 6: Create the SNMP template using the following device types, template, template name, and description:

Select Devices: **vEdge 100 B**, **vEdge 100 M**, **vEdge 100 WM**, **vEdge 1000**, **vEdge 2000**, **vEdge 5000**, **vEdge Cloud**

Template: SNMP

Template Name: **SNMP_Template**

Description: SNMP Template

Step 7: Configure the parameters in the following table.

Table 32. SNMP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	snmp_shutdown
	Name of Device for SNMP	Device Specific	snmp_device_name
	Location of Device	Device Specific	snmp_device_location
SNMP version	View/Name	Radio button	V2
View and Community	View/Name	Global	isoALL
	View/Object Identifiers	Global	1.3.6.1
	Community/Name	Global	c1sco123
	Community/ Authorization	Global/ drop-down	read-only
	Community/View	Global	isoALL
Trap	Trap Group/Group Name	Global	SNMP-GRP
	Trap Group/Trap Type Modules/ Severity Levels	Global	critical, major, minor
	Trap Group/Trap Type Modules/ Module Name	Global	all

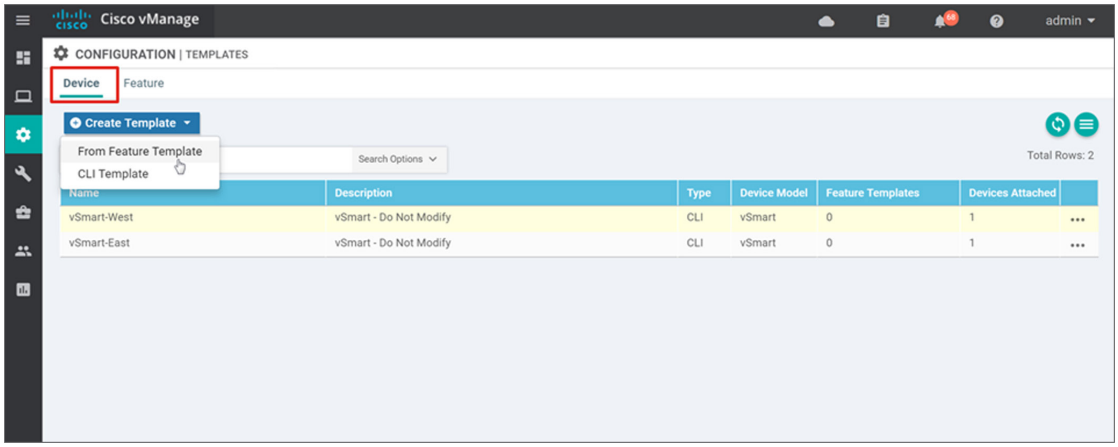
Step 8: Select **Save** to create the template.

Procedure 10 Create a device template

In this procedure, you create a device template that references the feature templates just created.

Step 1: On the vManage GUI, Go to **Configuration > Templates** and ensure the **Device** tab is selected (the default tab).

Step 2: Select **Create template** and select **From feature template** from the drop-down box.



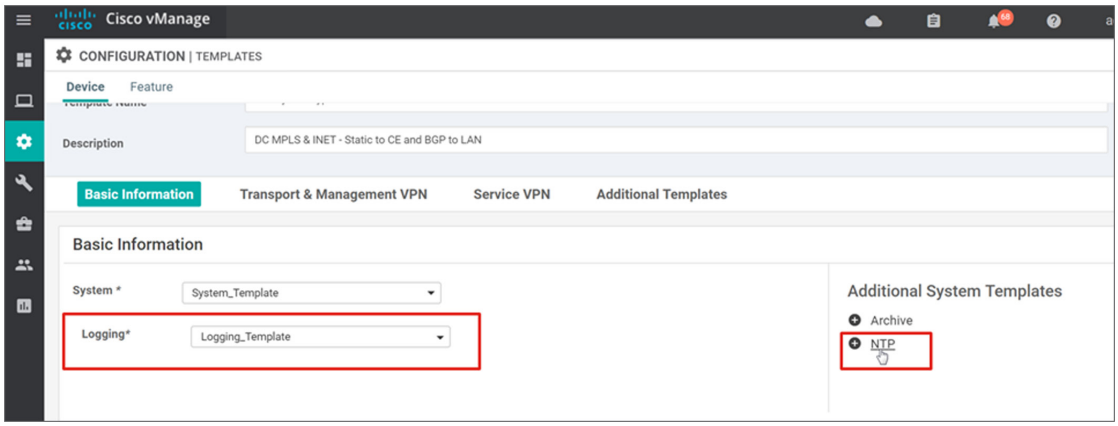
Step 3: Select the **Device Model** (vEdge 5000) from the drop-down box.

Step 4: Fill in a **Template Name** (**DC_Hybrid_Type_A_BGP**) and give it a **Description** (**DC MPLS and INET - Static to CE and BGP to LAN**). By default, the areas in the device template that require feature templates are pre-populated with default templates.

Step 5: Under **Basic information** next to **System**, select the feature template, **System_Template**, from the drop-down box.

Step 6: Next to **Logging**, select the feature template, **Logging_Template**, from the drop-down box.

Step 7: For NTP, this feature first needs to be added to the device template. Under **Additional System Templates**, click **NTP**, and select the feature template from the drop down, **NTP_Template**.



Step 8: Next to AAA, select the feature template, **AAA_Template**, from the drop-down box.

Step 9: Repeat Step 8 for **BFD**, **OMP**, and **Security**.

Table 33. Basic information section of device template

Template type	Template name
System	System_Template
Logging	Logging_Template
NTP	NTP_Template
AAA	AAA_Template
OMP	OMP_Template
BFD	BFD_Template
Security	Security_Template

Step 10: Under the **Transport and Management VPN** Section, select **VPN Interface** on the right side under **Additional VPN 0 Templates**. This will add a second VPN interface under the **Transport VPN**. Select the newly-created feature templates under the **VPN 0** drop-down box and under each **VPN Interface** drop-down box under VPN 0.

Step 11: For VPN 512, select the newly-created feature template under the **VPN 512** drop-down box and under the **VPN Interface** drop-down box under **VPN 512**.

Table 34. Transport and management VPN section of device template

Template type	Template sub-type	Template name
VPN0		DC_VPN0
	VPN Interface	DC_MPLS_Int
	VPN Interface	DC_INET_Int
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface

Step 12: Under the **Service VPN** section, hover over the **+ Service VPN** text. A window will appear with a text box for the number of service VPNs you want to create.

Step 13: Select **1** and press return. A **VPN** drop-down box will be added. In the **Additional VPN Templates** on the right side, select **VPN Interface** three times (for the two LAN interfaces and Loopback0 definition) and select the **BGP** template as well.

Step 14: Select the newly-created feature templates for each drop-down box added.

Table 35. Service VPN section of device template

Template type	Template sub-type	Template name
VPN1		DC _VPN1
	BGP	DC_BGP
	VPN Interface	DC_VPN1_Int1
	VPN Interface	DC_VPN1_Int2
	VPN Interface	VPN1_Lo0

Step 15: Under the **Additional templates** section, select the newly-created feature templates for each drop-down box (banner and SNMP). Localized policy has not yet been created, so there is no policy to reference yet in the drop-down box next to **Policy**.

Table 36. Additional templates section of device template

Template type	Template name
Banner	Banner_Template
Policy	
SNMP	SNMP_Template

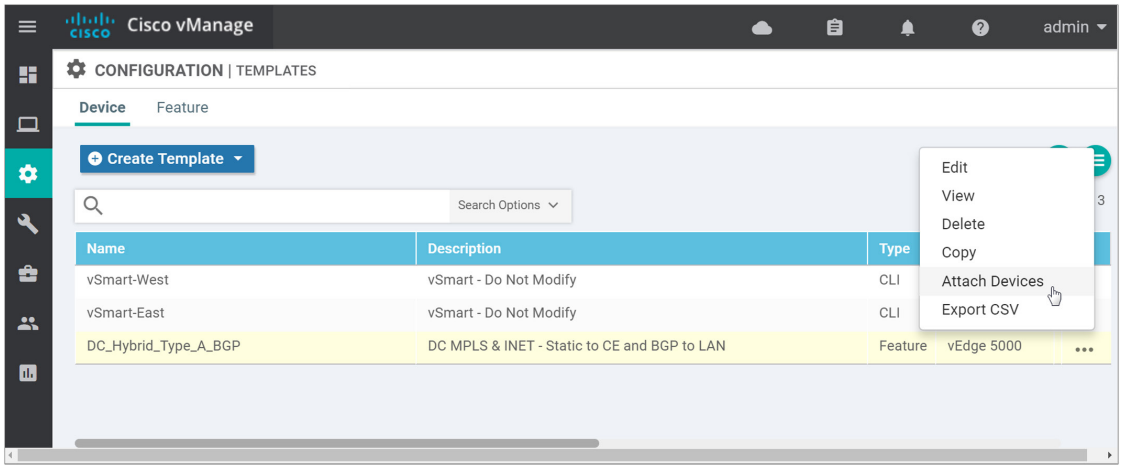
Step 16: Select **Create** to create and save the device template.

Procedure 11 Deploy the device templates to the vEdge routers

To deploy the device template created to the vEdge routers, the vManage builds the full configurations based on the feature templates and then pushes them out to the designated vEdge routers. Before the full configurations can be built and pushed out, you need to first define all variables associated with the feature templates attached to the device template. There are two ways to do this: either by entering in the values of the variables manually within the GUI, or by uploading a .csv file with a list of the variables and their values.

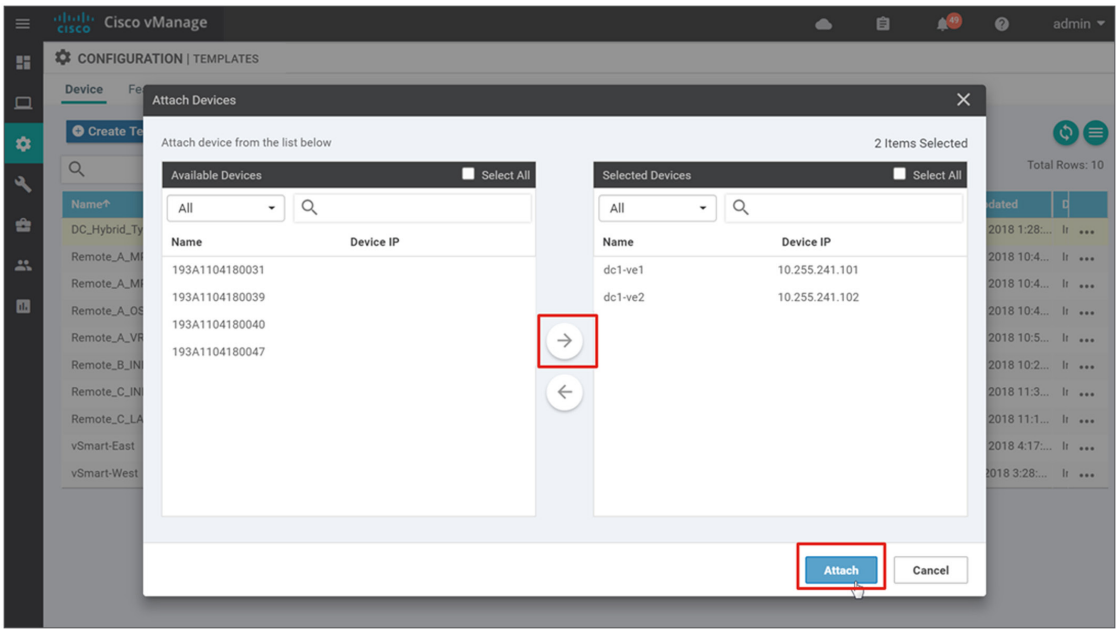
Enter values manually

Step 1: Go to **Configuration > Templates** and select the **Device** tab. Find the desired device template (**DC_Hybrid_Type_A_BGP**). Select the **...** to the right of the template, and select **Attach Devices**.

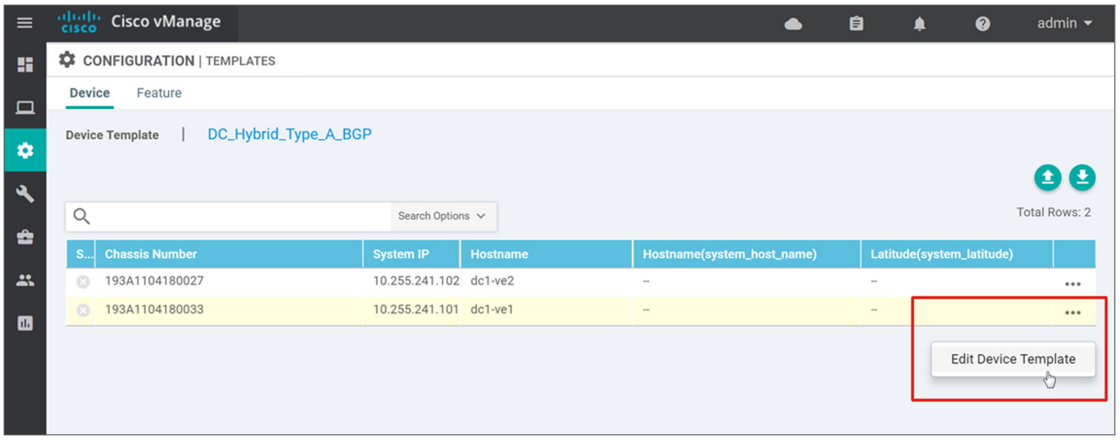


Step 2: A window pops up listing the available devices to be attached to this configuration. The list of available devices contains either the hostname and IP address of a device if it is known through vManage, or it will contain the chassis serial number of the devices that have not yet come up on the network and are unknown by vManage. In any case, the list contains only the device model that was defined when the template was created (vEdge 5000 in this case).

Step 3: Select the devices you want to apply the configuration template to, and select the arrow to move the device from the **Available Devices** box to the **Selected Devices** box. You can select multiple devices at one time by simply clicking each desired device. Select **Attach**.



Step 4: There will be a page listing the devices you have selected. Find the vEdge, dc1-ve1, and select **...** to the far right of it. Select **Edit Device Template**.



Step 5: A screen will pop up with a list of variables and empty text boxes. There may also be variables with check boxes to check or uncheck for on and off values. Fill in the values of the variables in the text boxes. All text boxes must be filled in, but check boxes can be left unmarked. For check boxes, checked means yes and unchecked means no. If you leave a text field empty, the text box will be highlighted red when you try to move to the next page. Fill in the variables listed in the following table.

Table 37. Dc1-ve1 device template variable values

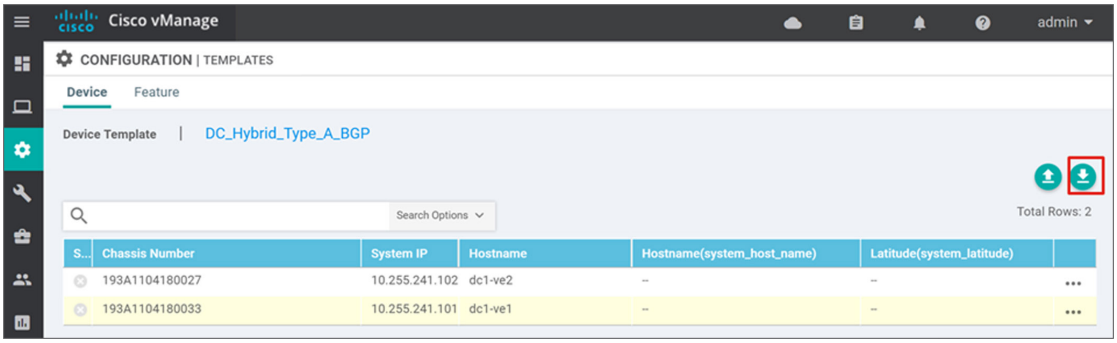
Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	dc1-ve1
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG3,Primary
System IP(system_system_ip)	10.255.241.101
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
Address(vpn0_mpls_next_hop_ip_addr)	10.4.1.1
Address(vpn0_inet_next_hop_ip_addr)	10.4.1.5
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.4.1.2/30

Variable	Value
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.4.1.6/30
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	1000000
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.167/23
AS Number(bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(bgp_router_id)	10.255.241.101
Address(bgp_neighbor_address1)	10.4.1.9
Address(bgp_neighbor_address2)	10.4.1.13
Description(bgp_neighbor1_description)	Agg-Switch1
Description(bgp_neighbor2_description)	Agg-Switch2
Remote AS(bgp_neighbor1_remote_as)	65112
Remote AS(bgp_neighbor2_remote_as)	65112
Password(bgp_neighbor1_password)	cisco123
Password(bgp_neighbor2_password)	cisco123
Interface Name(vpn1_lan_int1_gex/x)	ge0/4
Description(vpn1_lan_int1_description)	To DC1-SW1 G1/0/11
Shutdown(vpn1_lan_int1_shutdown)	☐

Variable	Value
IPv4 Address(vpn1_lan_int1_ip_addr/maskbits)	10.4.1.10/30
Interface Name(vpn1_lan_int2_gex/x)	ge0/5
Description(vpn1_lan_int2_description)	To DC1-SW2 G1/0/11
IPv4 Address(vpn1_lan_int2_ip_addr/maskbits)	10.4.1.14/30
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(vpn1_lo0_int_ip_addr/maskbits)	10.255.241.101/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-VE1
Location of Device(snmp_device_location)	Datacenter 1

Step 6: Select **Update**

When you are finished filling out the variables and before moving further, download the .csv file by selecting the download arrow symbol in the upper right corner.



The .csv file will be populated with the values you have filled in so far. If you deploy the configuration, and for any reason there is an error in one of the input variables and the configuration fails to deploy, when you come back to this page, all the values will be gone and you will need to enter them in again. If you downloaded the populated .csv file, just upload it by selecting the up arrow. Then you can select **...** to the right of the desired device and select **Edit device template**, and all of your latest values will be populated in the text boxes. Modify any input values, and try to deploy again.

Upload values via a .csv file

Step 7: On the upper right corner of the page, select the **download** arrow symbol. This will download the .csv file, and it will be named after the device template, *DC_Hybrid_Type_A_BGP.csv*. The .csv file will list the two devices that have been attached to the template and will list the necessary variables in each column. Since the dc1-ve1 device was already filled out manually, those values are already populated in the spreadsheet.

Step 8: Fill out the variable values, then save the .csv file. Keep it in .csv format when saving. Use the following table for variable values.

Table 38. Dc1-ve2 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	dc1-ve2
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG2,Secondary
System IP(system_system_ip)	10.255.241.102
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
Address(vpn0_mpls_next_hop_ip_addr)	10.4.2.1
Address(vpn0_inet_next_hop_ip_addr)	10.4.2.5
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.4.2.2/30
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.4.2.6/30
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000

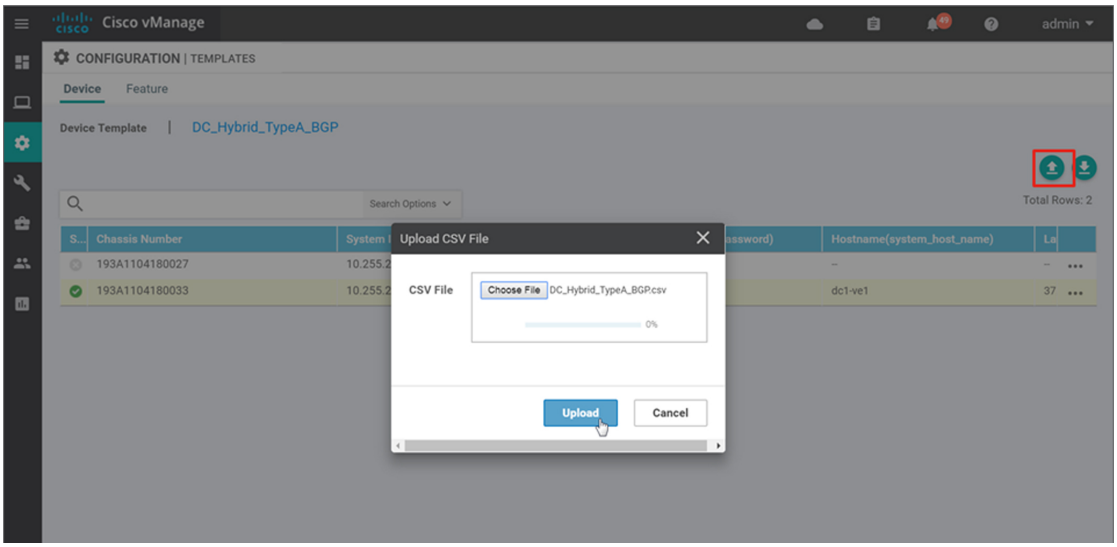
Variable	Value
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	1000000
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.168/23
AS Number(bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(bgp_router_id)	10.255.241.102
Address(bgp_neighbor_address1)	10.4.2.9
Address(bgp_neighbor_address2)	10.4.2.13
Description(bgp_neighbor1_description)	Agg-Switch1
Description(bgp_neighbor2_description)	Agg-Switch2
Remote AS(bgp_neighbor1_remote_as)	65112
Remote AS(bgp_neighbor2_remote_as)	65112
Password(bgp_neighbor1_password)	cisco123
Password(bgp_neighbor2_password)	cisco123
Interface Name(vpn1_lan_int1_gex/x)	ge0/4
Description(vpn1_lan_int1_description)	To DC1-SW1 G1/0/12
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(vpn1_lan_int1_ip_addr/maskbits)	10.4.2.10/30
Interface Name(vpn1_lan_int2_gex/x)	ge0/5
Description(vpn1_lan_int2_description)	To DC1-SW2 G1/0/12
IPv4 Address(vpn1_lan_int2_ip_addr/maskbits)	10.4.2.14/30
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(vpn1_lo0_int_ip_addr/maskbits)	10.255.241.102/32
Shutdown(snmp_shutdown)	☐

Variable	Value
Name of Device for SNMP(snmp_device_name)	DC1-VE2
Location of Device(snmp_device_location)	Datacenter 1

Step 9: Select the upload arrow in the top right corner of the screen to upload the .csv file.

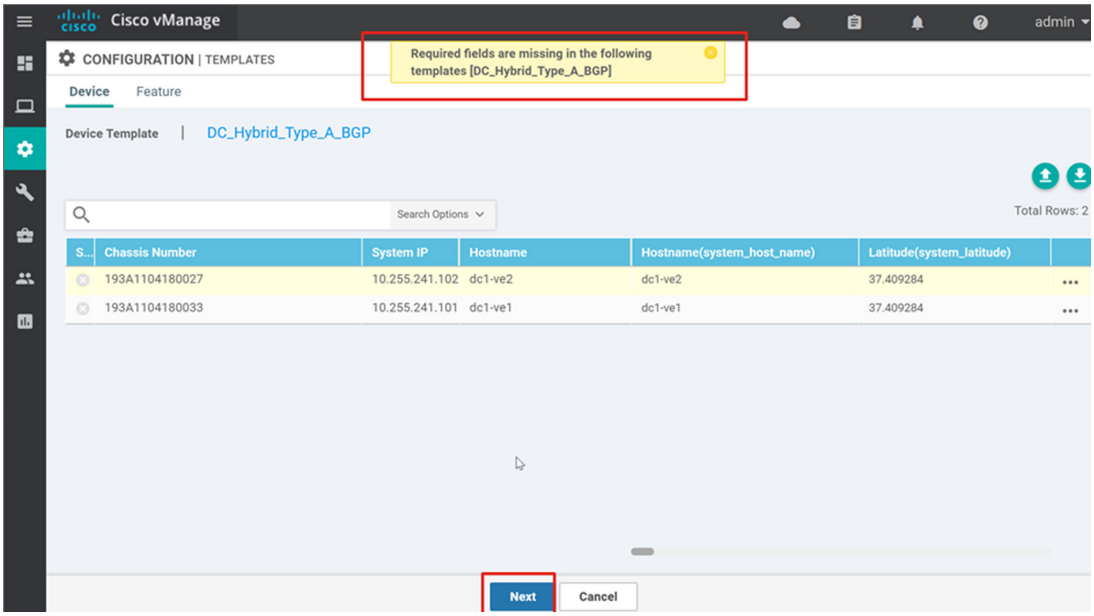
Step 10: A window will pop up. Select the **Choose File** button and select the completed .csv file with the saved variable values.

Step 11: Select the **Upload** Button. "File Uploaded Successfully" should appear in green at the top of the screen.



Step 12: You can scroll to the right and view all of the values and variables that have been used for input. You can also select **...** to the right of each device and select **Edit Device Template** to view all of the input variables and their values. You can adjust input by manually changing the input here, or you can re-upload a modified .csv file.

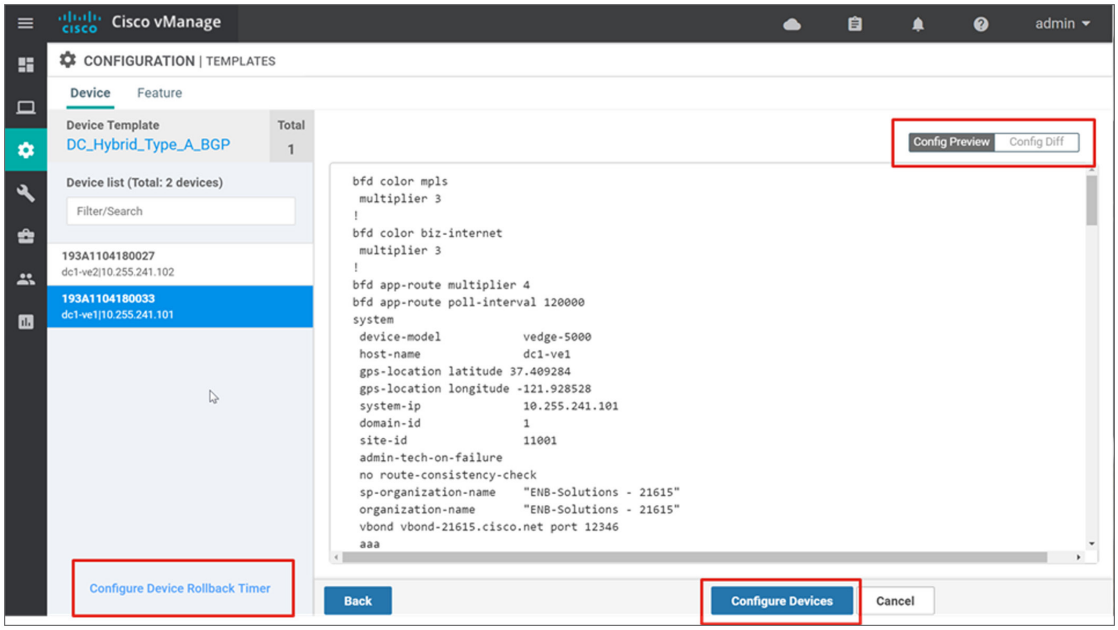
Step 13: When you are ready to deploy, select the **Next** button. If you forgot to add values for a device, you will get an error and you won't be able to move forward until it is corrected.



Step 14: The next screen will indicate that the configure action will be applied to two devices attached to one device template. Selecting a device on the left side will show you the configuration that will be pushed to the vEdge router (**Config Preview** tab). Select the **Config Diff** tab at the top of the screen to see the difference in the current local configuration versus the new configuration which is about to be pushed.

Step 15: Optionally, you may select the **Configure Device Rollback Timer** text in the lower left corner to view or change the rollback timer. By default, this is set to five minutes, meaning, if a configuration is pushed out which causes loss of connectivity to vManage, the vEdge router will roll back to the previous configuration in five minutes. You can change this timer and set it from six to 15 minutes, or disable it altogether (not recommended).

Step 16: Back at the **Config preview** page, select **Configure devices**.

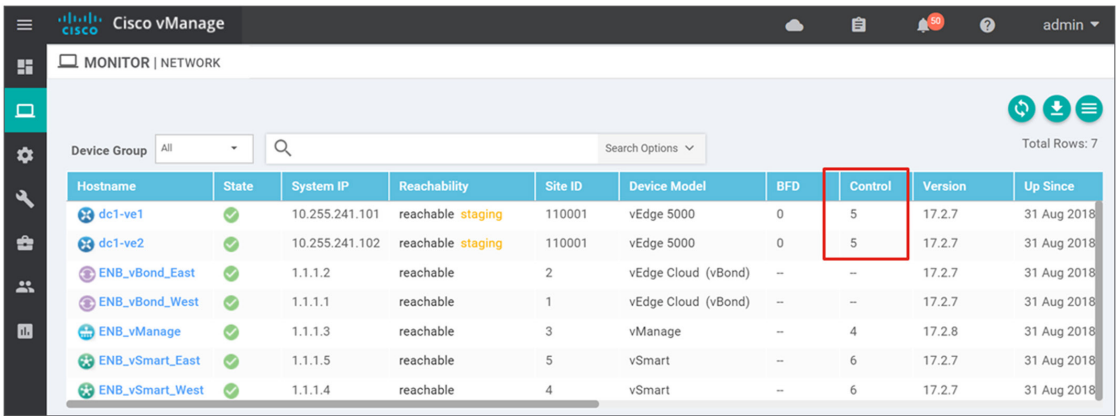


Step 17: A pop-up window says, "Committing these changes affects the configuration on 2 devices. Are you sure you want to proceed?" Select the check box to **Confirm configuration changes on 2 devices**. Select **OK**.

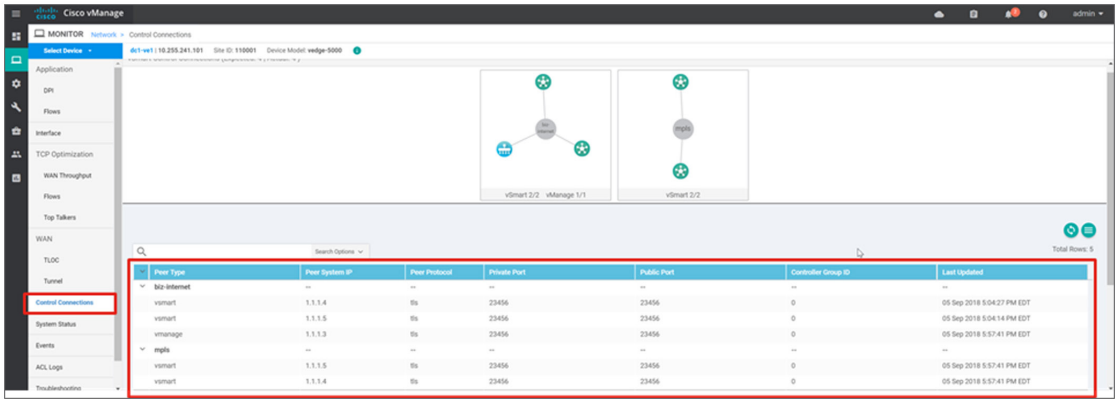
The configuration then gets pushed out to both devices. When complete, vManage should indicate success.

Because the vEdge routers are in staging mode, the vEdge status won't be seen from the vManage dashboard.

Step 18: Go to **Monitor>Network**. From the table, you can see that dc1-ve1 and dc1-ve2 are both reachable and have a total of five control connections each.



Step 19: Select dc1-ve1. Select **Control Connections,** and you can visualize the control connections that have been established over each transport.



Procedure 12 Create a localized policy

Localized policy is provisioned directly on the vEdge routers. Localized control policy examples are route policies, which can affect the BGP and OSPF routing behavior on the local site network and affect routing into or out of that specific site. Localized data policy controls the data traffic into and out of interfaces and interface queues on a vEdge router. Examples include access lists, which allows you to classify traffic and map the traffic to different classes, or traffic mirroring, policing, and QoS.

At the data center in the example network, the CE router marks all MPLS routes (transport and non-SD-WAN site routes) with a community of 101:101. Create an example localized policy that will:

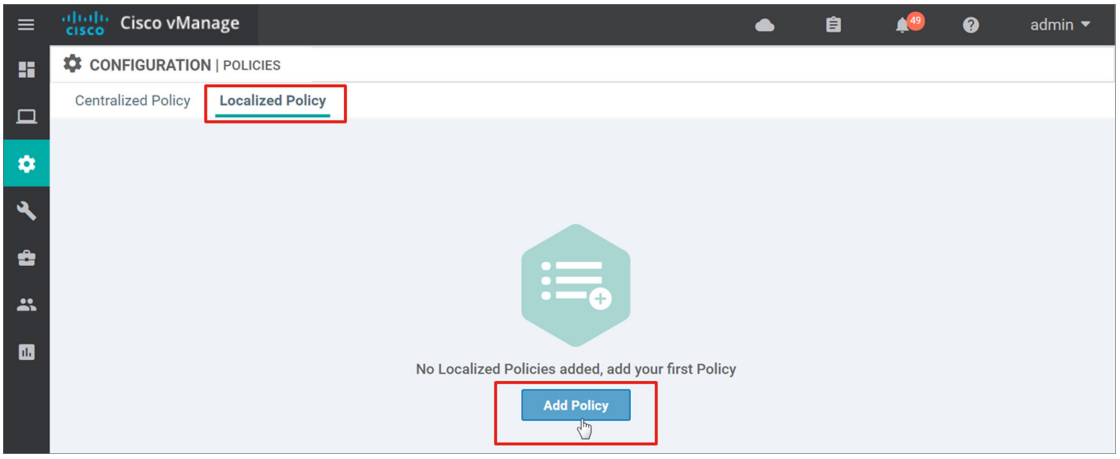
- Define a route-policy for BGP to filter any incoming prefixes for the MPLS transport (192.168.0.0/16, 10.101.1.0/30, 10.104.1.0/30, and 10.105.1.0/30)
- Within the route-policy for BGP, match and accept route prefixes with a community of 101:101
- Within the route-policy for BGP, match and accept other routes indicating local routes, with AS-PATH settings originating with 65112, and set the community for these routes to 1:100
- Turn on cflowd, so the vEdge router can do traffic flow monitoring and send the information to vManage
- Turn on Deep Packet Inspection (DPI), or application visibility. DPI will allow a vEdge router to discover, monitor, and track the applications running on the LAN. This enhances the application information that appears within the vManage GUI.

Note that only one localized policy can be applied per device, but one policy can be shared across many devices. If there are variables defined in the localized policy attached to a device, you need to define the values of the variables at the time the policy is applied, regardless of whether the device is referencing that part of the policy or not. Hence, you may want to create multiple localized policies and group according to similar device types to avoid having to enter unnecessary variable values.

Localized policy is attached to a device template in the **Additional templates** section next to **Policy**. Once attached to the template and deployed to the device, the route policies, access lists, and other components in the policy can be referenced in any of the feature templates attached to the device template. You will not be able to configure a feature template in a device template that contains a policy element without having a policy attached to the device template.

Step 1: From the vManage GUI, Go to **Configuration>Policies** and select the **Localized policy** tab.

Step 2: Select the **Add policy** button



Step 3: Type in the name (**DC_Policy**) and description (**DC Local Policy**)

In earlier versions of code, the localized policy is CLI-based. Lists are defined first, followed by route policy. For each route policy, sequences are defined, each with a match/action pair. Each route policy is evaluated from top to bottom from low to high sequence. Once a match is made, the route is either accepted or rejected/filtered. If the route is accepted, further actions can be taken with a set command. Processing stops once a match is made and an action is carried out. A match that does not reference a list matches all traffic. A default action occurs at the end of each route policy (either accept or reject) for any traffic that doesn't match any condition in the policy.

Step 4: Type or paste in the following CLI:

```
policy
app-visibility
 flow-visibility
 lists
  as-path-list Local-Routes
   as-path ^65112$
  !
  community-list Non-SD-WAN-Sites
   community 101:101
  !
  prefix-list MPLS-Transport
   ip-prefix 10.4.1.0/30
   ip-prefix 10.4.2.0/30
   ip-prefix 192.168.0.0/16 le 32
```

```
    ip-prefix 10.101.1.0/30
    ip-prefix 10.104.1.0/30
    ip-prefix 10.105.1.0/30
!
route-policy BGP-POLICY-IN
  sequence 10
   match
    address MPLS-Transport
   !
   action reject
   !
  !
  sequence 20
   match
    community Non-SD-WAN-Sites
   !
   action accept
   !
  !
  sequence 30
   match
    as-path   Local-Routes
   !
   action accept
    set
     community 1:100
    !
   !
  !
  default-action reject
 !
!
```

Step 5: Select **Add**

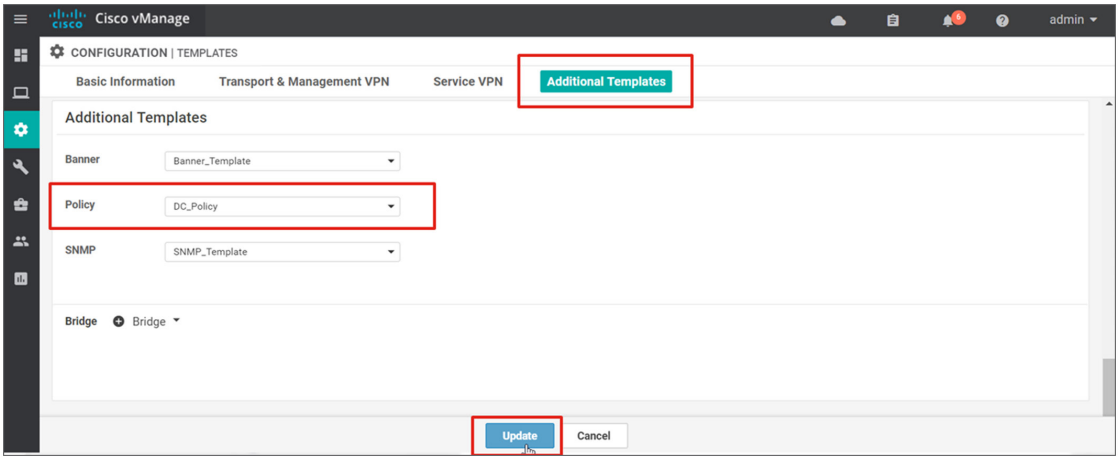
Procedure 13 Attach localized policy to a device template

Now that the localized policy has been created, it needs to be referenced by a device template. This causes the policy configuration to be downloaded to the vEdge router.

Step 1: Go to **Configuration>Templates** and ensure the **Device** tab is selected. Next to the template, **DC_Hybrid_Type_A_BGP**, select … to the right, and select **Edit**.

Step 2: Scroll to the **Additional Templates** section, or select **Additional Templates** in order to jump to that section of the device template.

Step 3: Next to **Policy**, select the newly-created localized policy, **DC_Policy**, and select **Update**.



Step 4: There are no variables to define, so select **Next**, then **Configure devices**.

Step 5: Confirm changes on two devices by selecting the check box, then select **OK**.

Step 6: The policy is pushed to the vEdge routers and the status should indicate success.

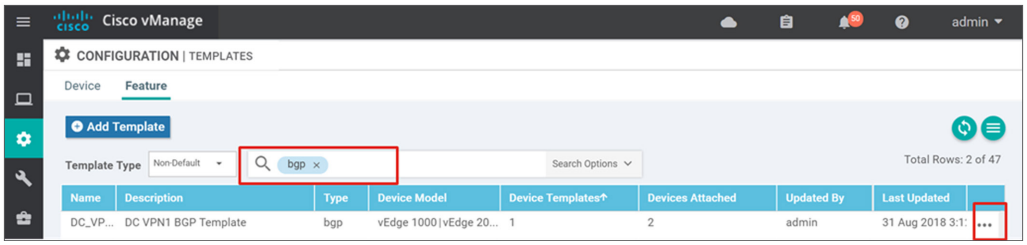
Procedure 14 Add localized policy references in the feature templates

Now that the localized policy is attached to the device template and downloaded to the vEdge devices, configure the route policy in the BGP feature template.

Step 1: Go to **Templates>Configuration** and select the **Feature** tab.

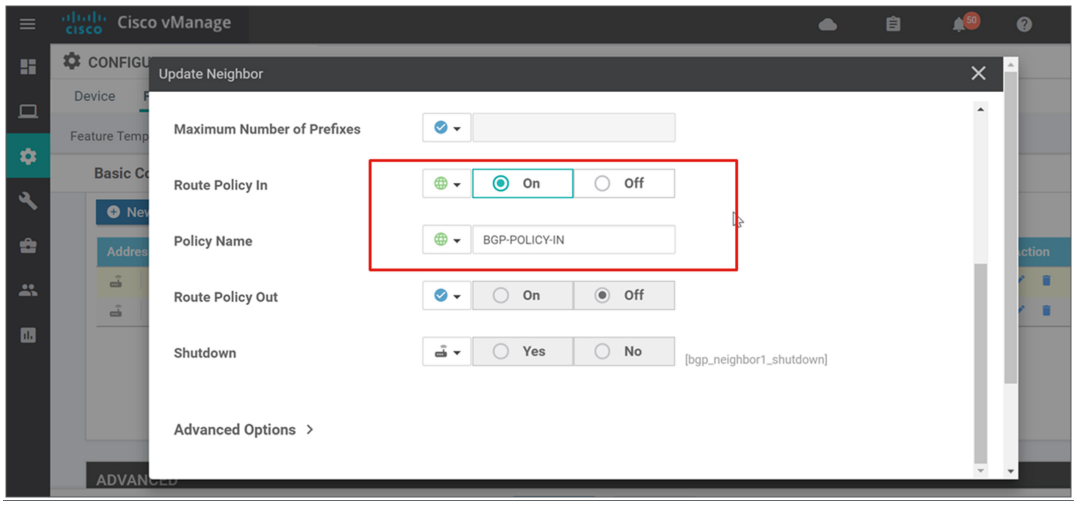
Step 2: In the search text box, type in **bgp** and press the return key. The templates are filtered for the keyword in the **Name**, **Description**, **Type**, and **Model** columns.

Step 3: Select **...** to the right of the template, **DC_VPN1_BGP**, and select **Edit**.



Step 4: Under **Neighbor**, select the edit symbol under the **Action** column on the first neighbor defined.

Step 5: For **Route Policy In**, select **Global** from the drop-down box, and select **On**. Type **BGP-POLICY-IN** next to **Policy name**.



Step 6: Select **Save Changes**.

Step 7: Repeat steps 4 through 6 for the second neighbor defined.

Step 8: Select **Update** to save the feature template. Because the modified feature template is attached to a device, vManage attempts to push out the modified configuration after any feature template change. vManage merges the new changes into its full local configuration, and pushes out the full configuration to the vEdge router.

Step 9: No new variable value input is needed, so select **Next**. Review configurations if needed. Otherwise, select **Configure Devices**.

Step 10: Confirm the configuration changes on two devices in the popup window and select **OK**.

Procedure 15 Bring vEdge devices out of staging mode

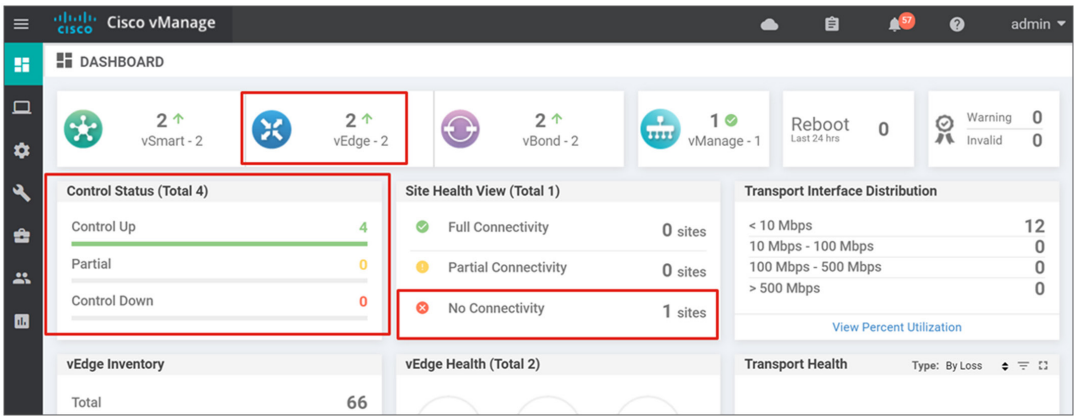
If the vEdge routers were initially put into staging mode, they can be brought online and made operational. This can be done at any time.

Step 1: Go to **Configuration>Certificates**, find the vEdge routers just configured (**dc1-ve1** and **dc1-ve2**), and select **Valid** for each of them.

Step 2: For each device, a popup message asks if you are sure you want to validate the devices. Select **Ok**.

Step 3: Once they are both valid, select the **Send to controllers** button so that the controllers have the latest authorized device list. The vEdge routers may initially show a non-reachability status and control down on the dashboard, but they should show reachability and control status up within a minute.

You should see this first site with no connectivity in the **Site health view** on the vManage dashboard. This is because all BFD sessions on these vEdge routers are in a down state. This is because no other sites are yet online and the two data center vEdge devices will not form BFD sessions with each other because they are both configured for the same site ID.



Process

Deploying remote sites

1. Create a localized policy for the branches
2. Configure the transport side feature templates
3. Configure the service side feature templates
4. Create the branch device templates
5. Attach the device templates
6. Bring remote vEdge routers online
7. Verify the network status

There are five branches which represent common greenfield deployments. The five branches are running a variety of features that are common in many deployments.

In this deployment, the localized policy and feature templates will first be configured, followed by the device templates. Then, the device templates will be attached to the vEdge routers and then the ZTP process will be used to bring the vEdge routers online. The routers will be upgraded through the ZTP process before they are brought online with their full configurations.

Procedure 1 Create a localized policy for the branches

Create a localized policy for the branches. You can create one larger policy that applies to all branches, or you can create smaller policies and apply different ones to different branch types. Note that you will be required to define values for all variables within a policy once attached to a device, even if the list or route policy containing the variable is not referenced within a feature template for that device. Only one localized policy can be attached to a single device template.

The example policy should include:

- Flow visibility
- App visibility, or Deep Packet Inspection (DPI)
- Route policies for BGP at the dual-vEdge router sites. One policy should advertise only the TLOC extension link subnet so that routers using the MPLS transport can connect to the vEdge router using the TLOC extension link for the MPLS transport. Another policy should filter all BGP routes coming into the transport VPN because a static default route pointing to the MPLS transport next hop will be used to route control traffic and IPSec tunnel endpoint traffic out of the transport VPN.
- A prefix list containing the default route in order for VRRP to track on it. When the OMP prefix route disappears, the vEdge router gives up VRRP primary status.

Initially, create two branch policies: **Branch_Policy** and **Branch_BGP_OSPF_Policy.** The **Branch_BGP_OSPF_Policy** will contain any route policies needed for the vEdge routers configured for BGP (to advertise the TLOC-extension subnet) or OSPF. Note that when you apply a localized policy to a device template that gets applied to multiple vEdge routers, you have to define values for any variables within that localized policy, regardless of whether that device uses those policy components within its feature templates. Optionally, create any additional policies so you are not defining unnecessary variables when applying the policies.

Step 1: From the vManage GUI, Go to **Configuration>Policies** and select the **Localized policy** tab.

Step 2: Select the **Add CLI Policy** button.

Step 3: Type in the name (**Branch_Policy**) and description (**Branch Local Policy**).

Step 4: Type or paste in the following CLI:

```
policy
 app-visibility
 flow-visibility
 lists
  prefix-list default-route
   ip-prefix 0.0.0.0/0
  !
 !
!
```

Step 5: Select **Add** to complete and save the localized policy.

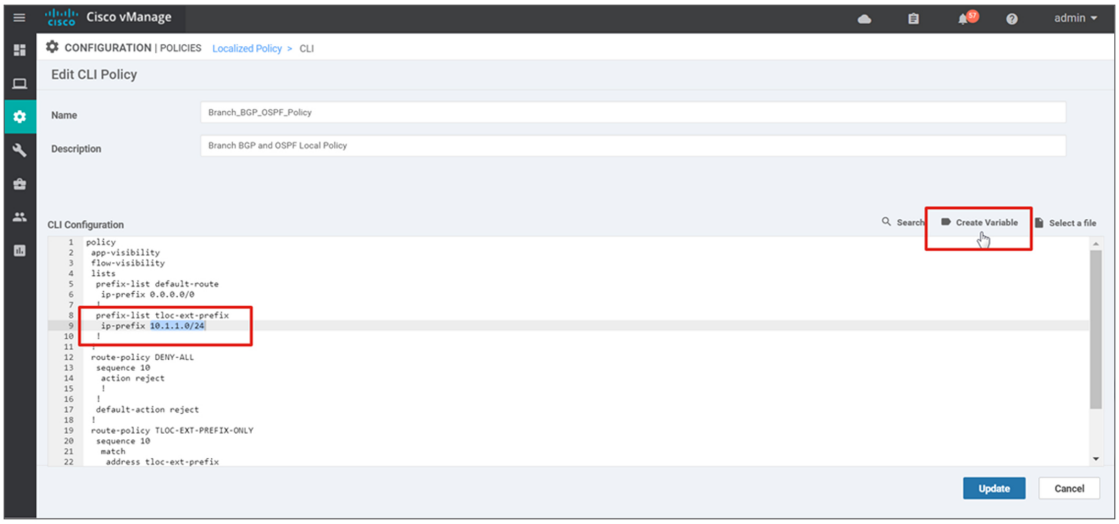
Step 6: Select the **Add CLI Policy** button.

Step 7: Type in the name (**Branch_BGP_OSPF_Policy**) and description (**Branch BGP and OSPF Local Policy**).

Step 8: Type or paste in the following CLI:

```
policy
 app-visibility
 flow-visibility
 lists
  prefix-list default-route
   ip-prefix 0.0.0.0/0
  !
  prefix-list tloc-ext-prefix
   ip-prefix 10.101.1.0/30
  !
 !
 route-policy DENY-ALL
  sequence 10
   action reject
   !
  !
  default-action reject
 !
 route-policy TLOC-EXT-PREFIX-ONLY
  sequence 10
   match
    address tloc-ext-prefix
   !
   action accept
   !
  !
  default-action reject
```

Step 9: Create a variable for the tloc-ext-prefix, 10.101.1.0/30, so this policy can apply to any branch. In the policy, highlight 10.101.1.0/30 in the prefix list, **tloc-ext-prefix**, and select **Create variable**.



Step 10: Under the **Variable name** text box, type in **bgp_tloc_ext_prefix_to_advertise** in the pop-up window.

Step 11: Select **Create variable**.

Step 12: Select **Add** to complete and save the localized policy.

Procedure 2 Configure the transport side feature templates

On the transport side of the example network, there are several different feature templates that should be created.

Subinterfaces are used in branch 4 because the single link between the two vEdge routers carries the WAN transport and TLOC-extension subinterfaces. Many times, a subinterface and physical interface can be combined into one feature template by specifying the interface name as a variable. By design, QoS is not supported on subinterfaces. A QoS policy, however, can be applied to a template that is combined to configure both physical interfaces and subinterfaces by creating a variable for the interface name, but the policy will be silently discarded when applying it to a subinterface.

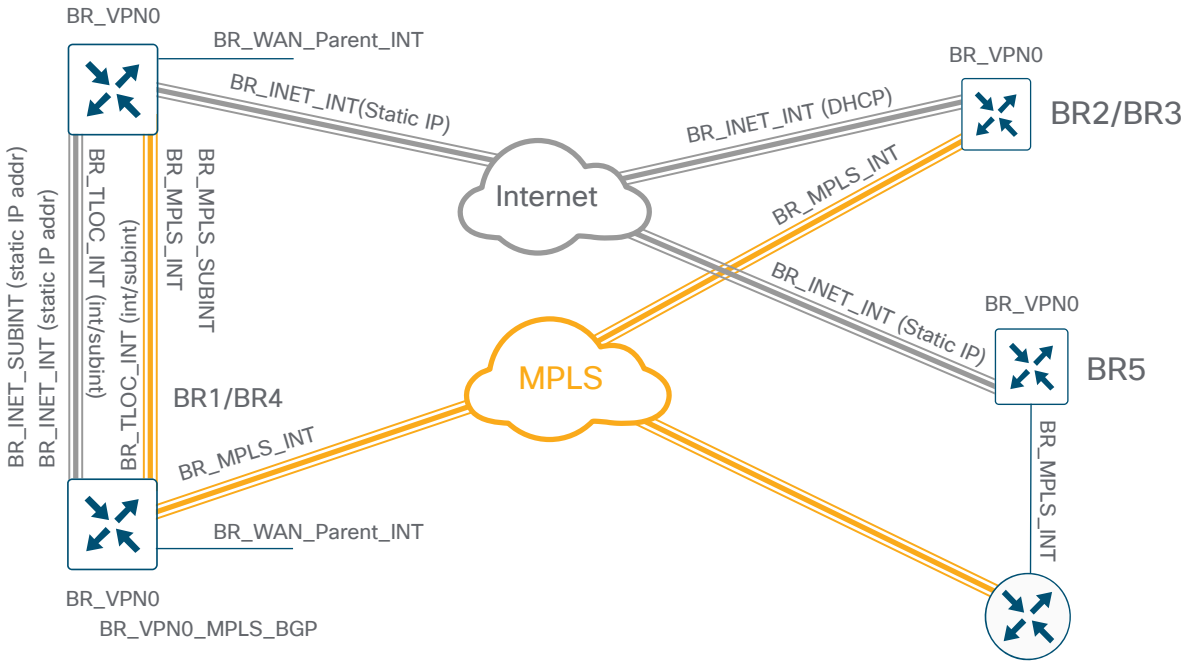
Re-write policies allow you to rewrite the DSCP values in the tunnel header in the event that the service provider supports less DSCP classes in use. If you need a re-write policy, vManage will not allow you to apply it to a subinterface, so it is best in this case to make a separate interface and subinterface template.

Subinterfaces require a physical, parent interface to be defined in VPN 0, and also require the subinterface MTU to be four bytes lower than the physical interface due to the 802.1q tag. It is recommended to configure the parent physical interface for an MTU of 1504 to take care of this requirement.

Following are the feature templates needed for the branch transport side:

- VPN 0 template – One feature template can be built for all branches (BR_VPN0 for all branches)
- VPN interface Ethernet templates – Several different interface templates are needed beneath VPN 0:
  - The physical interface for the MPLS transport (BR_MPLS_INT for all branches)
  - The subinterface for the MPLS transport using the-TLOC extension (BR_MPLS_SUBINT for branch 4)
  - The physical interface for the Internet transport using static IP addressing (BR_INET_INT for branches 1, 4, and 5)
  - They physical interface for the Internet transport using DHCP IP addressing (BR_INET_INT_DHCP for branch 2 and 3).
  - The subinterface for the Internet transport using static IP addressing (BR_INET_SUBINT for branch 4)
  - The TLOC interface or subinterface, which can be combined into one template (BR_TLOC_INT for branches 1 and 4)
  - WAN parent physical interface for the subinterfaces (BR_WAN_Parent_INT for branch 4)
- BGP – The BGP feature template is needed for the transport side of the MPLS-connected vEdge router to communicate the TLOC-extension link subnet to the MPLS transport (BR_VPN0_MPLS_BGP for branches 1 and 4).

Figure 15. Branch vEdge transport side templates



BR_VPN0

Step 1: Go to **Configuration > Templates** and select the **Feature** tab. Select the **Add template** button and use the following parameters to configure the VPN 0 feature template:

Select Devices: **vEdge 100 B, vEdge 100 M, vEdge100 WM, vEdge 1000**

Template: VPN

Template Name: **BR_VPN0**

Description: **Branch Transport VPN 0**

Table 39. Branch VPN 0 feature template

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	64.100.100.125
	Secondary DNS Address	Global	64.100.100.126
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn0_mpls_next_hop_ip_addr
	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

Step 2: Select **Save** to complete the template.

BR_MPLS_INT

Step 3: Add a new feature template using the following parameters:

Select Devices: **vEdge 100 B, vEdge 100 M, vEdge100 WM, vEdge 1000**

Template: **VPN Interface Ethernet**

Template Name: **BR_MPLS_INT**

Description: **Branch MPLS Interface with Static IP**

Table 40. Branch VPN0 MPLS interface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/ maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_ down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Tunnel>Allow Service	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_ preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 4: Select **Save** to create the template.

BR_MPLS_SUBINT

Step 5: Add a new feature template or copy the previous feature template using the following parameters. The only thing changed is the variable for **Interface Name**, which becomes **vpn0_mpls_int_gex/x.VLAN**.

Select Devices: **vEdge 100 B, vEdge 100 M, vEdge100 WM, vEdge 1000**

Template: **VPN Interface Ethernet**

Template Name: **BR_MPLS_SUBINT**

Description: **Branch MPLS Subinterface with Static IP**

Table 41. Branch VPN0 MPLS subinterface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x.VLAN
	Description	Global	MPLS Interface
IPv4 configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/ maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_ down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Allow service	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_ preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 6: Select **Save** or **Update** to save the template.

BR_INET_INT

Step 7: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface

Template Name: BR_INET_INT

Description: Branch Internet Interface with Static IP

Table 42. Branch VPN0 Internet interface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x
	Description	Global	Internet Interface
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/ maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_ down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_ preference
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 8: Select **Save** to create the template.

BR_INET_INT_DHCP

Step 9: Copy the last template created (**BR_INET_INT**). Edit by changing the parameter IPv4 radio button from static to dynamic.

Template Name: BR_INET_INT_DHCP

Description: Branch Internet Interface with DHCP IP

Table 43. Branch VPN0 Internet interface dynamic IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x
	Description	Global	Internet Interface
IPv4 configuration	IPv4 Address	Radio button	Dynamic
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_ preference
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 10: Select **Update** to save the template.

BR_INET_SUBINT

Step 11: Copy the Internet template static template created (**BR_INET_INT**). Edit by changing the interface name variable to **vpn0_inet_int_gex/x.VLAN**.

Template Name: BR_INET_SUBINT

Description: Branch Internet Subinterface with Static IP

Table 44. Branch VPN0 Internet subinterface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x.VLAN
	Description	Global	Internet Interface
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/ maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_ down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_ preference
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Step 12: Select **Update** to save the template.

BR_TLOC_INT

Step 13: Add a new feature template or copy an existing feature template. Use the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000.

Template: VPN Interface

Template Name: BR_TLOC_INT

Description: Branch TLOC Interface

Table 45. Branch VPN0 TLOC interface/subinterface feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_tloc_int_shutdown
	Interface Name	Device Specific	vpn0_tloc_int_gex/x_or_gex/x.VLAN
	Description	Global	TLOC Interface
IPv4 configuration	IPv4 address	Radio button	Static
	IPv4 address	Device Specific	vpn0_tloc_int_ip_addr/maskbits
Advanced	TLOC extension	Device Specific	vpn0_tloc_wan_int_gex/x

Step 14: Select **Save** to create the template.

BR_WAN_Parent_INT

Step 15: Add a new feature template. Use the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_WAN_Parent_INT

Description: Branch WAN Parent Interface

Table 46. Branch VPN0 WAN parent interface feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_wan_parent_int_ shutdown
	Interface Name	Device Specific	vpn0_wan_parent_int_gex/x
	Description	Global	WAN Parent Interface
Advanced	IP MTU	Global	1504

Step 16: Select **Save** to complete the template.

BR_VPN0_MPLS_BGP

Step 17: Add a new feature template. Use the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: BGP

Template Name: BR_VPN0_MPLS_BGP

Description: Branch VPN 0 MPLS BGP to provider

Table 47. Branch VPN0 MPLS BGP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_bgp _shutdown
	AS Number	Device Specific	vpn0_bgp_as_num
	Router ID	Device Specific	vpn_bgp_router_id
IPv4 Unicast address family	Maximum Paths	Global	2
	Address-Family	Drop-down	ipv4-unicast
	Re-distribute/Protocol	Global	connected
Neighbor	Address	Device Specific	vpn0_bgp_neighbor_address
	Description	Device Specific	vpn_bgp_neighbor_description
	Remote AS	Device Specific	vpn_bgp_neighbor_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	DENY-ALL
	Route-Policy out	Global	On
	Policy name	Global	TLOC-EXT-PREFIX-ONLY
	Shutdown	Device Specific	vpn0_bgp_neighbor_shutdown

Step 18: Select **Save** to complete the template.

Procedure 3 Configure the service side feature templates

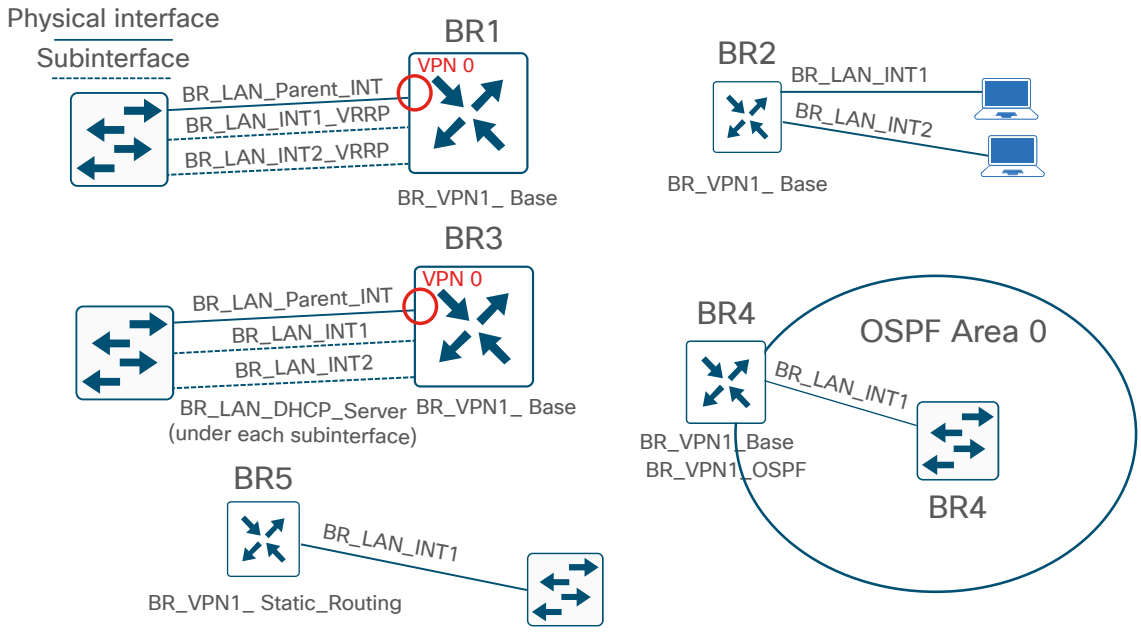
On the service side in the example network, there are several different feature templates that should be created.

Two Service VPN (VPN 1) templates can be built for all branches, one with static routes and one without static routes. The LAN interfaces associated with VPN 1 can be either physical or subinterfaces and static IP addressing is assumed everywhere. One template will represent both physical interfaces and subinterfaces. Most sites use DHCP relay to the data center, so an IP DHCP helper address is configured, but one site vEdge router functions as a DHCP server for the LAN segment. If you have two LAN interfaces on a single vEdge router in the same VPN, you need two separate feature templates; you cannot use the identical feature template under a single VPN more than once.

Following are the feature templates needed for the branch service side:

- VPN 1 base template – One base service VPN feature template can cover most requirements (BR_VPN1_Base for branches 1-4).
- VPN 1 template with static routing configured to point to the LAN side (BR_VPN1_Static_Routing for branch 5).
- VPN interface Ethernet templates – Several different interfaces templates are needed beneath VPN 1:
  - The physical interface/subinterface for one LAN interface with no VRRP (BR_LAN_INT1 for branches 2-5).
  - The physical interface/subinterface for the second LAN interface with no VRRP (BR_LAN_INT2 for branch 2-3).
  - The physical interface/subinterface for one LAN interface configured for VRRP (BR_LAN_INT1_VRRP for branch 1).
  - The physical interface/subinterface for the second LAN interface configured for VRRP (BR_LAN_INT2_VRRP for branch 1).
- The LAN parent physical interface for the subinterfaces. This feature template will actually belong to VPN 0 (BR_LAN_Parent_INT for branch 1 and 3).
- DHCP server pool – A DHCP server pool template is needed under the interface templates. Two need to be created, one for data and one for voice. The voice DHCP server template will contain a Trivial File Transfer Protocol (TFTP) server parameter not used under the data DHCP server template (BR_LAN_DATA_DHCP_Server and BR_LAN_VOICE_DHCP_Server for branch 3).
- OSPF – The OSPF feature template is needed under VPN 1 (BR_VPN1_OSPF for branch 4).

Figure 16. Branch vEdge service side templates



BR_VPN1_Base

One aggregate prefix for the remote site is advertised into OMP instead of multiple site routes. Redistribute connected is turned on to advertise the loopback interface for reachability to and from the data center for management.

Step 1: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN

Template Name: BR_VPN1_Base

Description: Branch VPN1 Base configuration

Table 48. Branch VPN 1 base feature template

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN
	Enhance ECMP Keying	Global	On
Advertise OMP	Connected	Global	On
	Aggregate	Global	On
	Aggregate/Prefix	Device Specific	vpn1_omp_aggregate_prefix
	Aggregate/Aggregate only	Global	On

Step 2: Select **Save** to create the template.

BR_VPN1_Static_Routing

Step 3: In this template, a static route is defined to reach the LAN segments behind a layer 3 switch. This static route needs to be redistributed into OMP since it was disabled within the OMP global template. A network statement in OMP is used to advertise the loopback interface for reachability to and from the data center for management.

Step 4: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN

Template Name: BR_VPN1_Static_Routing

Description: Branch VPN1 Static routing configuration

Table 49. Branch VPN 1 static routing feature template

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN
	Enhance ECMP Keying	Global	On
Advertise OMP	Static	Global	On
	Network	Global	On
	Prefix	Device Specific	vpn1_omp_network_lo_addr/ maskbits
IPv4 Route	Prefix	Device Specific	vpn1_br_static_route_prefix/ maskbits
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn1_next_hop_ip_addr

Step 5: Select Save

BR_LAN_INT1

Step 6: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT1

Description: Branch LAN Interface 1

Table 50. Branch VPN 1 interface 1 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int1_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int1_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10

Step 7: Select **Save** to create the template.

BR_LAN_INT2

Step 8: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT2

Description: Branch LAN Interface 2

Table 51. Branch VPN 1 interface 2 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1_lan_int2_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int2_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10

Step 9: Select **Save** to complete the template.

BR_LAN_INT1_VRRP

Step 10: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT1_VRRP

Description: Branch LAN Interface 1 VRRP

Table 52. Branch VPN 1 interface 1 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int1_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int1_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP (Select New VRRP)	Group ID	Global	1
	Priority	Device Specific	vpn1_vrrp_priority1
	Track OMP	Global	On
	Track prefix list	Global	default-route
	IP Address	Device Specific	vpn1_vrrp_ip_addr1

Step 11: Select **Save** to create the template.

BR_LAN_INT2_VRRP

Step 12: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT2_VRRP

Description: Branch LAN Interface 2 VRRP

Table 53. Branch VPN 1 interface 2 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1_lan_int2_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int2_description
IPv4 configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP (Select New VRRP)	Group ID	Global	2
	Priority	Device Specific	vpn1_vrrp_priority2
	Track OMP	Global	On
	Track prefix list	Global	default-route
	IP Address	Device Specific	vpn1_vrrp_ip_addr2

Step 13: Select **Save** to create the template.

BR_LAN_Parent_INT

Step 14: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_Parent_INT

Description: Branch LAN Parent Interface

Table 54. Branch VPN1 LAN parent interface feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_parent_int_shutdown
	Interface Name	Device Specific	vpn1_lan_parent_int_gex/x
	Description	Global	LAN Parent Interface
Advanced	IP MTU	Global	1504

Step 15: Select **Save** to complete the template.

BR_LAN_DATA_DHCP_Server

Step 16: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: DHCP Server

Template Name: BR_LAN_DATA_DHCP_Server

Description: Branch LAN DHCP Server for Data VLAN

Table 55. Branch VPN1 LAN DHCP Server for Data VLAN feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Address Pool	Device Specific	data_dhcp_address_pool/ maskbits
	Exclude Addresses	Device Specific	data_dhcp_address_exclude_ range
Advanced	Domain Name	Global	cisco.local
	Default Gateway	Device Specific	data_dhcp_default_gateway
	DNS Servers	Global	10.4.48.10

Step 17: Select **Save** to complete the template.

BR_LAN_VOICE_DHCP_Server

Step 18: Copy and edit the previous template and change the variable names. Also add the TFTP server's variable to the template since the second DHCP server pool is used for the VOICE VLAN. Use the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: DHCP Server

Template Name: BR_LAN_VOICE_DHCP_Server

Description: Branch LAN DHCP Server for Voice VLAN

Table 56. Branch VPN1 LAN DHCP Server for Voice VLAN feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Address Pool	Device Specific	voice_dhcp_address_pool/ maskbits
	Exclude Addresses	Device Specific	voice_dhcp_address_exclude_ range
Advanced	Domain Name	Global	cisco.local
	Default Gateway	Device Specific	voice_dhcp_default_gateway
	DNS Servers	Global	10.4.48.10
	TFTP Servers	Global	10.4.48.19

Step 19: Select **Update** to save the template.

BR_VPN1_OSPF

Step 20: Add a new feature template using the following parameters:

Devices: vEdge 100B, vEdge 100M, vEdge100WM, vEdge 1000

Template: OSPF

Template Name: BR_VPN1_OSPF

Description: Branch LAN VPN 1 OSPF

Table 57. Branch VPN1 OSPF feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Router ID	Device Specific	vpn1_ospf_router_id
Redistribute	Protocol	Global	omp
Area	Area Number	Global	0
	Interface/Interface Name	Device Specific	vpn1_ospf_interface_gex/x
	Interface/Interface Cost	Device Specific	vpn1_ospf_interface_cost
	Interface/Advanced/ OSPF Network Type	Global/ drop-down	point-to-point
	Interface/ Authentication/ Authentication Type	Global/ drop-down	message-digest
	Interface/Message Digest/Message Digest Key ID	Global	22
	Interface/Message Digest/Message Digest Key	Device Specific	vpn1_ospf_message_digest_ key
Area Range	Address	Device Specific	vpn1_ospf_area_range_ address_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Global	On

Step 21: Select **Save** to complete the template.

Procedure 4 Create the branch device templates

Once the feature templates are created, the device templates can be created. There are five general types of branches in this example network.

- Type A branch: Dual vEdge router site, hybrid configuration (MPLS and Internet), TLOC interfaces, layer 2 switch stack, VRRP
- Type B branch: Single vEdge router site, hybrid configuration (MPLS and Internet), no LAN switch
- Type C branch: Single vEdge router site, hybrid configuration (MPLS and Internet), single layer 2 LAN switch.
- Type D branch: Dual vEdge router site, hybrid configuration (MPLS and Internet), TLOC interfaces, layer 3 switch, OSPF
- Type E branch: Single vEdge router site, hybrid configuration (MPLS and Internet), CE router, layer 3 switch

For branches 1 and 4, the Internet-connected vEdge router and the MPLS-connected vEdge router each has a different vEdge device template because the BGP feature template needs to be added to the device template of the MPLS-connected vEdge router.

Configure the following device templates:

- Branch_A_MPLS_BGP_TLOC_VRRP (branch 1, vEdge 1)
- Branch_A_INET_TLOC_VRRP (branch 1, vEdge 2)
- Branch_B_INET(DHCP) (branch 2)
- Branch_C_INET(DHCP)_LAN_DHCPServer (branch 3)
- Branch_D_MPLS_BGP_TLOC_SubInt_OSPF (branch 4, vEdge 1)
- Branch_D_INET_TLOC_SubInt_OSPF (branch 4, vEdge 2)
- Branch_E_MPLS_CE_LAN_Static_Routing (branch 5)

Branch_A_MPLS_BGP_TLOC_VRRP

Step 1: From the vManage GUI, go to **Configuration>Templates** and ensure the **Device** tab is selected.

Step 2: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 3: Fill out the **Device Model**, **Template Name,** and **Description**.

Device Model: vEdge 1000

Template Name: Branch_A_MPLS_BGP_TLOC_VRRP

Description: Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-side Trunk and VRRP

Step 4: Configure with the following feature templates:

Table 58. Branch_A_MPLS_BGP_TLOC_VRRP device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_VRRP_INT1
	VPN Interface	BR_LAN_VRRP_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Step 5: Select **Create** to create and save the template.

Branch_A_INET_TLOC_VRRP

Step 6: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 7: Configure the device template with the following parameters:

Device Model: vEdge 1000

Template Name: Branch_A_INET_TLOC_VRRP

Description: Branch Dual vEdge Hybrid TLOC with INET and LAN-side Trunk and VRRP

Table 59. Branch_A_INET_TLOC_VRRP device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_VRRP_INT1
	VPN Interface	BR_LAN_VRRP_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Step 8: Select **Create** to create and save the template.

Branch_B_INET(DHCP)

Step 9: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 10: Configure the device template with the following parameters:

Device Model: vEdge 100 WM

Template Name: Branch_B_INET(DHCP)

Description: Branch Single vEdge Hybrid Internet DHCP address and No Switch

Table 60. Branch_B_INET(DHCP)

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_MPLS_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface	BR_LAN_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Step 11: Select **Create** to create and save the template.

Branch_C_INET(DHCP)_LAN_DHCPServer

Step 12: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 13: Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_C_INET(DHCP)_LAN_DHCPServer

Description: Branch Single vEdge Hybrid Internet DHCP address with LAN Trunk and DHCP Server

Table 61. Branch_C_INET(DHCP)_LAN_DHCPServer device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface>DHCP Server	BR_LAN_DATA_DHCP_Server
SNMP	VPN Interface	BR_LAN_INT2

Template type	Template sub-type	Template name
	VPN Interface>DHCP Server	BR_LAN_VOICE_DHCP_Server
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Step 14: Select **Create**

Branch_D_MPLS_BGP_TLOC_SubInt_OSPF

Step 15: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 16: Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_D_MPLS_BGP_TLOC_SubInt_OSPF

Description: Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP and LAN-side OSPF

Table 62. Branch_D_MPLS_BGP_TLOC_Subint_OSPF device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_INET_SUBINT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_WAN_Parent_INT

Template type	Template sub-type	Template name
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Step 17: Select **Create**

Branch_D_INET_TLOC_SubInt_OSPF

Step 18: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 19: Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_D_INET_TLOC_SubInt_OSPF

Description: Branch Dual vEdge Hybrid TLOC SubInts with INET and LAN-side OSPF

Table 63. Branch_D_INET_TLOC_SubInt_OSPF device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0

Template type	Template sub-type	Template name
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_SUBINT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Step 20: Select **Create** to create and save the template.

Branch_E_MPLS_CE_LAN_Static_Routing

Step 21: Select **Create Template** and select **From Feature Template** from the drop-down box.

Step 22: Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_E_MPLS_CE_LAN_Static_Routing

Description: Branch Single vEdge Hybrid with MPLS CE and Static Routing for LAN

Table 64. Branch_E_MPLS_CE_LAN_Static_Routing device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Step 23: Select **Create** to create and save the template.

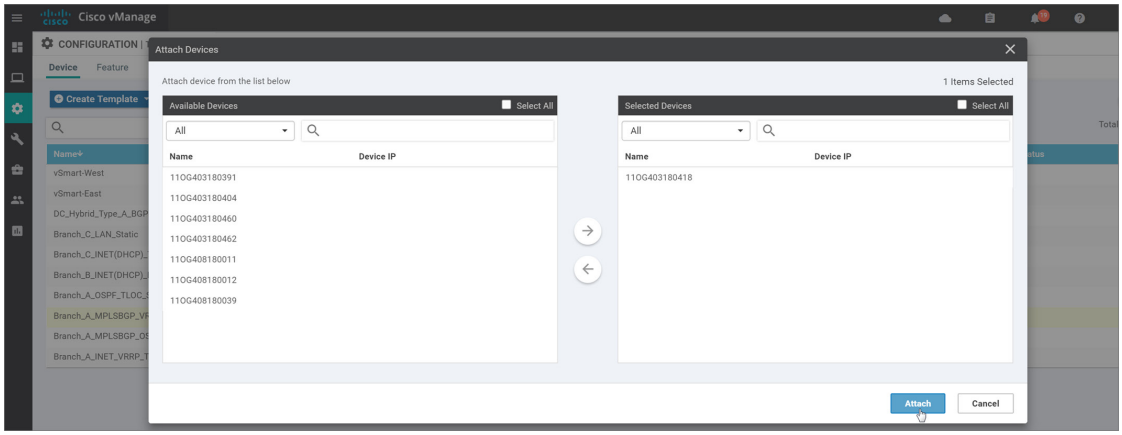
Procedure 5 Attach the device templates

In this procedure, you attach the device templates to the vEdge branch routers. When these routers become active and establish the controller connections in the network, the vManage will push the full configurations down to them.

Step 1: Go to **Configuration>Templates**. Ensure the **Device** tab is selected.

Step 2: Beside the desired template (**Branch_A_MPLS_BGP_TLOC_VRRP**), select **...** and select **Attach Devices**.

Step 3: Select branch 1 vEdge 1 connected to the MPLS transport, br1-ve1. You will need to find the serial number associated with this device because this device is not on the network yet. **Show hardware inventory** on the console is one way to view the serial number of a device. The serial numbers of all of the vEdge 1000 routers in the authorized serial list should show up in the pop-up window because that is the device type of the device template that was chosen. Select the serial number and then select the arrow to bring the device from the **Available Devices** row to the **Selected Devices** row. Select **Attach**.



Step 4: Similar to the data center device template deployment, you have to fill out the values to the variables of the device template. Select the **...** to the right of the device and select **Edit Device Template**.

Step 5: Fill in the following variables (via the .csv spreadsheet or manually).

Table 65. Branch 1 vEdge 1 device template variable values

Variable	Value
Password(user_admin_password)	admin
Hostname(system_host_name)	br1-ve1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,v1000,US,West,UG5,Primary
System IP(system_system_ip)	10.255.241.11
Site ID(system_site_id)	112002

Variable	Value
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	192.168.101.1
Address(vpn0_inet_next_hop_ip_addr)	10.101.2.2
AS Number(vpn0_bgp_as_num)	65201
Shutdown(vpn0_bgp_shutdown)	☐
Router ID(vpn_bgp_router_id)	10.255.241.11
Address(vpn0_bgp_neighbor_address)	192.168.101.1
Description(vpn0_bgp_neighbor_description)	MPLS BGP Service Provider
Shutdown(vpn0_bgp_neighbor_shutdown)	☐
Remote AS(vpn0_bgp_neighbor_remote_as)	102
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.101.2.1/30
NAT	☐
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	192.168.101.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000
Interface Name(vpn0_tloc_int_gex/x_or_gex/x.VLAN)	ge0/7

Variable	Value
IPv4 Address(vpn0_tloc_int_ip_addr/maskbits)	10.101.1.1/30
TLOC Extension(vpn0_tloc_wan_int_gex/x)	ge0/2
Shutdown(vpn0_tloc_int_shutdown)	☐
Interface Name(vpn1_lan_parent_int_gex/x)	ge0/4
Shutdown(vpn1_lan_parent_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.159/23
Prefix(vpn1_omp_aggregate_prefix)	10.101.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/4.10
Description(vpn1_int1_description)	Data Vlan
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.101.10.2/24
Shutdown(vpn1_lan_int1_shutdown)	☐
Priority(vpn1_vrrp_priority1)	200
IP Address(vpn1_vrrp_ip_addr1)	10.101.10.1
Interface Name(vpn_lan_int2_gex/x_or_gex/x.VLAN)	ge0/4.20
Description(vpn1_int2_description)	Voice Vlan
IPv4 Address(vpn_int2_ip_addr/maskbits)	10.101.20.2/24
Shutdown(vpn1_lan_int2_shutdown)	☐
Priority(vpn_vrrp_priority2)	200
IP Address(vpn_vrrp_ip_addr2)	10.101.20.1
IPv4 Address(vpn1_lo0_ip_addr/maskbits)	10.255.241.11/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-VE1
Location of Device(snmp_device_location)	Branch 1
vedgePolicy/bgp_tloc_ext_prefix_to_advertise	10.101.1.0/30

Step 6: Select **Update**. Before selecting next, you may want to download the .csv file to save your variable values for reuse before moving on.

Step 7: Select **Next**, and then **Configure**. Since the device is offline, the configuration will be attached when the device comes online.

Step 8: Repeat steps 1-8 with the following templates. See Appendix E for the variable values.

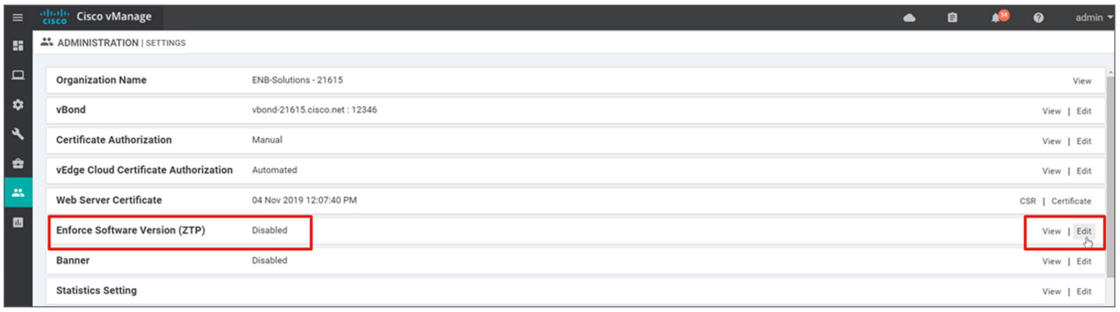
- BR1-VE2: Branch_A_INET_TLOC_VRRP
- BR2-VE1: Branch_B_INET(DHCP)
- BR3-VE1: Branch_C_INET(DHCP)_LAN_DHCPServer
- BR4-VE1: Branch_D_MPLS_BGP_TLOC_SubInt_OSPF
- BR4-VE2: Branch_D_INET_TLOC_SubInt_OSPF
- BR5-VE1: Branch_E_MPLS_CE_LAN_Static_Routing

Procedure 6 Bring remote vEdge routers online

In this procedure, the first vEdge, br1-ve2, will be brought online using ZTP. A software upgrade will also be performed by the ZTP process.

The ge0/0 interface on the vEdge 1000 router is configured for DHCP from factory default settings. Once the vEdge router gets an IP address, it will attempt to resolve ztp.viptela.com in order to find its vBond IP address and start the authentication process with the controllers.

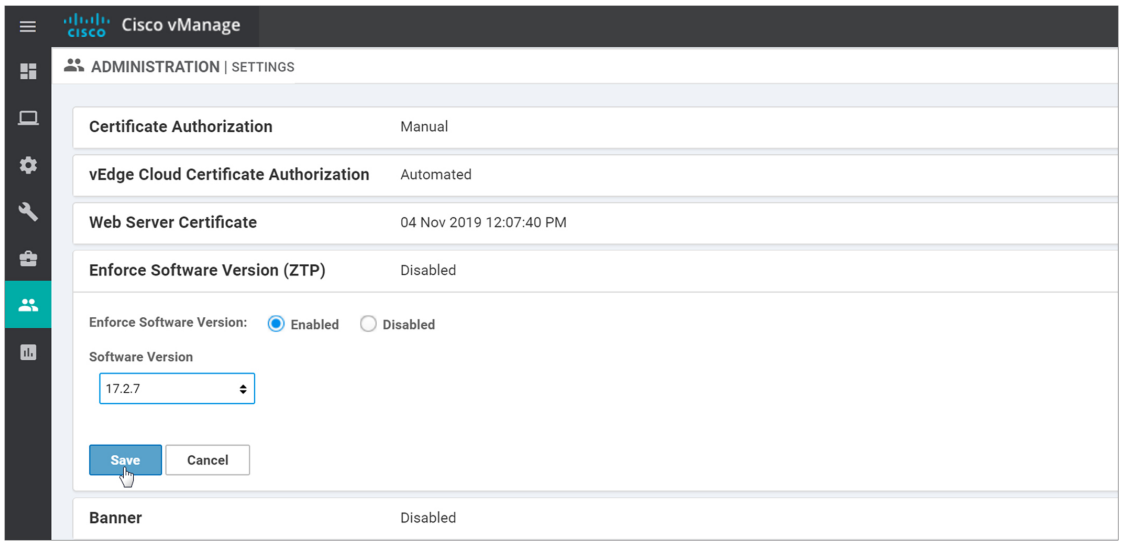
Step 1: To check the code version for the vEdge router that comes online via ZTP, go to **Administration>Settings** from the vManage GUI. Find the **Enforce Software Version (ZTP)** configuration. Select **Edit** in the far right.



Step 2: Next to **Enforce Software Version**, select the **Enabled** radio button.

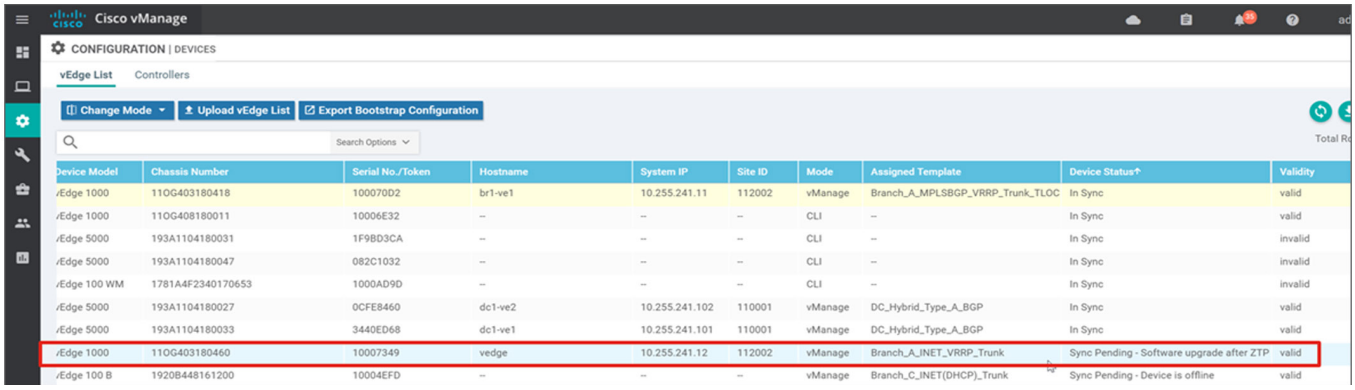
Step 3: From the drop-down box, choose the software version (17.2.7).

Step 4: Select **Save**.

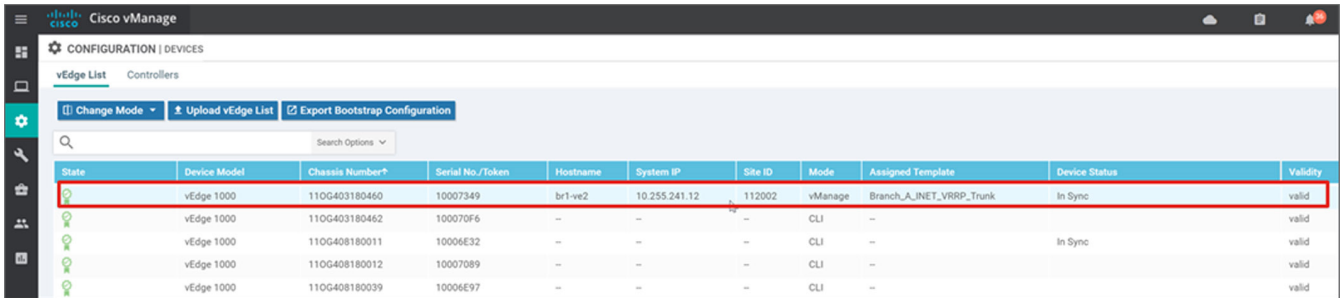


Br1-ve2 is installed into the network. It is a vEdge 1000 and its ZTP port, ge0/0, is plugged into the Internet transport. It is assumed that br1-ve2 is at factory defaults, and is currently running 17.2.6 software.

Step 5: Power on the vEdge router. The vEdge reaches out to the ZTP server, then authenticates to the vBond and the rest of the controllers. The code is then upgraded.



Step 6: The full configuration is pushed and the vEdge router becomes in sync with vManage.

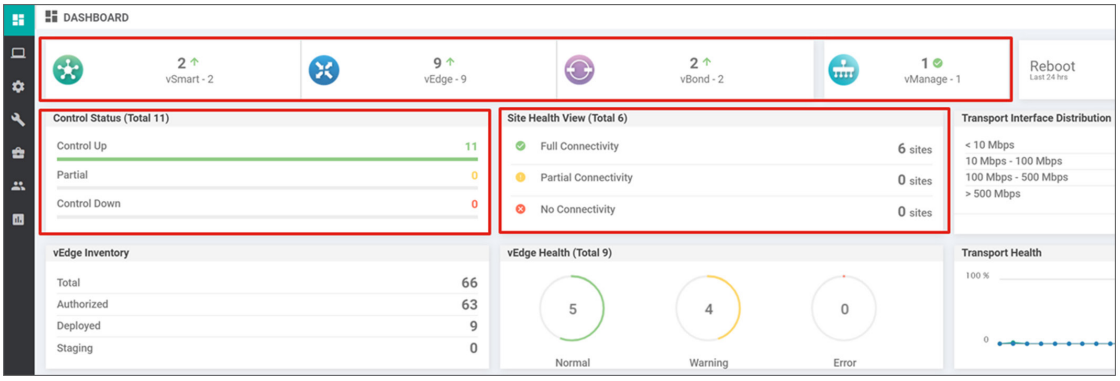


Step 7: Bring the additional vEdge devices up, either through ZTP or the bootstrap process.

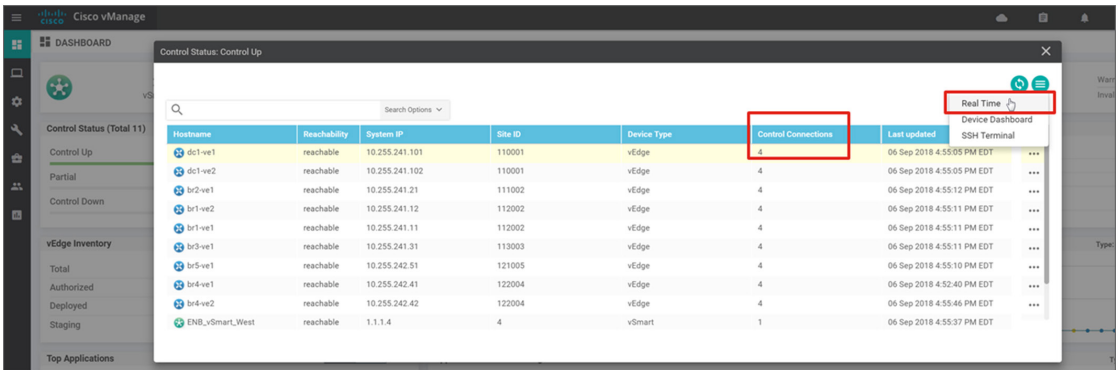
Step 8: Upgrade the vEdge routers if need be, either automatically through ZTP or through vManage.

Procedure 7 Verify the network status

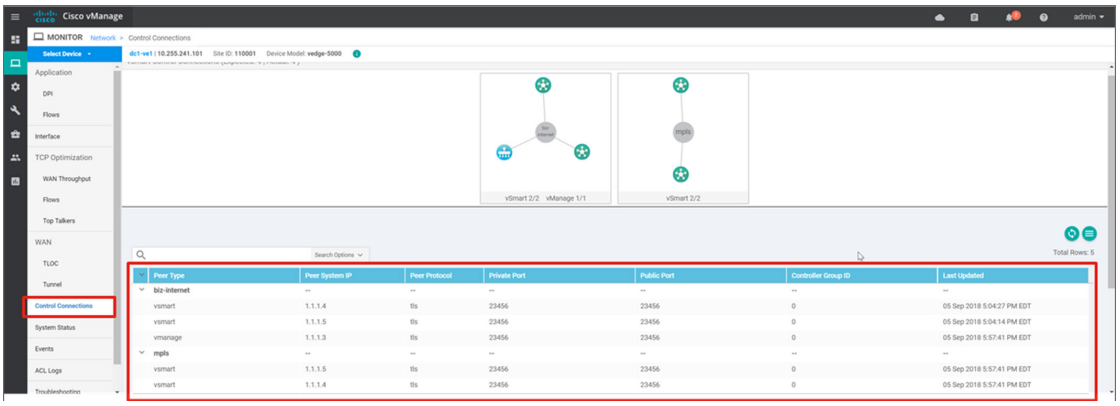
Step 1: Verify the status of the network. vManage should show that all devices are reachable at the top of the dashboard. The **Control Status** should show that all of the control connections are up for the nine vEdge routers and two vSmart controllers, and the **Site Health View** should show **Full Connectivity** to six sites, the data center and the five branches. This means that each vEdge device is able to connect to all other vEdge devices over each transport. Note that only MPLS-connected vEdge routers can connect to other MPLS-connected vEdge routers because the restrict keyword is configured.



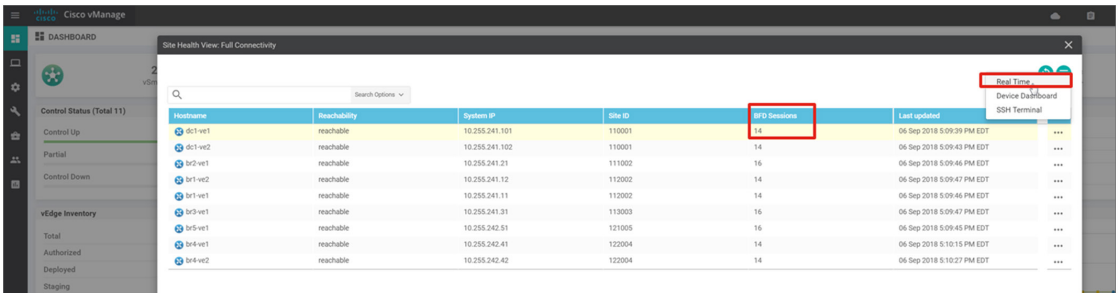
Step 2: If you select **Control Up**, **Partial**, or **Control Down** in the **Control Status** box, you will get a pop-up window summarizing the number of control connections each vEdge device has. This counts only the vSmart connections. To get more information, select **...** to the right of the desired device and select **Real Time** or **Device Dashboard**.



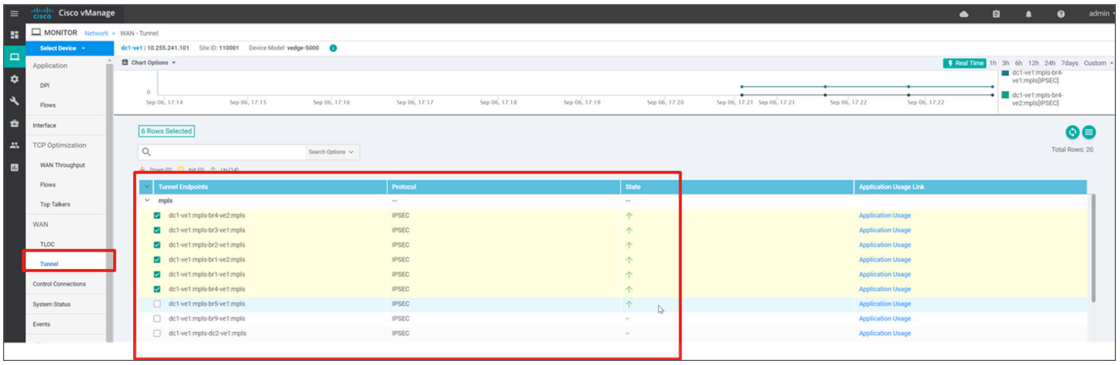
Step 3: To view the state of all of the control connections, select **Control Connections** in the left column.



Step 4: If you select **Full Connectivity**, **Partial Connectivity**, or **No Connectivity** in the **Site Health View** box, you will get a pop-up window summarizing the number of BFD connections each vEdge has. To get more information, to the right of the desired device, go to **...** and select **Real Time** or **Device Dashboard**.



Step 5: To view the state of all of the IPSec tunnel or data plane connections, select **Tunnel** under the WAN category in the left column.



Process

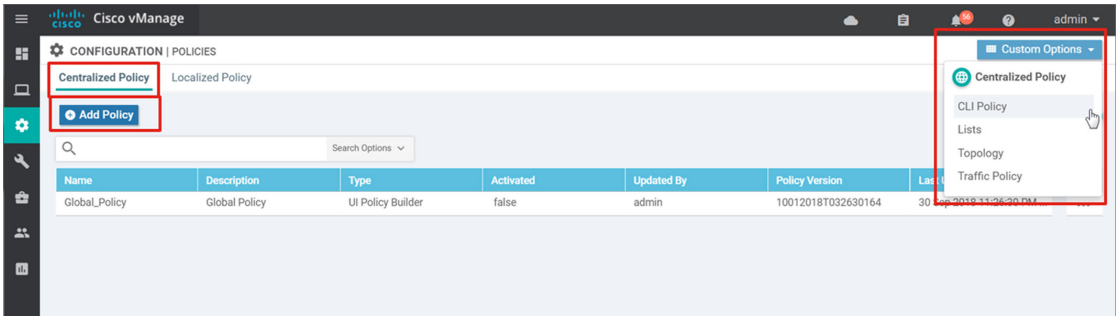
Configuring centralized policy

Centralized policies are configured in the vManage GUI under **Configuration>Policies**, under the **Centralized Policy** tab. This page will help create the centralized policy that will be downloaded to the vSmart controllers.

You can select **the Custom Options** box to create a CLI policy, or define lists, or create different policy definitions outside of the centralized policy. You can create policy definitions separately and then import, or attach them, into the centralized policy at any time. Once attached to the central policy, you cannot make any edits to the policy definitions through the central policy; you have to go to the **Custom Options** box on the **Configurations>Policies (Centralized Policy** tab**)** page, select Topology (for control policy) or Traffic Policy (for data policy) to bring up the list of policy definitions to edit them.

When you select the **Add Policy** button on this main page, you are actually starting the definition of a centralized policy, and only one centralized policy can be downloaded to a vSmart controller at any one time. You then start creating a series of control or data policy definitions inside the centralized policy, and then apply them to site and VPN lists. Once saved, the centralized policy will be downloaded to the vSmart controllers.

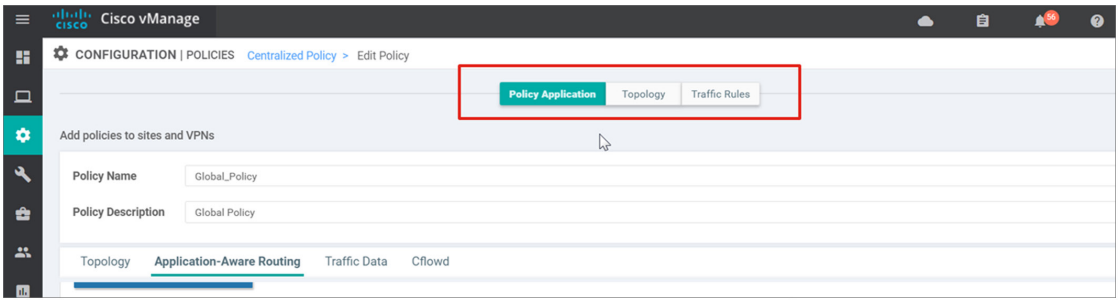
Figure 17. vManage centralized policy section



There are four main steps when creating centralized policy:

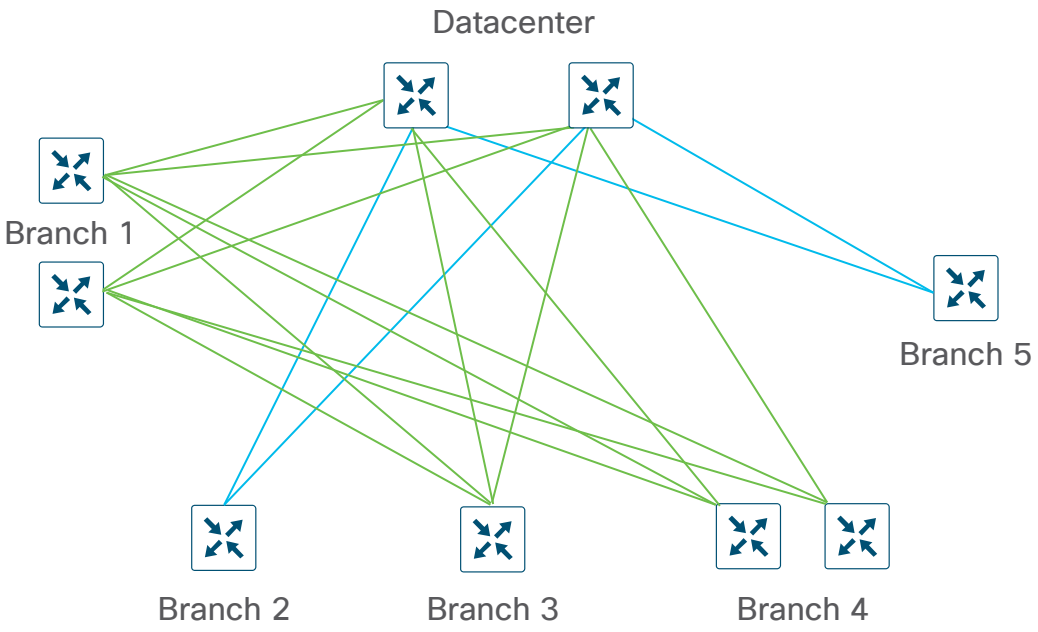
1. Create groups of interest. In this section, you will create lists that you will use in your policy, such as application, color, data prefixes, policer, prefix, site, SLA class, TLOC, and VPN lists. Minimally, you need to create a list of site IDs in order to apply the individual policy definitions. When you create site IDs for applying policy definitions, you must not overlap site IDs in different lists. You may also need a list of the Service VPNs a policy may apply to, as well as lists for match and action statements within the policy sequences.
2. Configure topology and VPN membership (control policy). Under the Topology and VPN Membership page, you can select either the Topology or VPN Membership tab. Under the Topology tab, you will be able to configure control policy. You can select from a full-mesh or hub-and-spoke predefined policy, or you can select to configure your own custom route and TLOC policy definition. You can also import an existing control policy into the centralized policy. Under the VPN Membership tab, you can create a policy definition that allows or restricts VPNs at various sites.
3. Configure traffic rules (data policy). Under the Traffic Rules page, you can create an application-aware routing, traffic data, or Cflowd policy. You can also import existing data policy definitions already created outside of the centralized policy.
4. Apply policies to sites and VPNs. In the last step, you name and describe the new centralized policy. You then apply the various policy definitions to a site list. You may need to apply a VPN list as well.

If you try to edit an existing centralized policy, you can navigate to the **Topology** and **Traffic Rules** pages to configure or import new policies by selecting the correct box at the top of the page. Once created or imported, you need to navigate back to **Policy Application** and attach the policy definition to a site list.



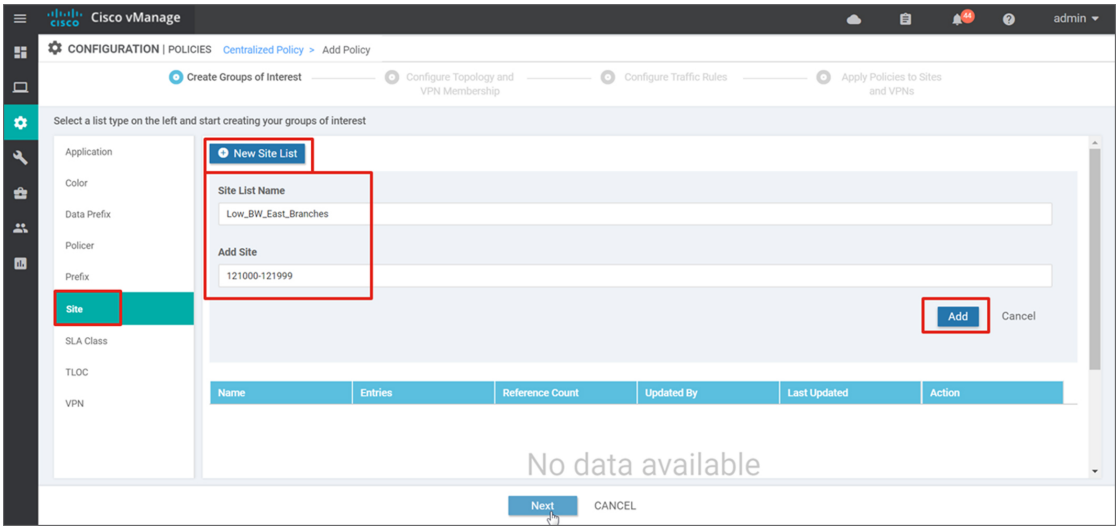
For the example network, create a centralized policy to create a hub-and-spoke topology for the low-bandwidth sites (branches 2 and 5). In the following figure, branches 2 and 5 only form IPSec tunnels with the data center vEdge routers. This is accomplished by filtering routes and TLOC routes.

Figure 18. Hub-and-spoke topology for branches 2 and 5



Step 1: Go to **Configuration>Policies** and ensure that the **Centralized Policy** tab is selected. Select **Add Policy**.

Step 2: Create a list of various sites. Select **Site** in the left column. Select **New Site List** and under **Site List Name**, type **Low_BW_East_Branches**. Then type **121000-121999** under **Add Site**. Select **Add**.



Step 3: Repeat step 2 and create the following:

a. **Low_BW_West Branches: 111000-111999**

b. **High_BW_East Branches: 122000-129999**

c. **High_BW_West Branches: 112000-119999**

d. **West_DC1: 110001**

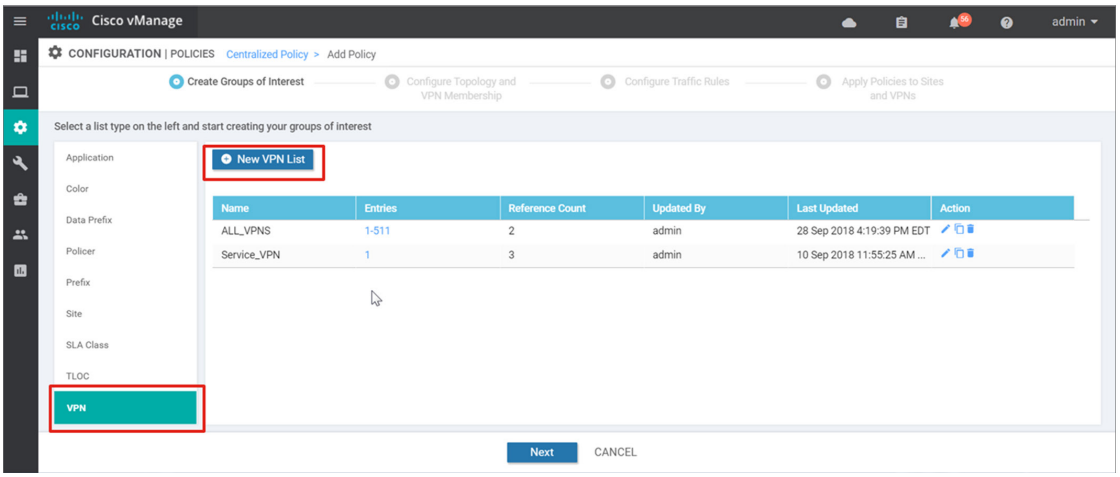
e. **ALL_SITES: 0-4294967295**

f. **All_US_Sites: 110000-129999**

g. **Low_BW_US_Sites: 111000-111999,121000-121999**

Step 4: Create a VPN list. The policy will apply to the Service VPN, VPN 1. Select **VPN on the left**, then select **New VPN List**. Type in the VPN list name (**Service_VPN**) and then type **1** in the **Add VPN** textbox. Select **Add**.

Step 5: Add another VPN list called **ALL_VPNS**, with a VPN list of **1-511**. Select **Add**.



Step 6: Select **Next**. You will now configure topology and VPN membership.

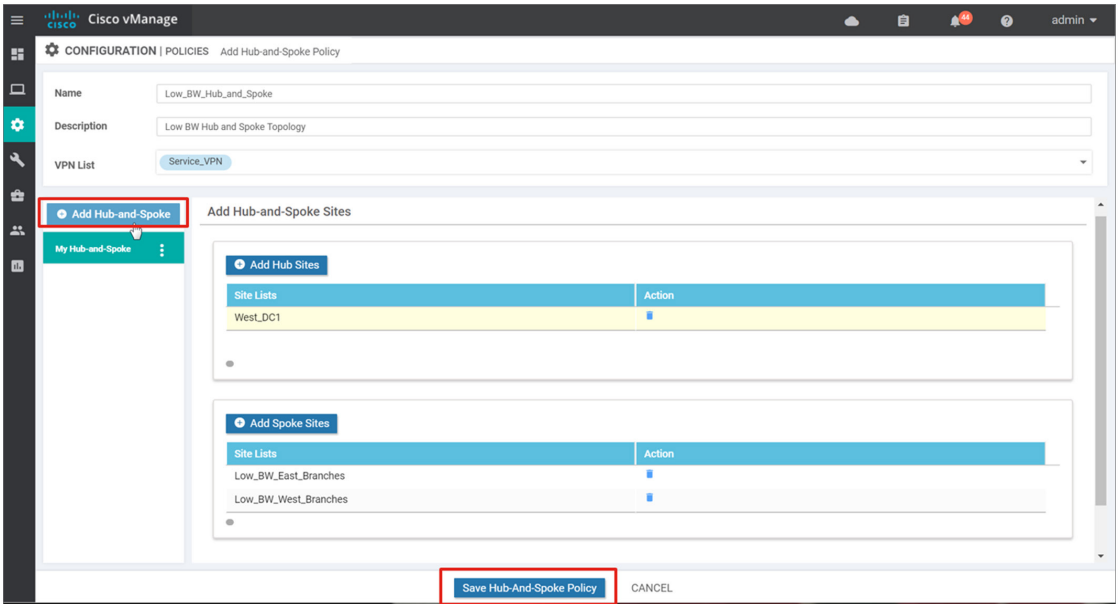
Step 7: Ensure you are on the **Topology** tab and select **Add Topology**. Select **Hub-and-Spoke** from the drop-down menu.

Step 8: Type **Name** (**Low_BW_Hub_and_Spoke**), and **Description** (**Low BW Hub and Spoke Topology**). Select **Service_VPN** list from the **VPN List**.

Step 9: Select **Add Hub Sites**. Under the site list, select **West_DC1** and select **Add**.

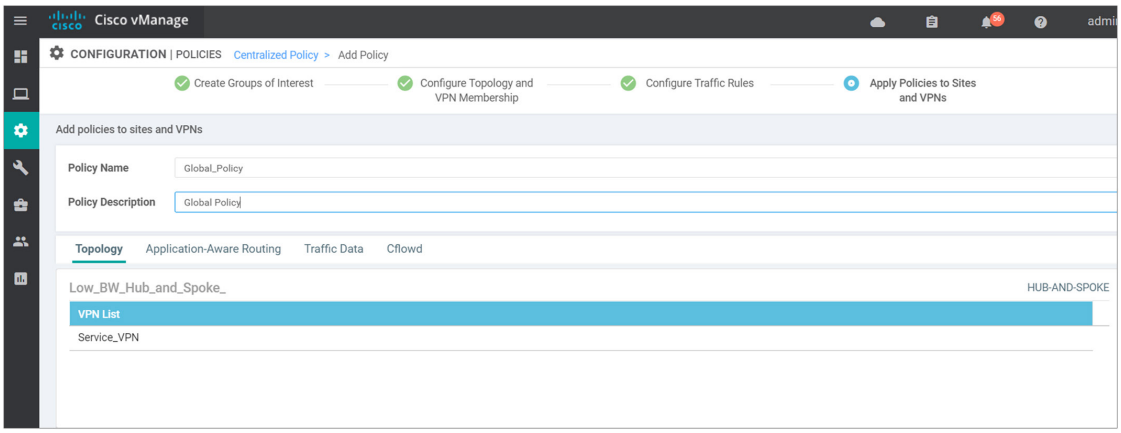
Step 10: Select **Add Spoke Sites**. Select **Low_BW_East_Branches** and select **Add**. Repeat the step for **Low_BW_West_Branches**.

Step 11: Select **Save Hub-And-Spoke Policy** at the bottom of the page. You have just finished a policy definition that needs to be applied to a site list.



Step 12: Select **Next**. Skip the **Traffic Rules** page by selecting **Next** again.

Step 13: On this page, the centralized policy is named. Type in the **Policy Name** (**Global_Policy**) and **Policy Description** (**Global Policy**), and select **Save Policy**.



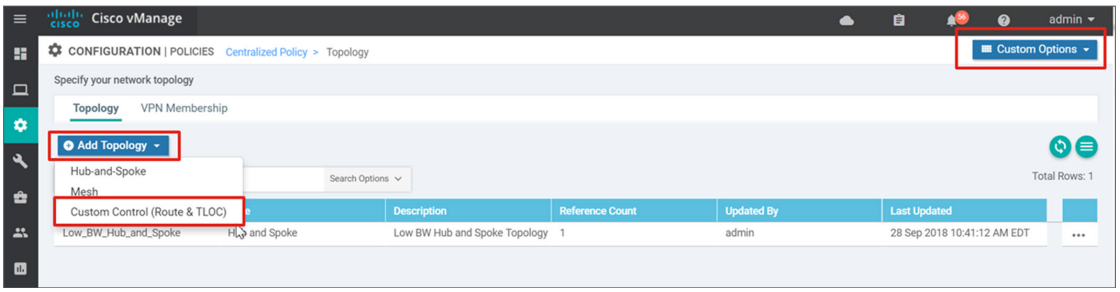
Tech tip

When you use the Predefined Hub-and-Spoke topology policy, only TLOCs and routes from the data center site are distributed to the low-bandwidth sites specified. Ensure a summary or default route is distributed from the data center if you want the low-bandwidth sites to reach other remote sites through the hub when using this policy.

Note that the high-bandwidth sites still have route and TLOC information from branches 2 and 5 and attempt to form IPSec tunnels with those branches but the low-bandwidth branches don't have connectivity back to any other branches. In this case, you will see partial connectivity in the vManage dashboard. One simple way to remediate this condition is that routes and TLOCs can also be filtered from the low-bandwidth sites. This would be applied to the high-bandwidth sites as an outbound policy on the vSmart controllers, so only routes and TLOCs to the high-bandwidth sites will be filtered (routes and TLOCs going to the data center will be untouched). If connectivity to the low-bandwidth sites is needed through the data center site, this assumes some sort of summary or default is advertised from the data center sites for that connectivity.

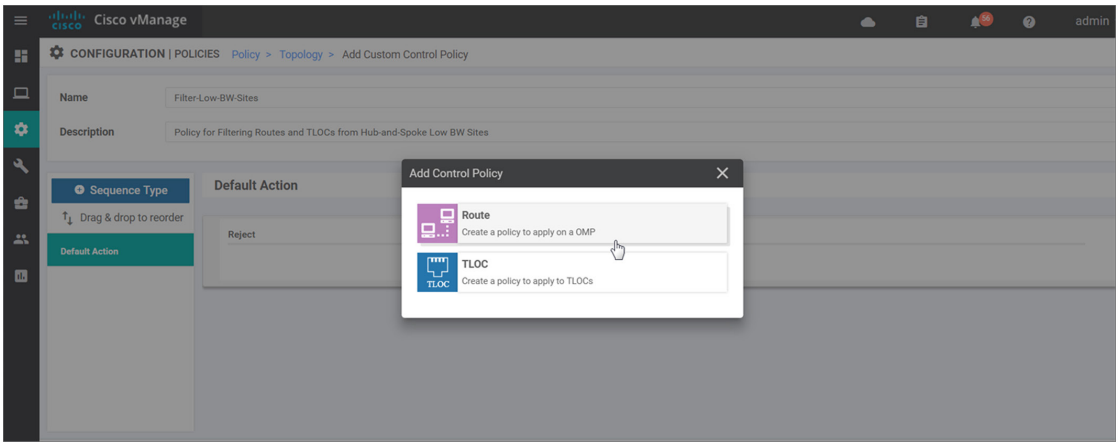
Step 14: From the **Configuration>Policies** page, select **Custom Options** in the top right corner of the page. Select **Topology** from the drop-down menu, since you are adding an additional control policy definition.

Step 15: Select **Add Topology** and select **Custom Control (Route and TLOC)** from the drop-down list.



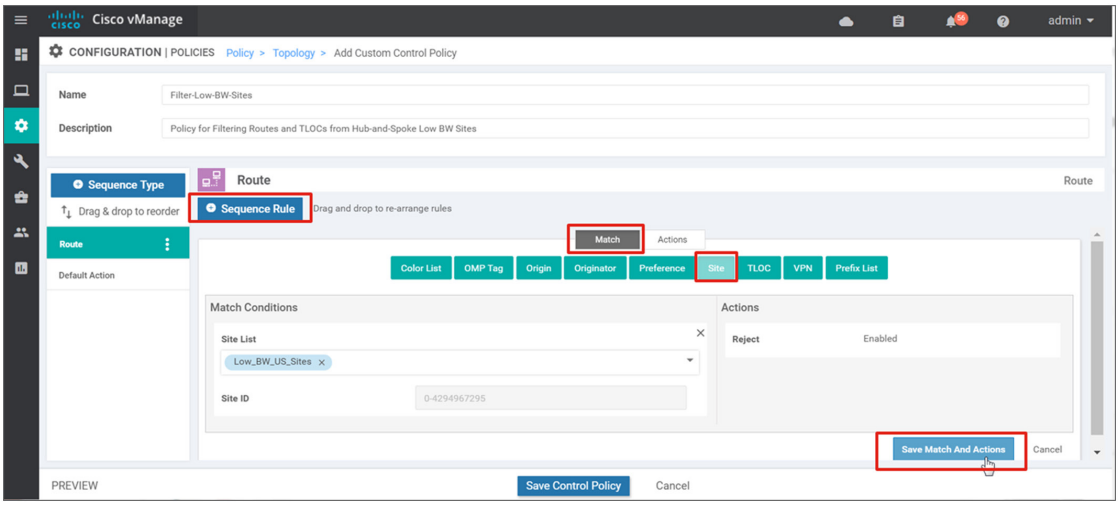
Step 16: Type **Name** (**Filter-Low-BW-Sites**) and **Description** (**Policy for Filtering Routes and TLOCs from Hub-and-Spoke Low BW Sites**).

Step 17: Select **Sequence Type** on the left of the page and on the **Add Control Policy** pop-up window, select **Route**.



Step 18: Select **Sequence Rule**. The **Match** box should be highlighted. Select **Site** and under **Site List**, select **Low_BW_US_Sites**. Under **Actions**, the default is already set to **Reject**.

Step 19: Select **Save Match and Actions.**

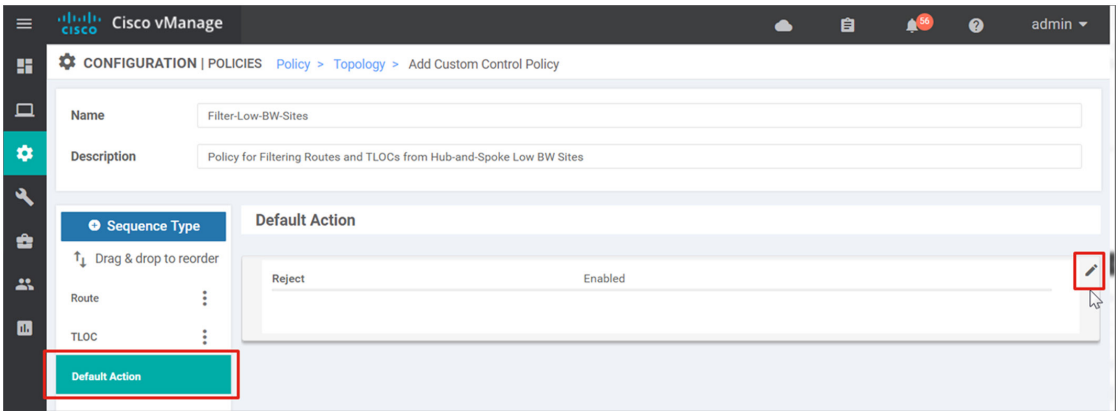


Step 20: Select **Sequence Type** on the left of the page and on the **Add Control Policy** pop-up window, select **TLOC**.

Step 21: Select **Sequence Rule**. The **Match** box should be highlighted. Select **Site** and under **Site List**, select **Low_BW_US_Sites**. Under **Actions**, the default is already set to **Reject**.

Step 22: Select **Save Match and Actions.**

Step 23: Select **Default Action** from the left column. Select the **Edit** symbol to the far right. Select the **Accept** box, then select **Save Match and Actions**.

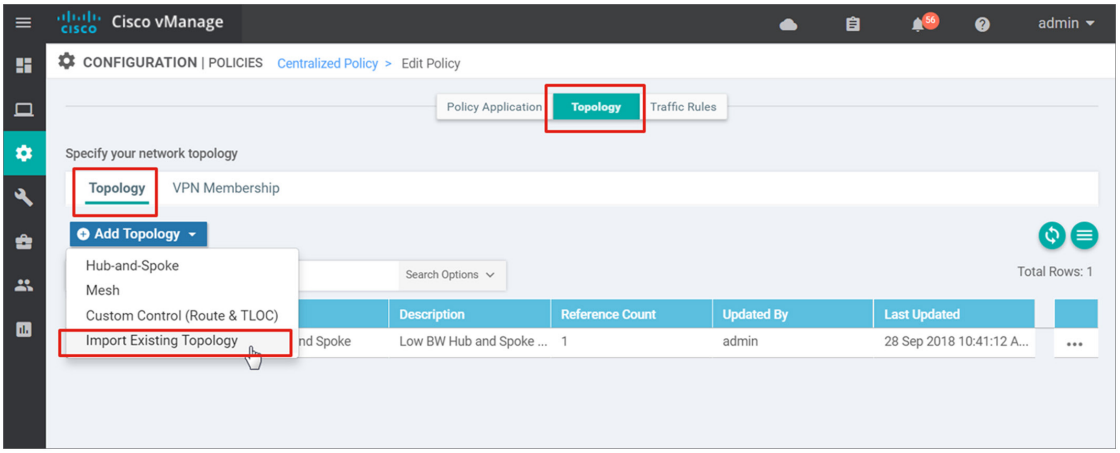


Step 24: Select **Save Control Policy** to save the policy definition.

Step 25: Since the policy definition was created outside of the centralized policy called **Global_Policy**, it needs to be imported into **Global_Policy** and applied to a site list. Go to **Configuration>Policies** and ensure the **Centralized Policy** tab is selected.

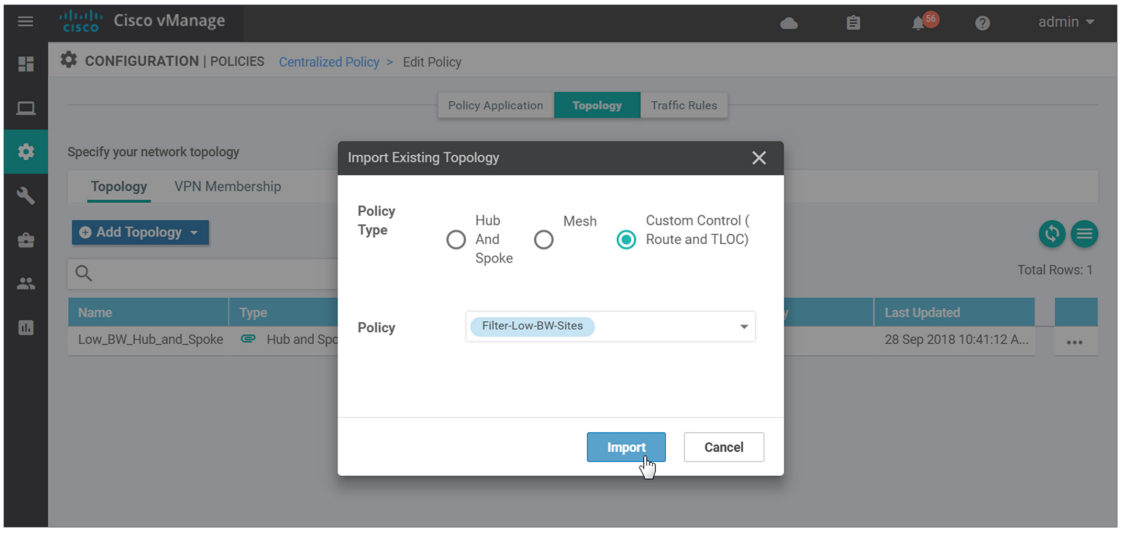
Step 26: Select **...** to the far right of the policy named **Global_Policy** and select **Edit** from the drop-down menu.

Step 27: Select the **Topology** box at the top of the page. Select **Add Topology** and **Import Existing Topology** from the drop-down menu.



Step 28: Next to **Policy Type**, select the **Custom Control (Route and TLOC)** radio button, then next to **Policy**, select **Filter-Low-BW-Sites** from the drop-down box.

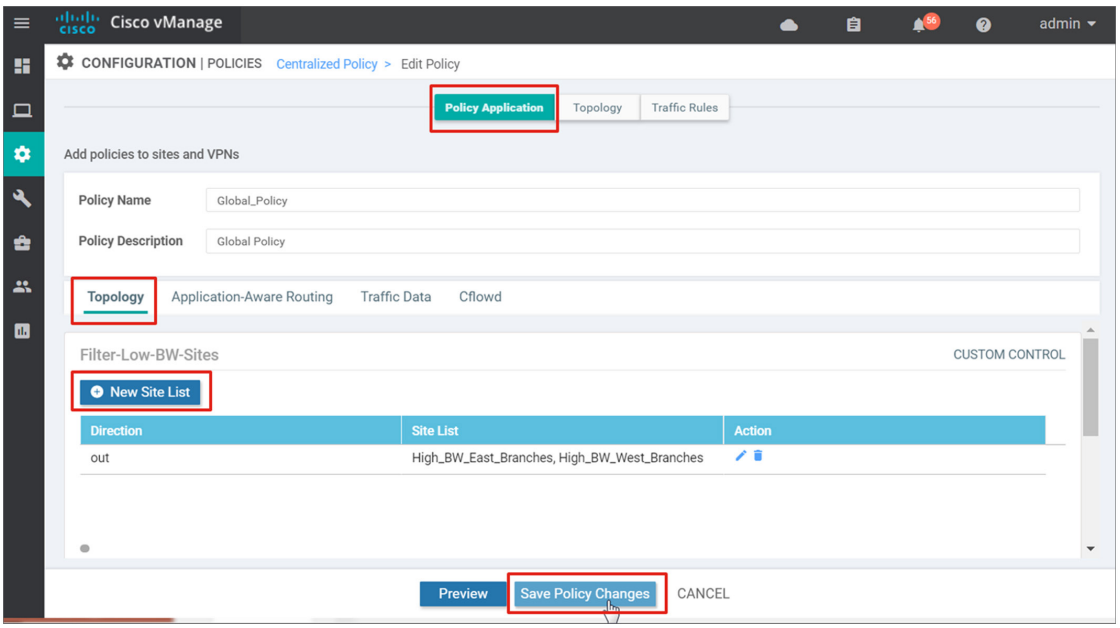
Step 29: Select **Import.**



Step 30: Now that the policy definition has been imported, select the **Policy Application** box at the top of the page in order to configure the site list the policy definition applies to.

Step 31: Under the **Filter-Low-BW-Sites** section, select **New Site List** and under the **Outbound Site List**, select **High_BW_East_Branches** and **High_BW_West_Branches**. Select **Add**.

Step 32: Select **Save Policy Changes**.



Step 33: Now that the policy is created, it can be attached to the vSmart controllers and activated. Under **Configuration>Policies** within **the Centralized Policy** tab**,** select **...** to the far right of the policy called **Global_Policy**. Select **Activate** from the drop-down menu.

A window pops up and states that the policy will be applied to the reachable vSmarts (1.1.1.5, 1.1.1.4). Select **Activate**. The policy will be pushed to the vSmart controllers and the status will indicate success.

Process

Configuring an application-aware routing policy

1. Create lists
2. Create the application-aware routing policy
3. Apply the policy definition

Application-aware routing policies are configured as part of a centralized policy. It affects traffic on a vEdge router that is flowing from the service (LAN) side to the transport tunnel (WAN) side. Traffic is matched and placed into an SLA class, with certain loss, jitter, and delay values. The routing behavior is as follows:

- Traffic will be load-balanced across all tunnels meeting the SLA class. If no tunnels meet the SLA, the traffic is sent through any available tunnel.
- If preferred colors are specified in the policy, then traffic will be sent through the preferred color tunnels as long as the SLA is met. If no tunnels meet the SLA, the traffic is sent through any available tunnel.
- If a backup-SLA preferred color is specified, then that tunnel is used when there are no paths that meet the SLA. Another path is used if the backup tunnel is unavailable.
- A strict keyword can be used in the policy, which means if no tunnel can meet the SLA, the traffic is dropped.
- The policy can be configured with no default action, meaning, if traffic does not match any sequence in the list, it is routed normally according to the routing protocol. Alternatively, this default traffic can be placed into an SLA class.

There are three main steps to creating an application-aware routing policy:

- Create any lists.
  - Create SLA class lists, which include the name of the SLA class, and any performance characteristics, like latency, loss, and jitter. Four SLA classes are supported.
  - Create any application lists for traffic to match on and to assign an SLA class to. This allows you to group applications so you can reference the group as a whole.
  - Create any site lists, VPN lists, or data prefix lists as needed. The routing policy gets applied to a site list and VPN list. Data prefixes can be used for matching traffic within the policy.
- Create the application-aware routing policy, which consists of matching traffic that gets placed into a specific SLA class.
- Apply the policy definition to a site list and vpn-list.

An example policy is configured in the following steps:

Procedure 1 Create lists

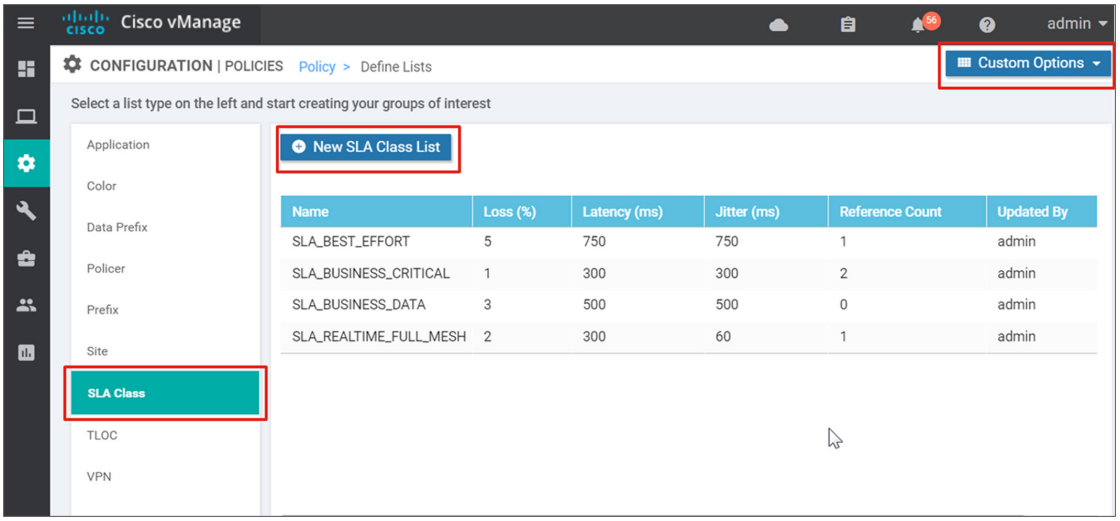
Once a centralized policy is created, it is not possible to build lists by editing the policy - you can only create policy definitions and apply them through the centralized policy configuration. You need to select **Custom Options** on the main policy page in order to modify or create lists.

Step 1: In the vManage GUI, go to **Configurations>Policies**. Select **Custom Options** in the top right corner of the page and select **Lists**.

Step 2: Select **SLA Class** on the left side, and select **New SLA Class List**. Type in the **SLA Class List Name**, the **Loss (%)**, the **Latency (ms)**, and **jitter (ms)**. Select **Add** and repeat for all of the SLA classes. Use the following settings:

Table 66. Application-aware routing policy SLA class list (example)

SLA class list name	Loss (%)	Latency (ms)	Jitter (ms)
SLA_BEST_EFFORT	5	750	750
SLA_BUSINESS_CRITICAL	1	300	300
SLA_BUSINESS_DATA	3	500	500
SLA_REALTIME	2	300	60



Step 3: Select **Application** on the left side, and select **New Application List**.

Step 4: Type in the **Application List Name**, and select several applications as part of the list. The application drop-down box allows you to enter keywords to search on various applications. Note that most of the applications are not abbreviated, meaning, SSH shows up as Secure Shell, so adjust the keyword search appropriately. Select **Add** and repeat for any additional application lists. Use the following example settings:

Table 67. Application-aware routing policy applications list (example)

Application list name	Application
APPS_SCAVENGER	apple_music, apple_update, facebook_messenger, facebook_video, facebook_mail, facebook_live, facebook_apps, facebook, twitter, instagram, youtube, youtube_hd, snapchat,
APPS_NETWORK_CONTROL	ntp, radius, ssh, tacacs_plus, telnet, telnets, xmlrpc

Step 5: Create a data prefix list to use within the application-aware route policy. Select **Data Prefix**, then select **New Data Prefix List**.

Step 6: Type the **Data Prefix List Name** (**MGT_Servers**), then in the **Add Data Prefix** text box, type in the data prefix list (**10.4.48.10/32,10.4.48.13/32,10.4.48.15/32,10.4.48.17/32**).

Step 7: Select **Add**.

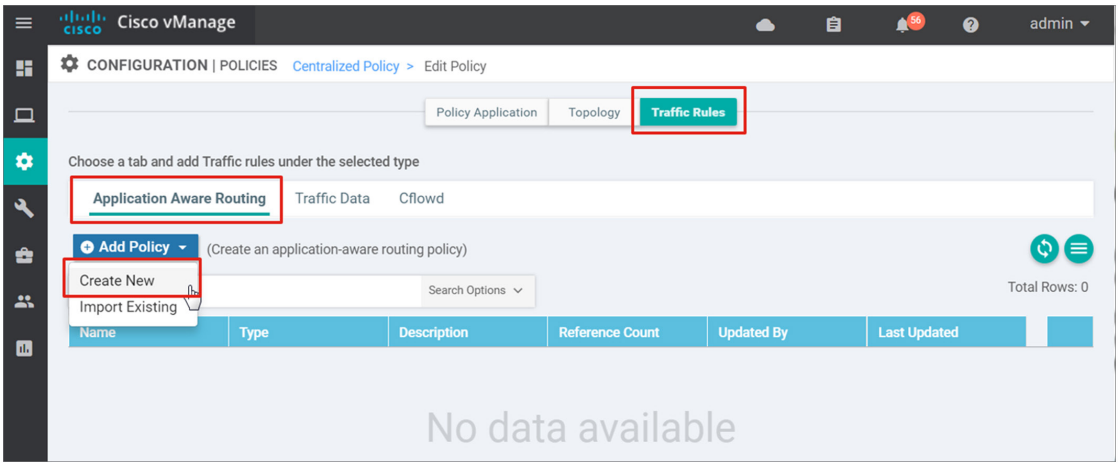
Procedure 2 Create the application-aware routing policy

Step 1: Go to **Configuration>Policies**, and ensure the **Centralized Policy** tab is selected.

Step 2: Next to the centralized policy that was created previously (**Global_Policy**), select **...** to the right of the page and select **Edit** from the drop-down menu.

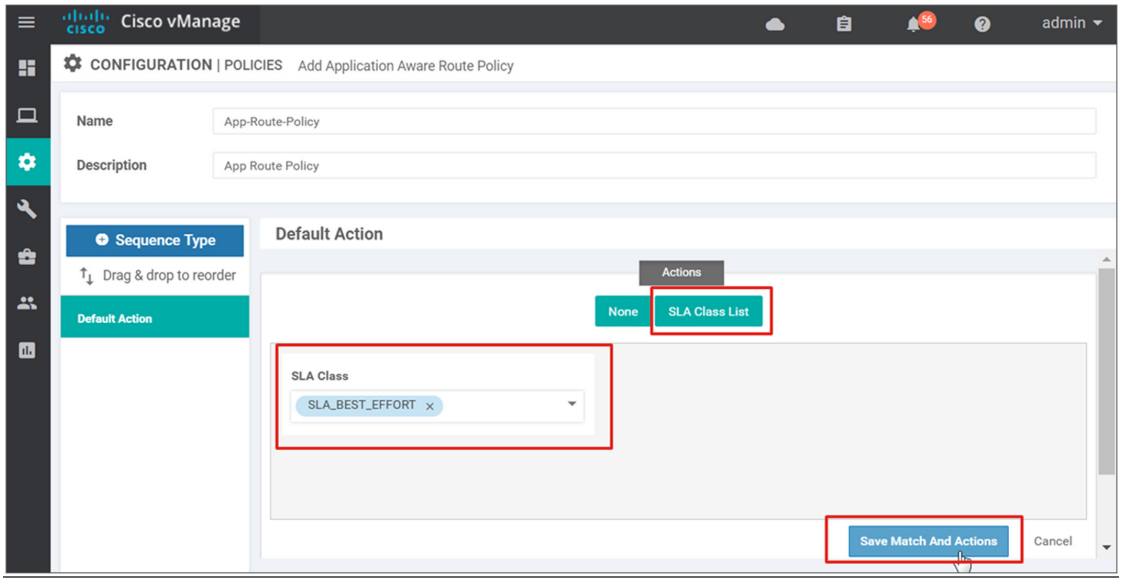
Step 3: The application-aware policy is part of data policy, listed under **Traffic Rules**. Select the **Traffic Rules** box at the top of the page to create a new application-aware policy inside the centralized policy. **Application Aware Routing** is the default tab on this page.

Step 4: Select **Add Policy** and select **Create New**.



Step 5: Type a **Name** (**App-Route-Policy**) and **Description** (**App Route Policy**) for the policy definition.

Step 6: Under Default Action, select the Edit symbol. None is the default. Select the **SLA Class List** box, and under the **SLA Class** text box, select **SLA_BEST_EFFORT** from the drop-down menu. Select **Save Match And Actions**.

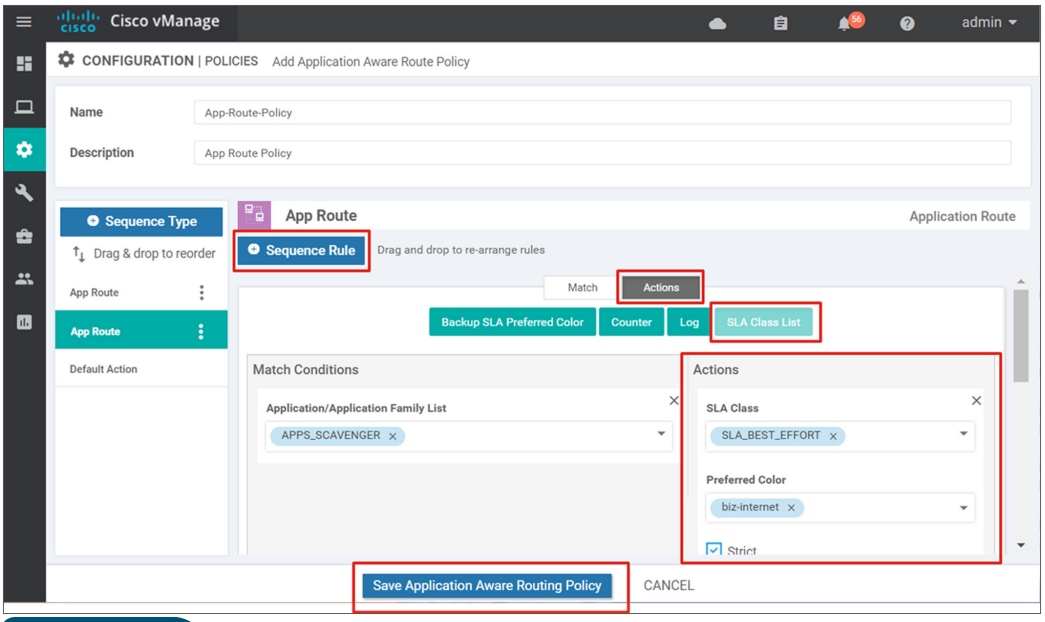


Step 7: Select **Sequence Type** on the left side, then select **Sequence Rule**.

Step 8: Select the **Match** conditions, then select the **Actions** box and select the actions. Select **Save Match and Actions**. To add another sequence, select **Sequence Rule** and repeat. When finished, **Select Save Application Aware Routing Policy** at the bottom of the page. Use the following example match/action options:

Table 68. Application-aware routing policy App Route Policy (example)

Match	Actions
Applications/Application Family List: APPS_SCAVENGER	SLA CLASS: SLA_BEST_EFFORT Preferred Color: biz-internet Strict
DSCP: 46	SLA CLASS: SLA_REALTIME Preferred Color: mpls
Destination Data Prefix: MGT_Servers	SLA Class: SLA_BUSINESS_CRITICAL
Applications/Application Family List: APPS_NETWORK_CONTROL	SLA Class: SLA_BUSINESS_CRITICAL
DSCP: 10 12 14 18 20 22 26 28 30 34 36 38	SLA Class: SLA_BUSINESS_CRITICAL
DSCP: 8 16 24 32 40 48 56	SLA Class: SLA_BUSINESS_DATA
DSCP: 0	SLA Class: SLA_BEST_EFFORT Preferred Color: biz-internet

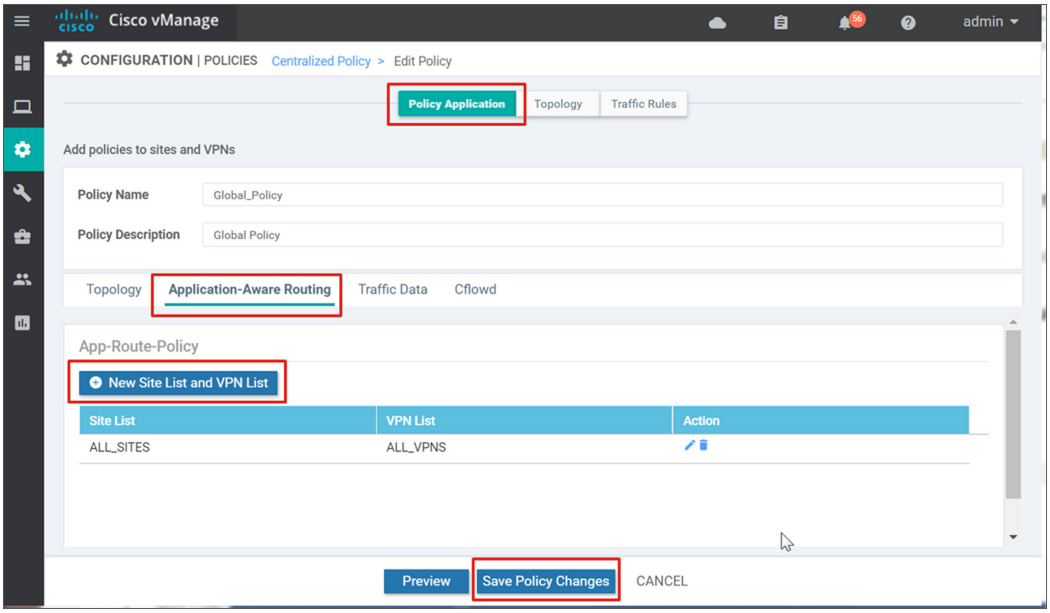


Procedure 3 Apply the policy definition

Step 9: Now that the app-route policy definition is created, select the **Policy Application** box at the top of the page.

Step 10: Select the **Application-Aware Routing** tab. Select **New Site List and VPN List** under the policy definition just created.

Step 11: Select the **Site List** (**ALL_SITES**), and select the **VPN List** (**ALL_VPNS**), and select **Add**.



Step 12: Select **Save Policy Changes**.

Step 13: A pop-up window states that the policy will be applied to the reachable vSmart controllers. Select **Activate**. The policy is downloaded to the vSmart controllers.

Process

Configuring symmetric traffic for DPI

1. Influence traffic from LAN to WAN
2. Influence traffic from WAN to LAN over the overlay

DPI is used in the example app-route policy to classify some applications and put them into different SLA classes. In order for DPI on a vEdge router to be able to classify most application traffic, it is important that the vEdge router sees network traffic in both directions. To ensure symmetry at dual vEdge router sites, traffic should prefer one router in both directions, from the LAN to the WAN and from the WAN to the LAN over the overlay.

In the following example, in the LAN-to-WAN direction, traffic will be influenced:

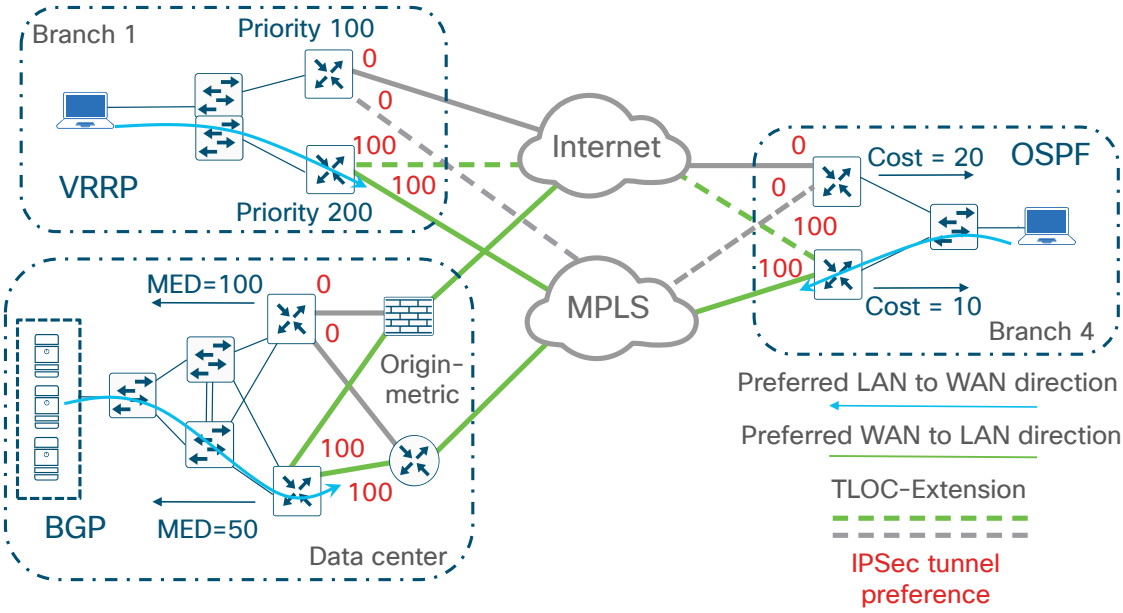
- With VRRP, by setting VRRP priority
- With OSPF, by creating a route policy that modifies the metric of routes distributed from OMP to OSPF
- With BGP, by creating a route policy that modifies the MED (metric) of routes distributed from OMP to BGP.

In the WAN-to-LAN direction, traffic will be influenced:

- With IPSec tunnel preference

vEdge 1 of each dual-vEdge router site will be picked as the primary vEdge router for traffic.

Figure 19. Configuring symmetric traffic



Procedure 1 Influence traffic from LAN to WAN

How traffic is influenced in the LAN-to-WAN direction depends on what protocol is running at the local site. Following is an explanation of how to influence traffic using VRRP, OSPF, and BGP.

VRRP

VRRP was already configured on the vEdge routers at branch 1 to prefer BR1-VE1 when the VRRP priority was set to 200 on BR1-VE1 and the VRRP priority was set to 100 on BR1-VE2.

OSPF

For OSPF, create a route policy that modifies the metric of routes redistributed from OMP to OSPF.

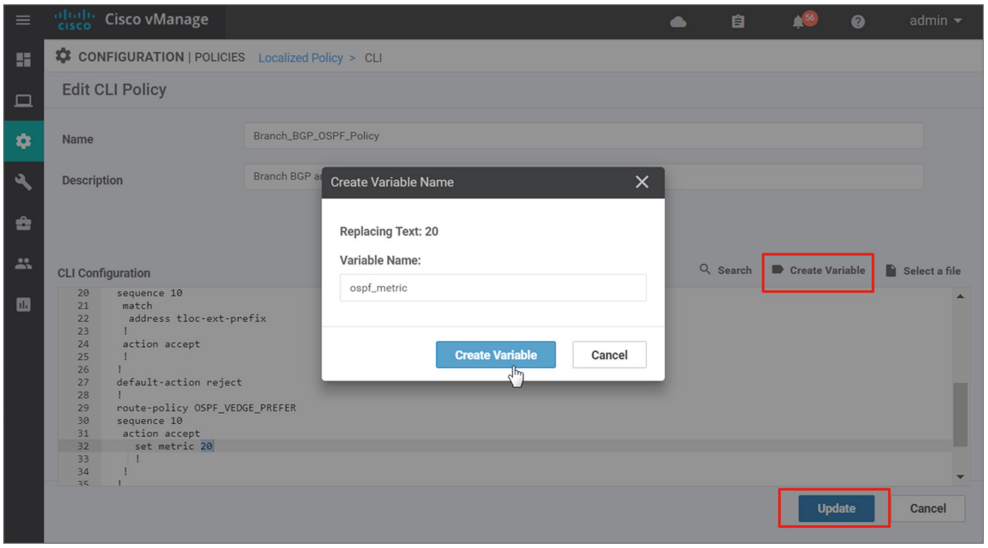
Step 1: Go to **Configuration>Policies** and select the **Localized Policy** tab.

Step 2: Edit the **Branch_BGP_OSPF_Policy**. Select **...** to the far right of the desired policy and select **Edit**.

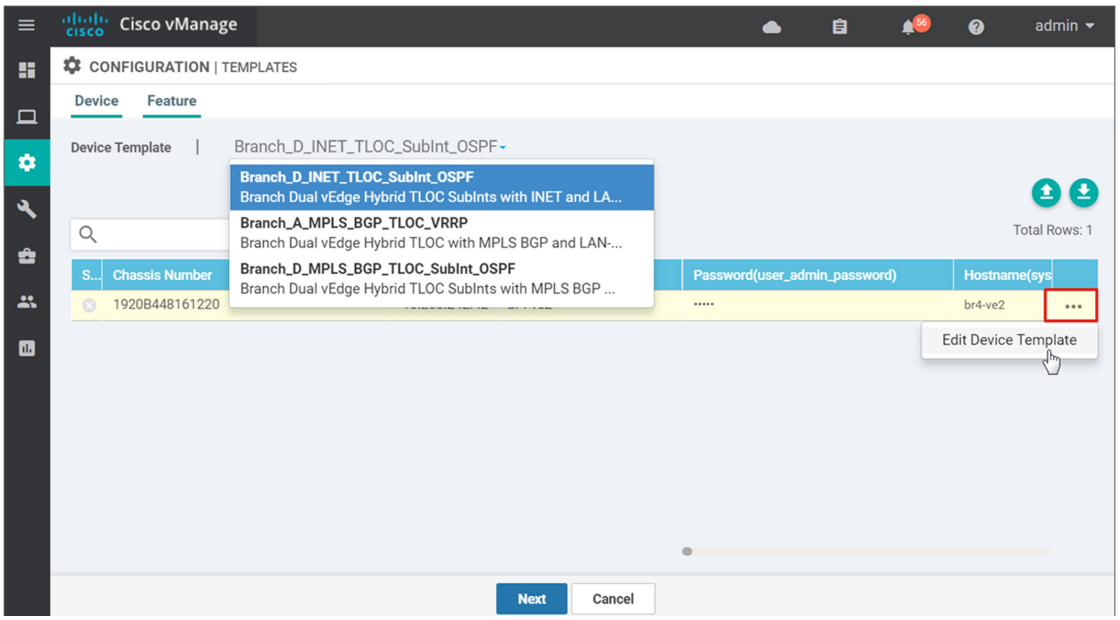
Step 3: Add the following route policy to the existing one:

```
route-policy OSPF_VEDGE_PREFER
 sequence 10
  action accept
    set metric 20
    !
  !
 !
 default-action reject
!
!
```

Step 4: Highlight the **20** in the **set metric** line of the policy and select **Create Variable**. Type **ospf_metric** into the text box. Select **Update** to save the policy configuration.



Step 5: Before the updated policy is pushed out to the vEdge routers, the variable value **ospf_metric** first needs to be defined for all vEdge routers that are attached to the policy. All three device templates are listed in a drop-down box in the top left of the GUI. When you select a device template, all vEdge routers that are attached to the device template appear on the main screen. Next to each vEdge router, select **...** to the right and select **Edit Device Template**.



Step 6: Fill in the necessary values. Then, select **Update** and repeat for the remaining device templates. Use the following values. The primary routers should get a lower metric (10), while the secondary routers get a higher metric (20). Note that any value could be supplied for BR1-VE1 because the OSPF route policy is not used in any feature templates for that device. To limit the number of policies, we chose to consolidate the BGP and OSPF route policies in one localized policy.

Table 69. Ospf_metric values

Device template	Device	ospf_metric
Branch_D_INET_TLOC_SubInt_OSPF	BR4-VE2	20
Branch_A_MPLS_BGP_TLOC_VRRP	BR1-VE1	0
Branch_D_MPLS_BGP_TLOC_SubInt_OSPF	BR4-VE1	10

Step 7: Select **Next** and then **Configure Devices.**

Step 8: Confirm configuration on three devices and select OK. The configurations will be pushed out and the screen will indicate success.

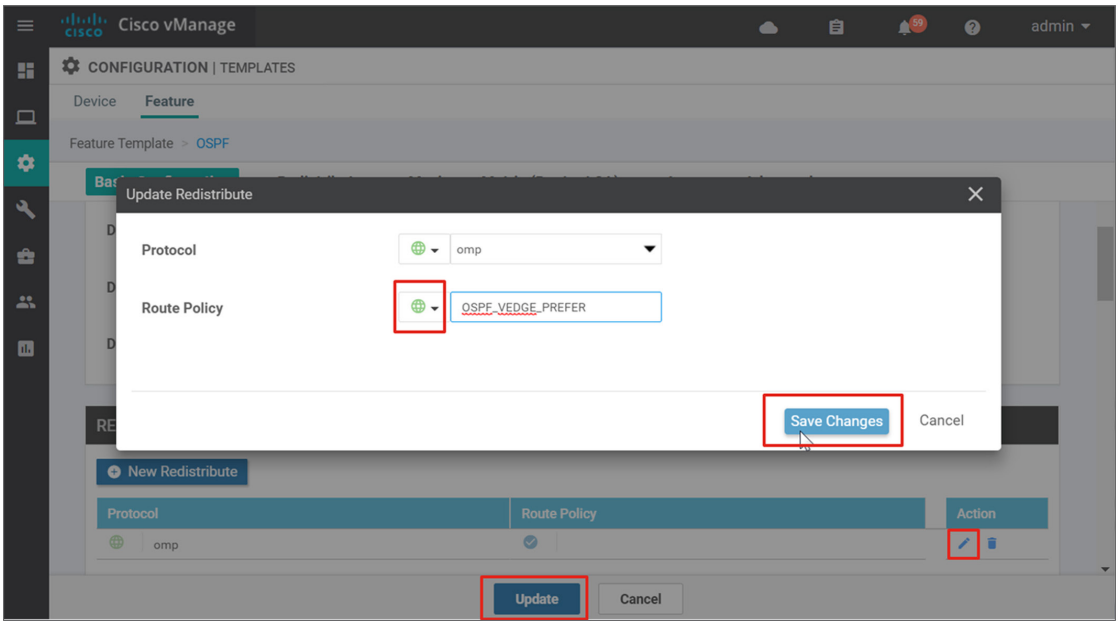
Step 9: Once the policy has been updated, the route policy can be referenced in the feature template. Go to **Configuration>Templates** and select the **Feature** tab.

Step 10: Edit the **BR_VPN1_OSPF** feature template

Step 11: Under the **Redistribute** section, select the **Edit** symbol next to the OMP protocol.

Step 12: Next to **Route Policy**, select **Global** and type in the route policy just added, **OSPF_VEDGE_PREFER**. Select **Save Changes**.

Step 13: Select **Update** to save the feature template configuration.



Step 14: Select **Next**, then **Configure Devices**. Confirm configuration changes on two devices, and then select OK. The configurations are pushed out and the screen will indicate success.

BGP

For BGP, create a route policy that sets MED (metric) on routes redistributed from OMP to BGP.

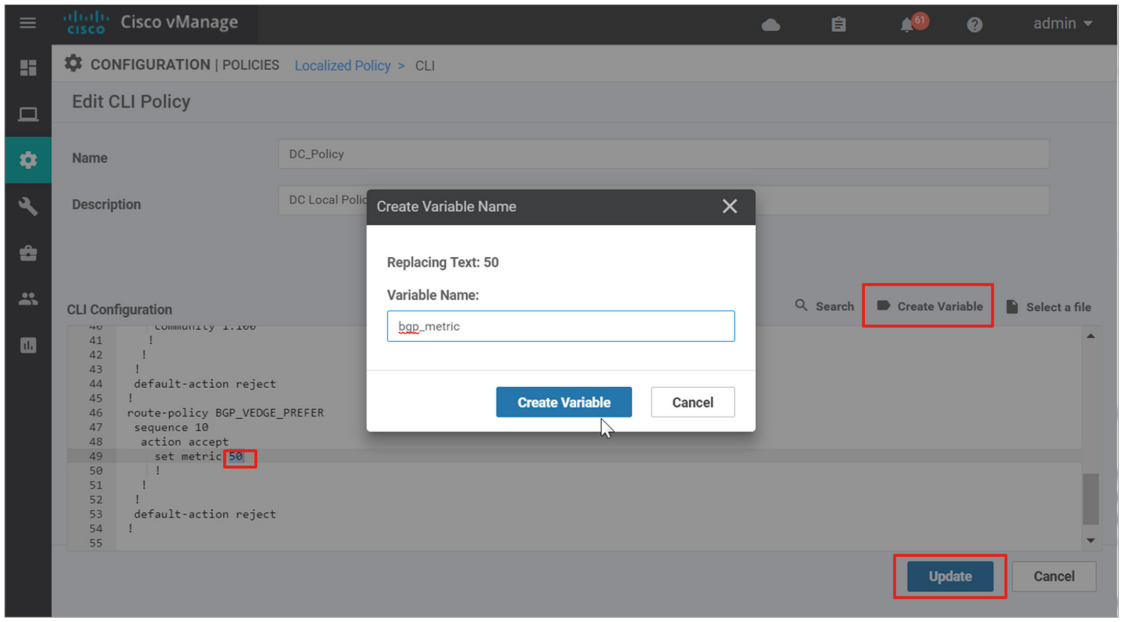
Step 1: Go to **Configuration>Policies** and select the **Localized Policy** tab.

Step 2: Edit the **DC_Policy**. Select … to the far right of the desired policy and select **Edit.**

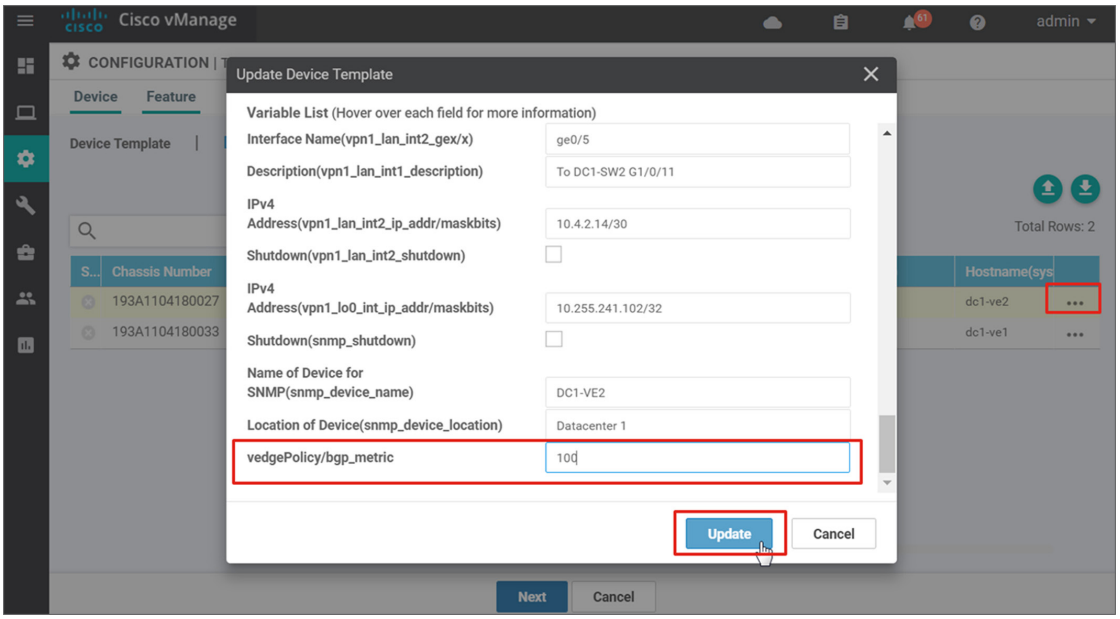
Step 3: Add the following route policy to the current policy:

```
route-policy BGP_VEDGE_PREFER
 sequence 10
  action accept
    set metric 50
    !
  !
 !
 default-action reject
!
```

Step 4: Highlight the **50** in the policy and select **Create Variable**. Type **bgp_metric** into the text box. Select **Update** to save the policy configuration.



Step 5: Before the updated policy is pushed out to the vEdge routers, the variable value first needs to be defined for all vEdge routers that are attached to the policy. There are two devices attached to the device template the policy is applied to. Select **...** to the right of one of the devices, dc1-ve2, and select **Edit Device Template**. Dc1-ve2 is the secondary vEdge so set this metric to **100.** Select **Update.**



Step 6: Select **...** to the right of the other vEdge device, dc1-ve1, and select **Edit Device Template**. Dc1-ve1 is the primary vEdge so set this metric to **50**.

Step 7: Select **Next** and then **Configure Devices**

Step 8: Confirm configuration on three devices and select **OK**. The configurations will be pushed out and the screen will indicate success.

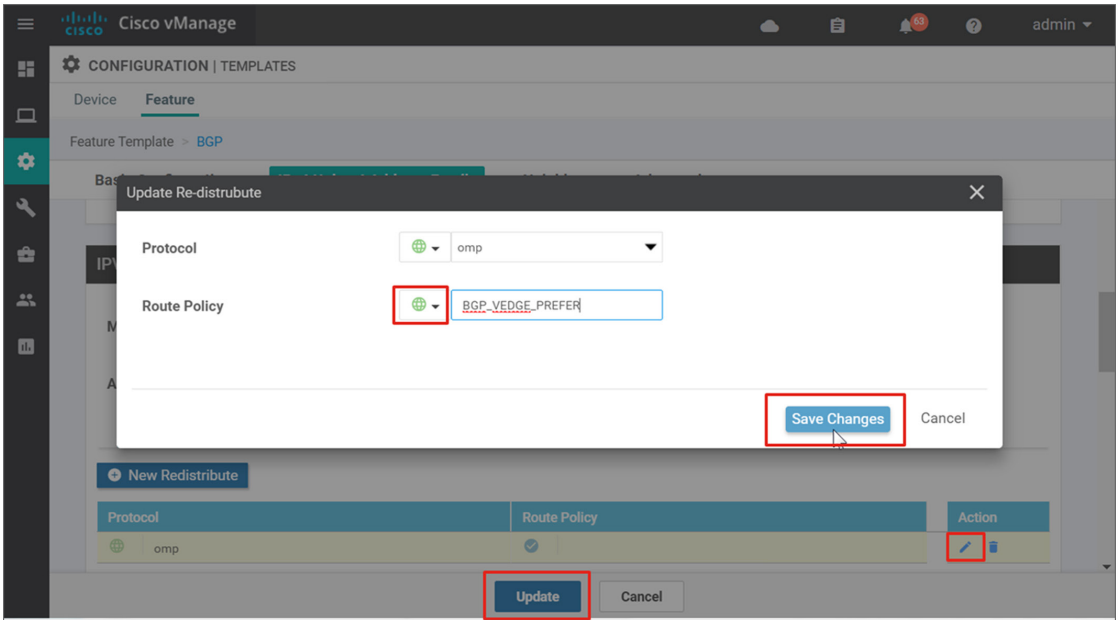
Step 9: Once the policy has been updated, the route policy can be referenced in the feature template. Go to **Configuration>Templates** and select the **Feature** tab.

Step 10: Edit the **DC_VPN1_BGP** feature template.

Step 11: Under the **Redistribute** section, select the **Edit** symbol next to the OMP protocol.

Step 12: Next to **Route Policy**, select **Global** and type in the route policy just added, **BGP_VEDGE_PREFER**. Select **Save Changes**.

Step 13: Select **Update** to save the feature template configuration.



Step 14: Select **Next**, then **Configure Devices**. Confirm configuration changes on two devices, and then select **OK**. The configurations are pushed out and the screen will indicate success.

Procedure 2 Influence traffic from WAN to LAN over the overlay

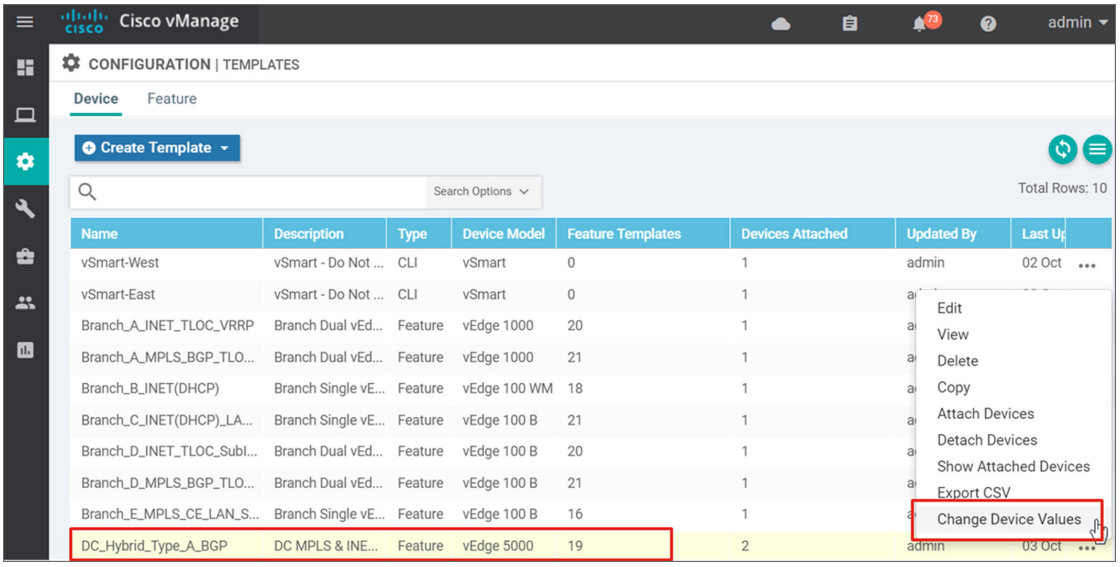
IPSec tunnel preference

There are different ways to influence traffic in the WAN-to-LAN direction over the overlay, but one of the most straightforward ways is through IPSec tunnel preference. This parameter is contained within the Tunnel section of the MPLS and Internet VPN Interface Ethernet templates, and a variable was already created for it when the feature templates were created. Initially, the tunnel preference for all tunnels was set to 0. Change the preference to prefer vEdge 1 over vEdge 2 at the dual-vEdge sites by changing the IPSec tunnel preference of the primary vEdge to 100. Only three device templates need to be modified:

- **DC_Hybrid_Type_A_BGP**
- **BR1-VE1: Branch_A_MPLS_BGP_TLOC_VRRP**
- **BR4-VE1: Branch_D_MPLS_BGP_TLOC_SubInt_OSPF**

Step 1: Go to **Configuration>Templates** and ensure the **Device** tab is selected.

Step 2: Go to the right of the **DC_Hybrid_Type_A_BGP** device template, select **...** and select **Change Device Values** from the drop-down menu.



Step 3: To the right of dc1-ve1, select **...** and select **Edit Device Template**. Next to **vpn0_mpls_tunnel_ipsec_pref** and **vpn0_inet_tunnel_ipsec_pref**, type **100**. DC1-VE2 values are already set to 0 so they do not need to be modified. Select **Update**.

Step 4: Select **Next**, then **Configure Devices**. A pop-up window asks you to confirm configuration changes on two devices. Select the check box and select **OK**. The updated configurations are pushed to the vEdge devices and should indicate success.

Step 5: Repeat steps 1-5 for the device templates, **Branch_A_INET_TLOC_VRRP** and **Branch_D_MPLS_BGP_TLOC_SubInt_OSPF**. Change the tunnel IPSec preference values of **vpn0_mpls_tunnel_ipsec_pref** and **vpn0_inet_tunnel_ipsec_pref** to 100 for BR1-VE1 and BR4-VE1.

Process

Configuring quality of service

1. Configure localized policy
2. Define QoS classification access list
3. Update feature templates

Following is an example of configuring a six-class QoS model. The access list that matches traffic is configured as a centralized data policy instead of a localized policy. The access list shows a variety of ways traffic can be classified. An example of a re-write policy is also given, which re-marks the DSCP in the outer tunnel header policy to support a smaller-class QoS model for the service provider.

The following classes are used in this example:

Table 70. Class of service used for example QoS policy

Class name	Traffic type	DSCP values
VOICE	Voice traffic	ef (46)
INTERACTIVE-VIDEO	Interactive video (video conferencing)	af41, af42 ,af43 (34, 36, 38)
BULK	Bulk data (FTP, email, back-ups)	af11, af12, af13 (10, 12, 14)
CONTROL-SIGNALING	Routing and voice and video call signaling	cs6 (48), cs3 (24)
CRITICAL-DATA	Network management, transactional, streaming video, mission-critical	cs2, cs4, cs5, af21, af22, af23, af31, af32, af33 (16, 32, 40, 18, 20, 22, 26, 28, 30)
CLASS-DEFAULT	Best effort	All others

The following table illustrates the bandwidth percentage and buffer percentage, the congestion avoidance algorithm, and the outer-tunnel DSCP values for each forwarding class:

Table 71. Bandwidth, congestion avoidance, and tunnel DSCP values

Class of service	Bandwidth (scheduling)	Congestion avoidance	Tunnel DSCP values for re-write policy
VOICE	10 (priority queuing)	---	ef (46)
INTERACTIVE-VIDEO	20 (WRR)	RED	af41 (34)
BULK	10 (WRR)	RED	af11 (10)
CONTROL-SIGNALING	10 (WRR)	---	af21 (18)
CRITICAL-DATA	30 (WRR)	RED	af21 (18)
CLASS-DEFAULT	20 (WRR)	RED	default (0)

Following are the steps needed in order to configure Quality of Service (QoS):

1. Map each QoS forwarding class to an output queue (localized policy).
2. Configure the QoS scheduler, which assigns the scheduling method, bandwidth percentage, buffer percentage, and drop algorithm for each forwarding class (localized policy).
3. Create a QoS map, where all of the QoS schedulers are grouped (localized policy).
4. Create a re-write policy (optional) (localized policy).
5. Define an access list to match traffic and assign to forwarding classes (centralized or localized policy).
6. Apply the classification access list to an interface (configured in the VPN Interface Ethernet template in localized policy or configured in centralized policy).
7. Apply the QoS map and, optionally, the re-write policy, to an egress interface (configured in the VPN Interface Ethernet template).

Procedure 1 Configure localized policy

Step 1: Go to **Configuration>Policies** and select the **Localized Policy** tab.

Step 2: To the right of **Branch_Policy**, select **...** and select **Edit**.

Step 3: Map the QoS classes to output queues by configuring or copying the following into the localized policy already created:

```
class-map
  class BULK queue 2
  class CLASS-DEFAULT queue 3
  class CONTROL-SIGNALING queue 5
  class CRITICAL-DATA queue 1
  class INTERACTIVE-VIDEO queue 4
  class VOICE queue 0
!
```

Step 4: Configure the QoS scheduler for each class by configuring or copying the following into the localized policy:

```
!
 qos-scheduler QOS-BULK-DATA
  class             BULK
  bandwidth-percent 10
  buffer-percent    10
  drops             red-drop
 !
 qos-scheduler QOS-CLASS-DEFAULT
  class             CLASS-DEFAULT
  bandwidth-percent 20
  buffer-percent    20
  drops             red-drop
 !
 qos-scheduler QOS-CONTROL-SIGNALING
  class             CONTROL-SIGNALING
  bandwidth-percent 10
  buffer-percent    10
 !
 qos-scheduler QOS-CRITICAL-DATA
  class             CRITICAL-DATA
  bandwidth-percent 30
  buffer-percent    30
  drops             red-drop
 !
 qos-scheduler QOS-INTERACTIVE-VIDEO
  class             INTERACTIVE-VIDEO
  bandwidth-percent 20
  buffer-percent    20
  drops             red-drop
 !
```

```
qos-scheduler QOS-VOICE
 class             VOICE
 bandwidth-percent 10
 buffer-percent    10
 scheduling        llq
!
```

Step 5: Configure the QoS map in order to group the QoS schedulers by configuring or copying the following into the localized policy:

```
qos-map QOS
  qos-scheduler QOS-VOICE
  qos-scheduler QOS-CRITICAL-DATA
  qos-scheduler QOS-BULK-DATA
  qos-scheduler QOS-CLASS-DEFAULT
  qos-scheduler QOS-INTERACTIVE-VIDEO
  qos-scheduler QOS-CONTROL-SIGNALING
!
```

Tech tip

For vEdge cloud and vEdge 5000 routers, to enable QoS scheduling and shaping for the transport-side tunnel interfaces, you must use the **cloud-qos** command in the policy. In addition, to enable QoS scheduling and shaping for the service-side interfaces, you must use the **cloud-qos-service-side** command in the policy.

Step 6: (optional) Create a re-write policy to modify the tunnel outer DSCP values by configuring or copying the following into the localized policy:

```
!
 rewrite-rule QOS-REWRITE
  class BULK low dscp 10
  class BULK high dscp 10
  class CLASS-DEFAULT low dscp 0
  class CLASS-DEFAULT high dscp 0
  class CONTROL-SIGNALING low dscp 18
  class CONTROL-SIGNALING high dscp 18
  class CRITICAL-DATA low dscp 18
  class CRITICAL-DATA high dscp 18
  class INTERACTIVE-VIDEO low dscp 34
  class INTERACTIVE-VIDEO high dscp 34
!
```

Step 7: Select **Update**, then **Next**, and then **Configure Devices**. Confirm the changes to the configuration by selecting the check box and selecting **OK**. The modified localized policy will be downloaded to devices already configured with **Branch_Policy**.

Step 8: Repeat steps 1-7 for the other branch policy, **Branch_BGP_OSPF_Policy** and any additional policies.

Procedure 2 Define QoS classification access list

This example uses a centralized policy to configure the QoS classification access list.

Step 1: Go to **Configuration>Policies** and ensure the **Centralized Policy** tab is selected.

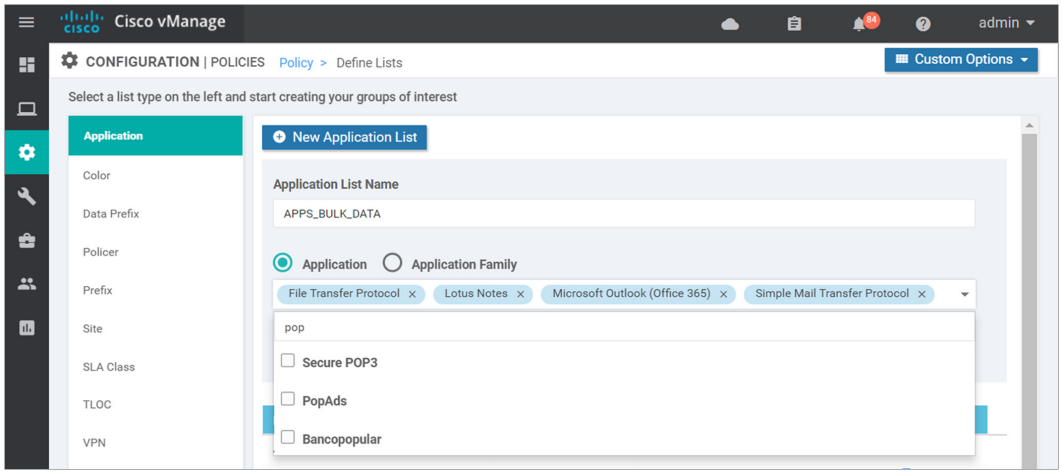
Step 2: Select **Custom Options**, and select **Lists** from the drop-down menu.

Step 3: Select **Application** on the left side, and select **New Application List**.

Step 4: Type in the **Application List Name**, and select several applications as part of the list. The application drop-down box allows you to enter keywords to search on various applications. Note that most of the applications are not abbreviated, meaning SSH shows up as Secure Shell, so adjust the keyword search appropriately. Select **Add** and repeat for any additional application lists. Use the following example settings. Note that the APPS_SCAVENGER list may already be defined, since it was defined under the application-aware routing policy configuration.

Table 72. Quality of service applications list (example)

Application list name	Application
APPS_SCAVENGER	apple_music, apple_update, facebook_messenger, facebook_video, facebook_mail, facebook_live, facebook_apps, facebook, twitter, instagram, youtube, youtube_hd, snapchat
APPS_BULK_DATA	ftp, lotusnotes, outlook, smtp, pop3s, pop3, imap, imaps



Step 5: Select **Data Prefix** on the left-side menu. Ensure that the data prefix list called **MGT_Servers** is configured, which was defined under the application-aware routing policy. If it is present, skip to step 7.

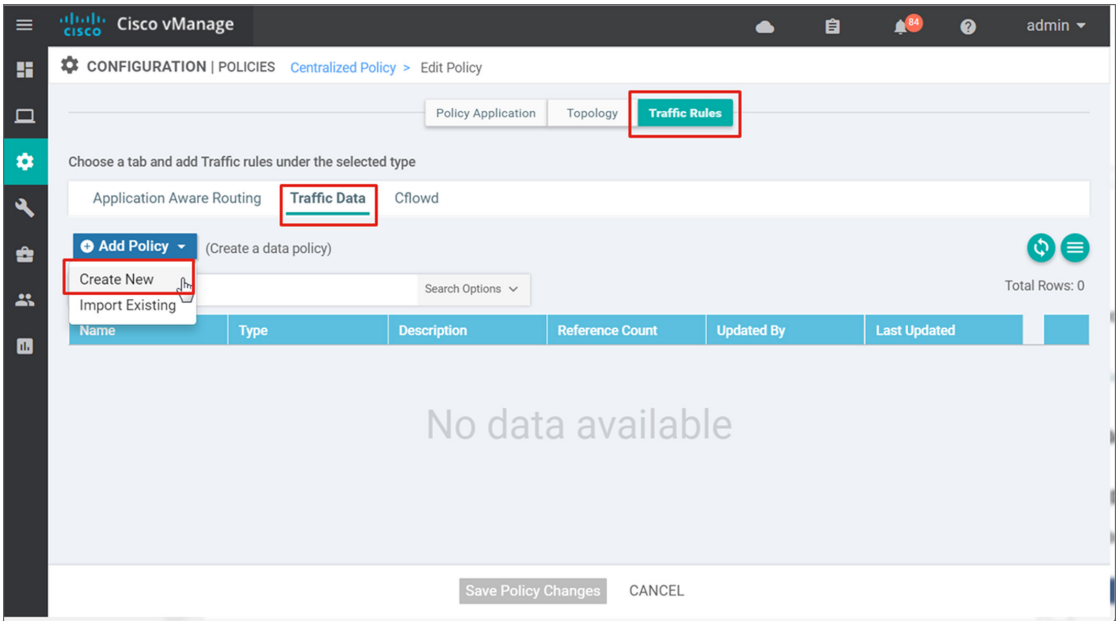
Step 6: If the data prefix list MGT_Servers is not configured, then create a Data Prefix list to use within the QoS policy. Select **New Data Prefix List**. Type the **Data Prefix List Name** (**MGT_Servers**), then in the **Add Data Prefix** text box, type in the data prefix list (**10.4.48.10/32,10.4.48.13/32,10.4.48.15/32,10.4.48.17/32**) and select **Add**.

Step 7: Go to **Configuration>Policies** and ensure the **Centralized Policy** tab is selected.

Step 8: To the right of **Global_policy**, select **...** and select **Edit**.

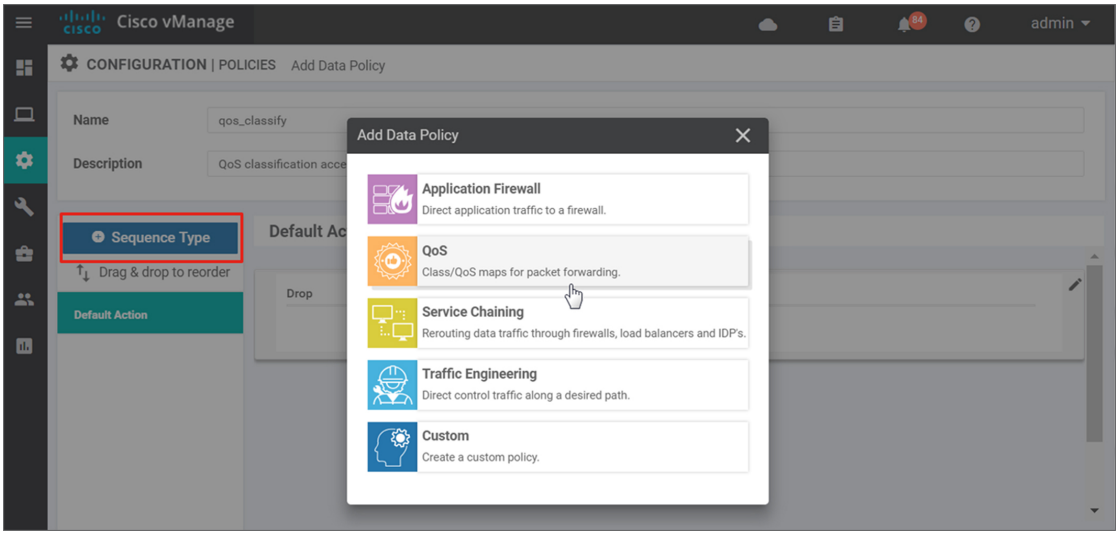
Step 9: Select the **Traffic Rules** box at the top of the page to create a centralized data policy.

Step 10: Select the **Traffic Data** tab. Select **Add Policy** and select **Create New** from the drop-down menu.

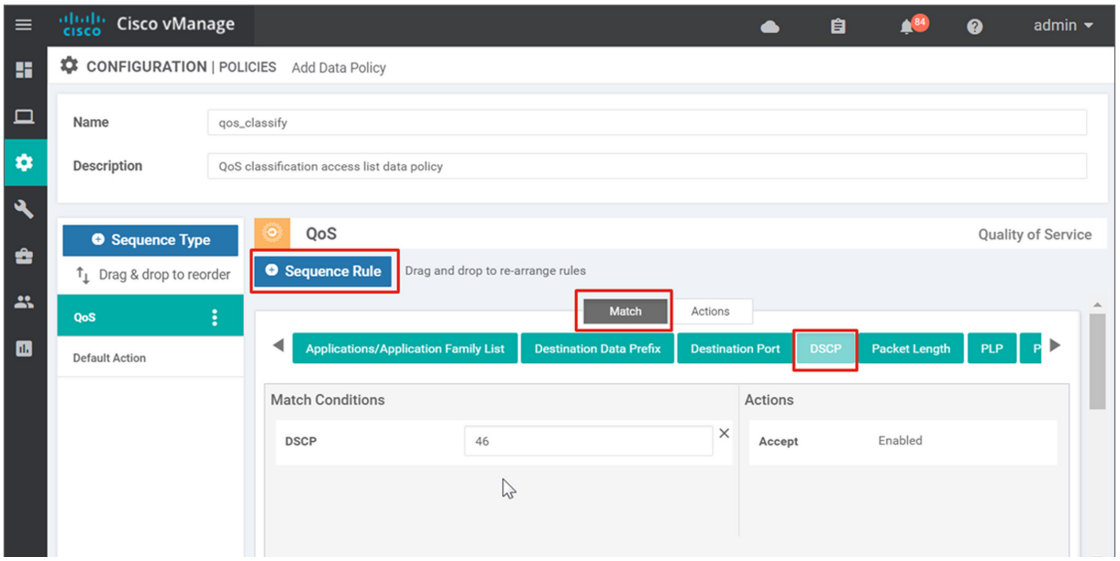


Step 11: Type in the **Name** (**qos_classify**) and **Description** (**QoS classification access list data policy**).

Step 12: Select **Sequence Type**, and select **QoS** from the **Add Data Policy** pop-up window.

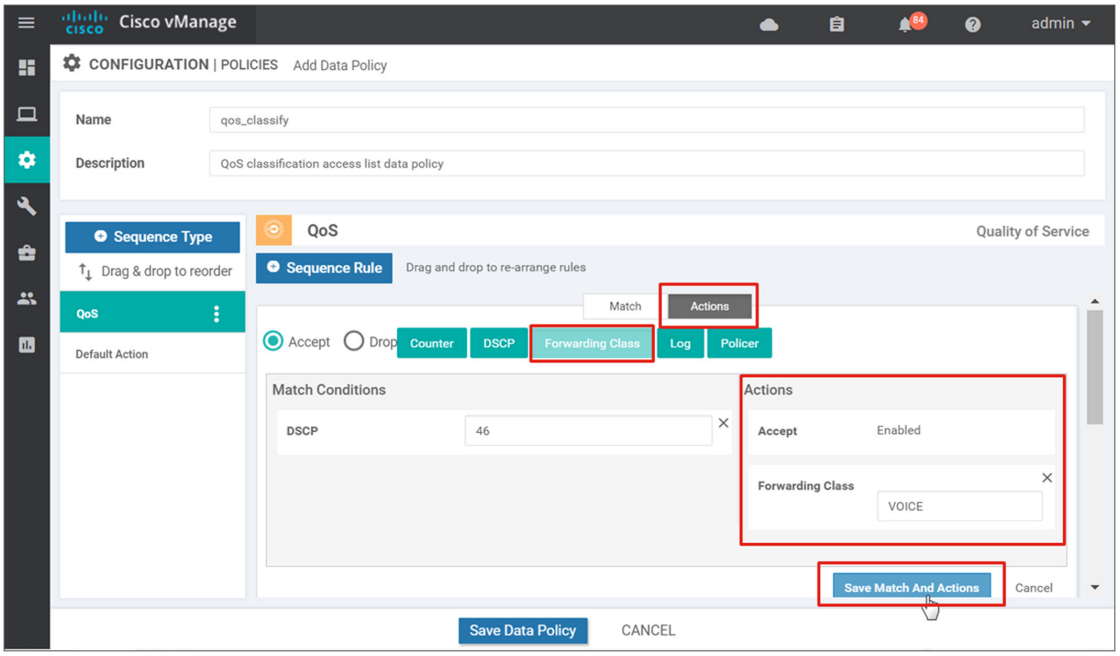


Step 13: Select **Sequence Rule** and select the match conditions (**DSCP 46**).



Step 14: Select the Actions box, select the Accept or Drop radio button (**Accept**), and select an action (**Forwarding Class VOICE**).

Step 15: Select **Save Match and Actions**.



Step 16: Repeat steps 12-15 for the remaining match/action statements:

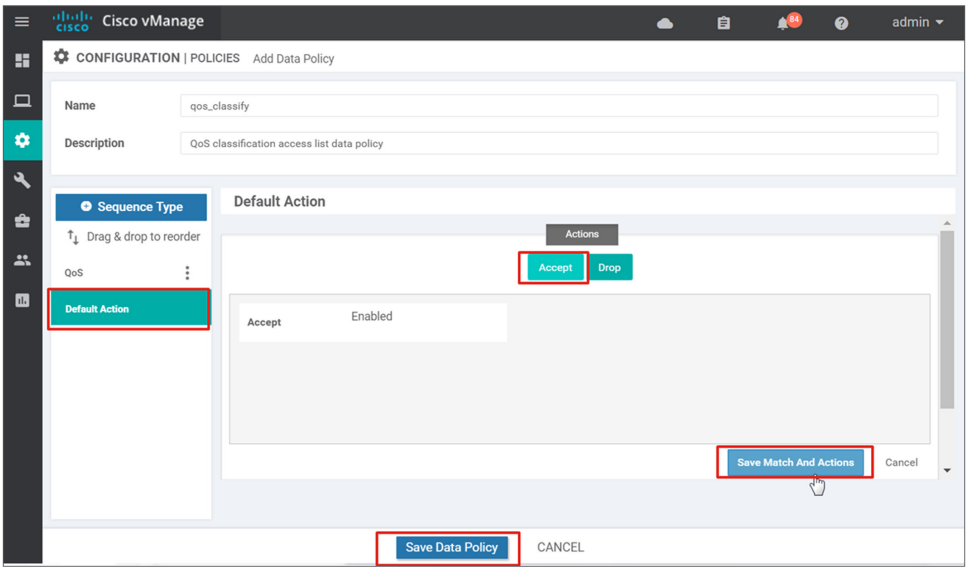
Table 73. QoS classification access list

Match conditions	Accept or drop	Actions
DSCP 46	Accept	Forwarding Class VOICE
DSCP 34 36 38	Accept	Forwarding Class INTERACTIVE-VIDEO
DSCP 10 12 14	Accept	Forwarding Class BULK
Applications/Application Family List APPS_BULK_DATA	Accept	Forwarding Class BULK DSCP 10
DSCP 48 24	Accept	Forwarding Class CONTROL-SIGNALING
Destination Data Prefix MGT_Servers Protocol 17 6	Accept	Forwarding Class CRITICAL-DATA DSCP 16
DSCP 24	Accept	Forwarding Class CONTROL-SIGNALING
Destination Port 11000-11999 1300 1718 1719 1720 5060 5061 Protocol 6	Accept	Forwarding Class CONTROL-SIGNALING DSCP 24
DSCP 16 32 40 18 20 22 26 28 30	Accept	Forwarding Class CRITICAL-DATA
DSCP 8 0	Accept	Forwarding Class CLASS-DEFAULT
Applications/Application Family List APPS_SCAVENGER	Accept	Forwarding Class CLASS-DEFAULT DSCP 0

Step 17: Select **Default Action** on the left side, and select the edit symbol.

Step 18: Select the **Accept** box and select **Save Match and Actions**.

Step 19: Select **Save Data Policy**.



Step 20: You can now apply the policy. Select the **Policy Application** box at the top of the page.

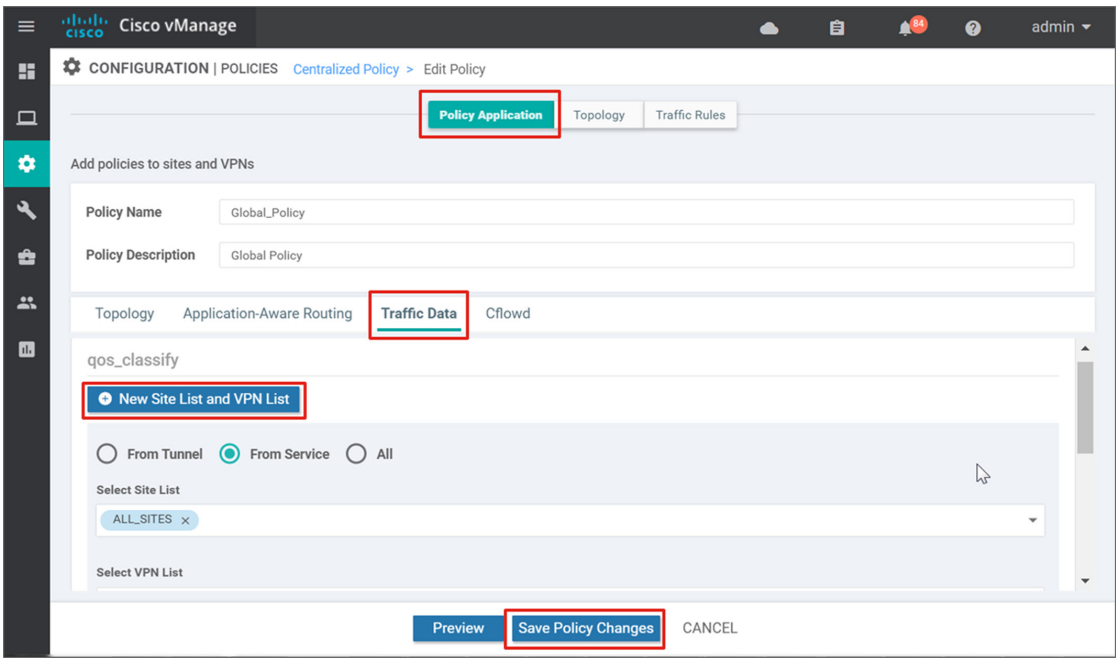
Step 21: Select the **Traffic Data** tab.

Step 22: Under the **qos_classify** policy section, select **New Site List and VPN list**.

Step 23: Select the **From Service** radio button since this is applied incoming on the LAN, or service side.

Step 24: Under the **Select Site List** box, select **ALL_SITES**, and under the **Select VPN List** box, select **ALL_VPNS**. Select **Add**.

Step 25: Select **Save Policy Changes**.



Step 26: A window pops up indicating the policy will be applied to the vSmart controllers. **Select Activate**.

Step 27: vManage pushes the configuration to the vSmart controllers and indicates success.

Procedure 3 Update feature templates

Because centralized policy was used to configure and apply the QoS classification access list, the classification QoS access list does not need to be configured through an interface feature template. The QoS map and re-write policy created, however, needs to be referenced in the VPN Interface feature templates in order to apply them.

The following feature templates need to be modified (assuming only branch templates in this example, and note that QoS is only supported on physical interfaces and not subinterfaces):

- BR_MPLS_INT
- BR_INET_INT_Static
- BR_INET_INT_DHCP

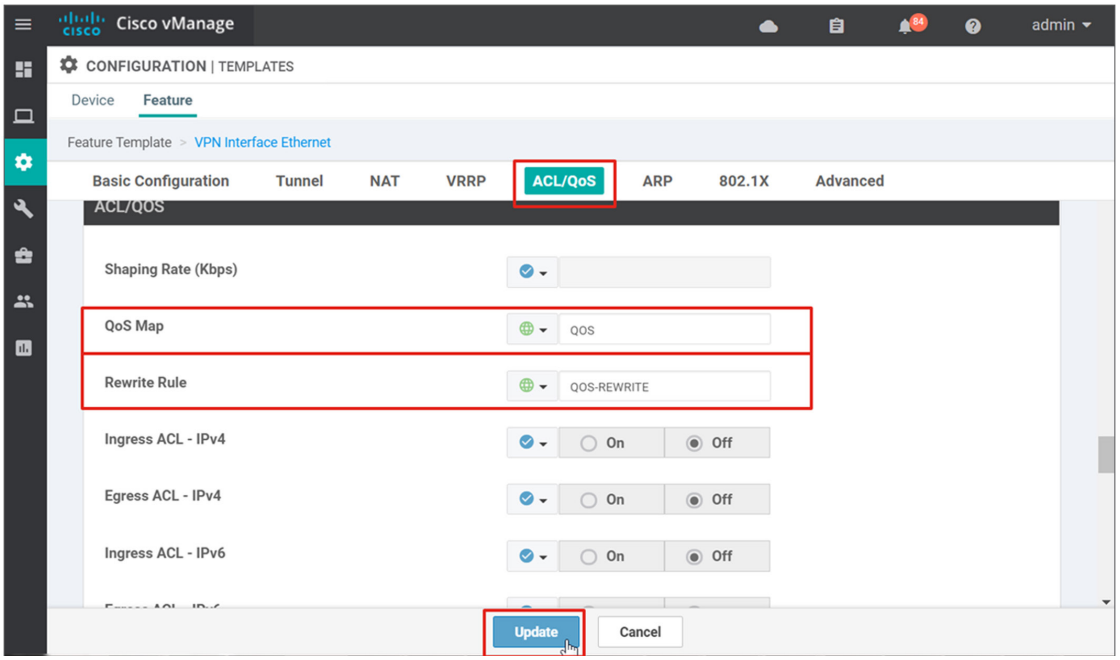
Step 1: Go to **Configuration>Templates** and ensure that the **Feature** tab is selected.

Step 2: Select **...** to the right of the **BR_MPLS_INT** template and select **Edit** from the drop-down menu.

Step 3: Under the **ACL/QOS** section, next to **QoS Map**, select **Global**, and type in **QOS** in the text box. If there will be differing QoS policies according to sites, this setting could be made into a device specific variable instead.

Step 4: Under **Rewrite Rule**, select **Global** and type in **QOS-REWRITE**.

Step 5: Select **Update**.



Step 6: Select **Next** and then select **Configure Devices**. A window pops up that asks you to confirm changes on multiple devices. Select the check box and select **OK**.

Step 7: Repeat steps 1-6 for the remaining two feature templates, **BR_INET_INT** and **BR_INET_INT_DHCP**.

Appendices

Appendix A: Product list

The following products and versions were included as part of the validation in this deployment guide.

Location	Product	Software version
Cloud	Cisco vManage NMS	17.2.7
Cloud	Cisco vSmart Controller	17.2.7
Cloud	Cisco vBond Orchestrator	17.2.7
Data center	Cisco vEdge 5000 Series Routers	17.2.7
Branch	Cisco vEdge 1000 Series Routers	17.2.7
Branch	Cisco vEdge 100 Series Routers	17.2.7

Location	Product	Software version
Data center	Cisco ASR 1002	3.16.7bS
Data center	Cisco Catalyst® 3850 switch	3.6.8E
Data center	ASA 5512	9.4.4(17)
Branch	Catalyst 3850 switch	16.3.6
Branch	Catalyst 2960X switch	15.2(6)E1
Branch	Catalyst 3750E switch	15.0(2)SE11
Branch	Catalyst 3650 switch	3.6.8E
Branch	4321 Integrated Services Router (ISR)/K9	3.16.7bS

Appendix B: Factory default settings

The following text shows how to reset a vEdge router back to factory default settings (typically not needed). A default factory setting configuration of a new vEdge 5000 hardware router that has a network module installed in slot 0 is also shown.

You can reset the configuration to factory defaults by issuing a **request software reset** command. Alternatively, you can go back to the factory-default configuration by pressing the reset button for more than 10 seconds. The router will reboot after you release it. The factory default username/password is admin/admin.

1. Set default software (optional). Before you reset back to factory defaults, you may want to change the default software version if you haven't done so already. The default software version will load, not necessarily the last one you upgraded to, and all other code versions will be deleted. In the CLI, issue a **show software** to see the default version:

```
vedge# show software

VERSION  ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
--------------------------------------------------------------------------
16.3.0  false  true     true      -                2017-10-18T17:21:15
17.2.5   true    false    false     user       2018-05-07T17:16:47
```

Type request **software set-default** [**version**] in executive mode to change the code version and answer **yes** when it asks you if you are sure you want to proceed.

```
vedge# request software set-default 17.2.5
This will change the default software version.
Are you sure you want to proceed? [yes,NO] yes
```

2. To reset the configuration back to factory default, use the **request software reset** command in executive mode and answer **yes** when it asks you if you are sure you want to proceed.

```
vedge# request software reset
Are you sure you want to reset to factory defaults? [yes,NO] yes
```

Verify the code version after the reset with a **show version** command.

```
vedge# show version
17.2.5
```

Following is a default factory setting configuration for a vEdge 5000:

```
system
 host-name               vedge
 admin-tech-on-failure
 no route-consistency-check
 vbond ztp.viptela.com
 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
  !
  usergroup tenantadmin
  !
  user admin
   password [admin password]
  !
 !
 logging
  disk
   enable
  !
 !
!
omp
 no shutdown
 graceful-restart
 advertise connected
 advertise static
!
security
 ipsec
  authentication-type ah-sha1-hmac sha1-hmac
 !
!
vpn 0
 interface ge0/0
```

```
  ip dhcp-client
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   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
  !
  no shutdown
 !
!
vpn 512
 interface mgmt0
  ip address 192.168.1.1/24
  no shutdown
 !
```

Appendix C: Manual upgrade of a vEdge 5000 router

The following text provides an example of an upgrade using an external FTP server from the VPN 512 interface. This process assumes that the VPN 512 interface is configured and contains an interface with an IP address and that the FTP server is reachable through that interface. The code required should be available on the FTP default directory of the server.

In this case, we are loading viptela-17.2.5-x86_64.tar (vEdge 5K software) from the FTP server at 192.168.254.51.

First, verify that the server is reachable:

```
vedge# ping 192.168.254.51 vpn 512
Ping in VPN 512
PING 192.168.254.51 (192.168.254.51) 56(84) bytes of data.
64 bytes from 192.168.254.51: icmp_seq=1 ttl=128 time=9.03 ms
64 bytes from 192.168.254.51: icmp_seq=2 ttl=128 time=0.422 ms
```

Next, install the software. It will be activated with a separate command. Activation will cause the vEdge router to reboot with the selected code version.

vedge# request software install ftp://admin:c1sco123@192.168.254.51/viptela-17.2.5-x86_64.tar.gz vpn 512

```
--2018-07-18 15:57:52--  ftp://admin:*password*@192.168.254.51/viptela-
17.2.5-x86_64.tar.gz
           => 'viptela-17.2.5-x86_64.tar.gz'
Connecting to 192.168.254.51:21... connected.
Logging in as admin ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> SIZE viptela-17.2.5-x86_64.tar.gz ... 216733499
==> PASV ... done.    ==> RETR viptela-17.2.5-x86_64.tar.gz ... done.
Length: 216733499 (207M) (unauthoritative)

100%[===================================>] 216,733,499  101MB/s   in 2.1s

2018-07-18 15:57:54 (101 MB/s) - 'viptela-17.2.5-x86_64.tar.gz' saved
[216733499]

Signature verification Suceeded.
EFI boot loader Secure Boot check Succeeded
Successfully installed version: 17.2.5
```

Now, activate the new software version with the following command and reply with "yes" when it asks if you want to proceed. The vEdge router will then reboot and will boot into the desired software version.

```
vedge# request software activate 17.2.5
This will reboot the node with the activated version.
Are you sure you want to proceed? [yes,NO] yes
vedge# Wed Jul 18 15:58:55 UTC 2018: The system is going down for reboot NOW!
Stopping services...
acpid: exiting
ok: down: acpid: 0s, normally up
ok: down: button: 712s, normally up
ok: down: cloudinit: 651s, normally up
ok: down: ephemeral: 0s, normally up
ok: down: getty-tty1: 0s, normally up
```

When the reboot is complete, the vEdge router will indicate the currently-running software version on the console.

```
Wed Jul 18 16:02:03 UTC 2018: System Ready


viptela 17.2.5


vedge login:
Password:
```

You can also issue a “show version” to view the current software version.

```
vedge# show ver
17.2.5
```

Appendix D: Supporting network device configurations

For convenience, following are portions of the configurations for the supporting network devices in the example network.

Data center CE router:

```
interface GigabitEthernet0/0/2
 description To DC1-VE1
 ip address 10.4.1.1 255.255.255.252
 negotiation auto
interface GigabitEthernet0/1/2
 description TO DC1-VE2
 ip address 10.4.2.1 255.255.255.252
 negotiation auto

router bgp 65111
 bgp router-id 10.255.241.106
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor 10.4.0.13 remote-as 65112
 neighbor 10.4.0.13 description DC1-SW1
 neighbor 10.4.0.13 password cisco123
 neighbor 10.4.0.17 remote-as 65112
 neighbor 10.4.0.17 description DC1-SW2
 neighbor 10.4.0.17 password cisco123
 neighbor 192.168.1.1 remote-as 101
 neighbor 192.168.1.1 description MPLS Provider
 !
```

```
 address-family ipv4
  ! advertise vEdge connected networks for vEdge IPSec tunnel connections and
  ! controller connections to the Internet
  network 10.4.1.0 mask 255.255.255.252
  network 10.4.2.0 mask 255.255.255.252
  ! aggregate and advertise MPLS transport networks for controller
  ! connections to the Internet
  aggregate-address 192.168.0.0 255.255.0.0 summary-only
  neighbor 10.4.0.13 activate
  neighbor 10.4.0.13 send-community
  neighbor 10.4.0.17 activate
  neighbor 10.4.0.17 send-community
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 next-hop-self
  neighbor 192.168.1.1 route-map mark-mpls-routes in
  maximum-paths 2
 exit-address-family
!
route-map mark-mpls-routes permit 10
 set community 101:101
```

DC1-SW1

```
interface Port-channel1
 description To DC1-SW2
 no switchport
 ip address 10.4.0.9 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/1
 description To Core
 no switchport
 ip address 10.4.0.2 255.255.255.252
 ip ospf network point-to-point
!
```

```
interface GigabitEthernet1/0/2
 description To DC1-CE1
 no switchport
 ip address 10.4.0.13 255.255.255.252
!
interface GigabitEthernet1/0/11
 description To DC1-VE1
 no switchport
 ip address 10.4.1.9 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/12
 description To DC1-VE2
 no switchport
 ip address 10.4.2.9 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/23
 no switchport
 no ip address
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
 no switchport
 no ip address
 channel-group 1 mode active
!
router ospf 1
 router-id 10.255.241.103
 auto-cost reference-bandwidth 100000
 redistribute static subnets
 redistribute bgp 65112 metric 10 subnets
 passive-interface default
 no passive-interface GigabitEthernet1/0/1
```

```
 no passive-interface Port-channel1
 network 10.4.0.0 0.0.0.3 area 0
 network 10.4.0.8 0.0.0.3 area 0
 network 10.255.241.103 0.0.0.0 area 0
!
router bgp 65112
 bgp router-id 10.255.241.103
 bgp log-neighbor-changes
 network 0.0.0.0
 network 10.0.0.0
 network 10.4.0.0 mask 255.252.0.0
 timers bgp 3 9
 neighbor 10.4.0.10 remote-as 65112
 neighbor 10.4.0.10 description DC1-SW2
 neighbor 10.4.0.10 password cisco123
 neighbor 10.4.0.10 send-community
 neighbor 10.4.0.14 remote-as 65111
 neighbor 10.4.0.14 description DC1-CE1
 neighbor 10.4.0.14 password cisco123
 neighbor 10.4.0.14 send-community
 neighbor 10.4.1.10 remote-as 65113
 neighbor 10.4.1.10 description DC1-VE1
 neighbor 10.4.1.10 password cisco123
 neighbor 10.4.1.10 next-hop-self
 neighbor 10.4.1.10 send-community
 neighbor 10.4.2.10 remote-as 65113
 neighbor 10.4.2.10 description DC1-VE2
 neighbor 10.4.2.10 password cisco123
 neighbor 10.4.2.10 send-community
 maximum-paths 2
```

DC1-SW2

```
interface Port-channel1
 description To DC1-SW1
 no switchport
 ip address 10.4.0.10 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/1
 description To Core
 no switchport
 ip address 10.4.0.6 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/2
 description To DC1-CE1
 no switchport
 ip address 10.4.0.17 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/0/11
 description To DC1-VE1
 no switchport
 ip address 10.4.1.13 255.255.255.252
!
interface GigabitEthernet1/0/12
 description To DC1-VE2
 no switchport
 ip address 10.4.2.13 255.255.255.252
!
interface GigabitEthernet1/0/23
 no switchport
 no ip address
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
 no switchport
```

```
 no ip address
 channel-group 1 mode active
!
router ospf 1
 router-id 10.255.241.104
 auto-cost reference-bandwidth 100000
 redistribute static subnets
 redistribute bgp 65112 metric 10 subnets
 passive-interface default
 no passive-interface GigabitEthernet1/0/1
 no passive-interface Port-channel1
 network 10.4.0.4 0.0.0.3 area 0
 network 10.4.0.8 0.0.0.3 area 0
 network 10.255.241.104 0.0.0.0 area 0
!
router bgp 65112
 bgp router-id 10.255.241.104
 bgp log-neighbor-changes
 network 0.0.0.0
 network 10.0.0.0
 network 10.4.0.0 mask 255.252.0.0
 timers bgp 3 9
 neighbor 10.4.0.9 remote-as 65112
 neighbor 10.4.0.9 description DC1-SW1
 neighbor 10.4.0.9 password cisco123
 neighbor 10.4.0.9 send-community
 neighbor 10.4.0.18 remote-as 65111
 neighbor 10.4.0.18 description DC1-CE1
 neighbor 10.4.0.18 password cisco123
 neighbor 10.4.0.18 send-community
 neighbor 10.4.1.14 remote-as 65113
 neighbor 10.4.1.14 description DC1-VE1
 neighbor 10.4.1.14 password cisco123
 neighbor 10.4.1.14 next-hop-self
 neighbor 10.4.1.14 send-community
 neighbor 10.4.2.14 remote-as 65113
```

```
 neighbor 10.4.2.14 description DC1-VE2
 neighbor 10.4.2.14 password cisco123
 neighbor 10.4.2.14 next-hop-self
 neighbor 10.4.2.14 send-community
 maximum-paths 2
!
```

Data center firewall (DMZ)

```
interface GigabitEthernet0/2
 nameif outside
 security-level 0
 ip address 64.100.1.2 255.255.255.240
!
interface GigabitEthernet0/3.1
 nameif vedge-1
 security-level 50
 ip address 10.4.1.5 255.255.255.252
!
interface GigabitEthernet0/3.2
 nameif vedge-2
 security-level 50
 ip address 10.4.2.5 255.255.255.252
!
object network ve1
 host 10.4.1.6
object network ve2
 host 10.4.2.6
!
object network ve1
 nat (vedge-1,outside) static 64.100.1.11
object network ve2
 nat (vedge-2,outside) static 64.100.1.12
route outside 0.0.0.0 0.0.0.0 64.100.1.1 1
```

Branch 1 switch stack (br1-sw1)

```
!
vlan 10
 name data
!
vlan 20
 name voice
!
interface TenGigabitEthernet1/0/1
 description To BR1-VE1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 load-interval 30
 spanning-tree portfast trunk
!
interface TenGigabitEthernet2/0/1
 description To BR1-VE2
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 load-interval 30
 spanning-tree portfast trunk
```

Branch 3 switch (br3-sw1)

```
!
vlan 10
 name data
!
vlan 20
 name voice
!
!
interface GigabitEthernet1/0/1
 description To BR3-VE1
 switchport access vlan 10
```

```
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 spanning-tree portfast edge trunk
!
```

Branch 4 switch (br4-sw1)

```
!
interface GigabitEthernet1/0/1
 description To BR4-VE1
 no switchport
 ip address 10.104.0.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 22 md5 cisco123
 ip ospf network point-to-point
 load-interval 30
!
interface GigabitEthernet1/0/2
 description To BR4-VE2
 no switchport
 ip address 10.104.0.5 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 22 md5 cisco123
 ip ospf network point-to-point
 load-interval 30
!
router ospf 1
 router-id 10.255.242.43
 auto-cost reference-bandwidth 100000
 network 10.0.0.0 0.255.255.255 area 0
!
```

Branch 5 switch (br5-sw1)

```
interface GigabitEthernet1/0/2
 description To BR5-VE1
 no switchport
 ip address 10.105.0.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 10.105.0.2
!
```

Branch 5 CE (br5-ce1)

```
!
interface GigabitEthernet0/0/0
 description To Service Provider
 ip address 192.168.105.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
 description To BR5-VE1
 ip address 10.105.1.1 255.255.255.252
 negotiation auto
!
router bgp 65205
 bgp log-neighbor-changes
 network 10.105.1.0 mask 255.255.255.252
 neighbor 192.168.105.1 remote-as 102
 neighbor 192.168.105.1 route-map Deny-All in
!
ip route 0.0.0.0 0.0.0.0 192.168.105.1
!
route-map Deny-All deny 10
!
```

Appendix E: vEdge configuration template summary

For convenience, this section summarizes the vEdge feature templates, device templates, and variable values for the SD-WAN devices in the example network.

Shared feature templates

System feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge5000, vEdge Cloud

Template: System

Template Name: **System_Template**

Description: System Template

Table 74. System feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_hostname
	Device Groups	Device Specific	system_device_groups
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset

Logging feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: Logging

Template Name: **Logging_Template**

Description: Logging Template

Table 75. Logging feature template settings

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	10.4.48.13
	VPN ID	Global	1
	Source Interface	Global	loopback0

NTP feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: NTP

Template Name: **NTP_Template**

Description: NTP Template

Table 76. NTP feature template settings

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	time.nst.gov

AAA feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: AAA

Template Name: **AAA_Template**

Description: AAA Template

Table 77. AAA feature template settings

Section	Parameter	Type	Variable/value
Authentication	Authentication Order	Drop-down	local
Local	User/admin/ Password	Device Specific	user_admin_passwd

OMP feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: OMP

Template Name: **OMP_Template**

Description: OMP Template

Table 78. OMP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Number of Paths Advertised per Prefix	Global	16
	ECMP Limit	Global	16
Advertise	Connected	Global	Off
	Static	Global	Off

BFD feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: BFD

Template Name: **BFD_Template**

Description: BFD Template

Table 79. BFD feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Poll Interval	Global	120000
Color (MPLS)	Color	Drop-down	MPLS
	Path MTU	Global	Off
Color (Biz Internet)	Color	Drop-down	Biz Internet
	Path MTU	Global	Off

Security feature template

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: Security

Template Name: **Security_Template**

Description: Security Template

Table 80. Security feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Replay wIndow	Global/ drop-down	4096

VPN 512

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: VPN

Template Name: **VPN512_Template**

Description: VPN 512 Out-of-Band Management

Table 81. VPN512 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	512
	Name	Global	Management VPN
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn512_mgt_next_hop_ip_addr

VPN 512 interface

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: VPN

Template Name: **VPN512_Interface**

Description: VPN 512 Management Interface

Table 82. VPN512 interface feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgt_int_mgmt0_or_gex/x
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_mgt_next_hop_ip_addr

VPN interface Ethernet Loopback0

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: **VPN Interface Ethernet**

Template Name: **VPN1_Lo0**

Description: Service VPN 1 Interface Loopback 0

Table 83. VPN1 interface Ethernet feature template settings (Loopback 0)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Global	No
	Interface Name	Global	loopback0
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lo0_int_ip_addr/maskbits

Banner

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: Banner

Template Name: **Banner_Template**

Description: Banner Template

Table 84. banner feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	MOTD Banner	Global	This is a private network. It is for authorized use only.

SNMP

Devices: vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud

Template: SNMP

Template Name: **SNMP_Template**

Description: SNMP Template

Table 85. SNMP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	snmp_shutdown
	Name of Device for SNMP	Device Specific	snmp_device_name
	Location of Device	Device Specific	snmp_device_location
SNMP Version	View/Name	Radio button	V2
View and community	View/Name	Global	isoALL
	View/Object Identifiers	Global	1.3.6.1
	Community/ Name	Global	c1sco123
	Community/ Authorization	Global/ drop-down	read-only
	Community/View	Global	isoALL
Trap	Trap Group/ Group Name	Global	SNMP-GRP
	Trap Group/Trap Type Modules/ Severity Levels	Global	critical, major, minor
	Trap Group/Trap Type Modules/ Module Name	Global	all

Data center feature templates

Data center transport VPN (VPN 0) feature template

Devices: vEdge 2000, vEdge 5000

Template: VPN

Template Name: **DC _VPN0**

Description: DC Transport VPN 0

Table 86. VPN0 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	64.100.100.125
	Secondary DNS Address	Global	64.100.100.126
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio Button	Next Hop
	Next Hop	Device Specific	vpn0_mpls_next_hop_ip_addr
	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

Data center VPN interface (MPLS)

Devices: vEdge 2000, vEdge 5000

Template: VPN Interface

Template Name: **DC _MPLS_Interface**

Description: DC MPLS Interface

Table 87. VPN0 interface feature template settings (MPLS)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
	Allow Service>DHCP	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Data center VPN interface (Internet)

Devices: vEdge 2000, vEdge 5000

Template: VPN Interface

Template Name: **DC_INET_Interface**

Description: DC Internet Interface

Table 88. VPN0 interface feature template settings (Internet)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface name	Device Specific	vpn0_inet_int_gex/x
	description	Global	Internet interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
	Restrict	Global	Off
	Allow Service>DHCP	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

Data center service VPN 1

Devices: vEdge 2000, vEdge 5000

Template: VPN

Template Name: **DC _VPN1**

Description: DC Service VPN 1

Table 89. VPN512 interface feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN 1
	Enhance ECMP Keying	Global	On
Advertise OMP	BGP	Global	On

Data center VPN interface Ethernet 1

Devices: vEdge 2000, vEdge 5000

Template: VPN Interface Ethernet

Template Name: **DC _VPN1_Int1**

Description: DC Service VPN 1 Interface 1

Table 90. VPN1 interface Ethernet feature template settings (interface 1)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1 _lan_int1_gex/x
	Description	Device Specfic	vpn1_lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits

Data center VPN interface Ethernet 2

Devices: vEdge 2000, vEdge 5000

Template: VPN Interface Ethernet

Template Name: **DC _VPN1_Int2**

Description: DC Service VPN 1 Interface 2

Table 91. VPN1 interface Ethernet feature template settings (interface 2)

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1 _lan_int2_gex/x
	Description	Device Specific	vpn1_lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits

Data center VPN 1 BGP

Devices: vEdge 2000, vEdge 5000

Template: BGP

Template Name: **DC_VPN1 _BGP**

Description: DC VPN1 BGP Template

Table 92. BGP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	bgp _shutdown
	AS Number	Device Specific	bgp_as_num
	Router ID	Device Specific	bgp_router_id
	Propagate AS Path	Global	On
IPv4 Unicast Address family	Maximum Paths	Global	2
	Address Family	Drop-down	Ipv4-unicast
	Re-Distribute/ Protocol	Drop-down	omp

Section	Parameter	Type	Variable/value
	Network/Network Prefix	Device Specific	bgp_network_lo_addr/maskbits
Neighbor (1)	Address	Device Specific	bgp_neighbor1_address
	Description	Device Specific	bgp_neighbor1_description
	Remote AS	Device Specific	bgp_neighbor1_remote_as
	Address Family	Global	On
	Address Family	Global	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	BGP-POLICY-IN
	Shutdown	Device Specific	bgp_neighbor1_shutdown
	Advanced Options/ Password	Device Specific	bgp_neighbor1_password
	Advanced Options/ Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9
Neighbor (2)	Address	Device Specific	bgp_neighbor2_address
	Description	Device Specific	bgp_neighbor2_description
	Remote AS	Device Specific	bgp_neighbor2_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	BGP-POLICY-IN
	Shutdown	Device Specific	bgp_neighbor2_shutdown

Section	Parameter	Type	Variable/value
	Advanced Options/ Password	Device Specific	bgp_neighbor2_password
	Advanced Options/ Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9

Branch feature templates

Table 93. Branch VPN 0 feature template

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	64.100.100.125
	Secondary DNS Address	Global	64.100.100.126
IPv4Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn0_mpls_next_hop_ip_addr
	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

BR_MPLS_INT

Devices: vEdge 100 B, vEdge 100 M, vEdge 100 WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: **BR_MPLS_INT**

Description: **Branch MPLS Interface with Static IP**

Table 94. Branch VPN0 MPLS interface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Allow Service	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

BR_MPLS_SUBINT

Devices: vEdge 100 B, vEdge 100 M, vEdge 100 WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: **BR_MPLS_SUBINTv**

Description: Branch MPLS Subinterface with Static IP

Table 95. Branch VPN0 MPLS subinterface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex/x.VLAN
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Allow service	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_mpls_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350

BR_INET_INT

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface

Template Name: BR_INET_INT

Description: Branch Internet Interface with Static IP

Table 96. Branch VPN0 Internet interface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

BR_INET_INT_DHCP

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface

Template Name: **BR_INET_INT_DHCP**

Description: Branch Internet Interface with DHCP IP

Table 97. Branch VPN0 Internet interface dynamic IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio button	Dynamic
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

BR_INET_SUBINT

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface

Template Name: **BR_INET_SUBINT**

Description: **Branch Internet Subinterface with Static IP**

Table 98. Branch VPN0 Internet subinterface static IP feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex/x.VLAN
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr/maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_down
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow service	DHCP	Global	Off
Allow service	NTP	Global	On
Tunnel>Advanced options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	vpn0_inet_nat_enable
Advanced	TCP MSS	Global	1350
	Clear-Dont-Fragment	Global	On

BR_TLOC_INT

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface

Template Name: **BR_TLOC_INT**

Description: Branch TLOC Interface

Table 99. Branch VPN0 TLOC interface feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_tloc_int_shutdown
	Interface Name	Device Specific	vpn0_tloc_int_gex/x_or_gex/x.VLAN
	Description	Global	TLOC Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_tloc_int_ip_addr/maskbits
Advanced	TLOC Extension	Device Specific	vpn0_tloc_wan_int_gex/x

BR_WAN_Parent_INT

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template Name: BR_WAN_Parent_INT

Template: VPN Interface Ethernet

Description: **Branch WAN Parent Interface**

Table 100. Branch VPN0 WAN parent interface feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_wan_parent_int_shutdown
	Interface Name	Device Specific	vpn0_wan_parent_int_gex/x
	Description	Global	WAN Parent Interface
Advanced	IP MTU	Global	1504

BR_VPN0_MPLS_BGP

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: BGP

Template Name: BR_VPN0_MPLS_BGP

Description: Branch VPN 0 MPLS BGP to Provider

Table 101. Branch VPN0 MPLS BGP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn0_bgp _shutdown
	AS Number	Device Specific	vpn0_bgp_as_num
	Router ID	Device Specific	vpn_bgp_router_id
IPv4 Unicast address family	Maximum Paths	Global	2
	Address-Family	Drop-down	ipv4-unicast
	Re-distribute/ Protocol	Global	connected
Neighbor	Address	Device Specific	vpn0_bgp_neighbor_address
	Description	Device Specific	vpn_bgp_neighbor_description
	Remote AS	Device Specific	vpn_bgp_neighbor_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	DENY-ALL
	Route-Policy Out	Global	On
	Policy Name	Global	TLOC-EXT-PREFIX-ONLY
	Shutdown	Device Specific	vpn0_bgp_neighbor_shutdown

BR_VPN1_Base

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN

Template Name: BR_VPN1_Base

Description: Branch VPN1 Base Configuration

Table 102. Branch VPN 1 base feature template

Section	Parameter	Type	Variable/value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN
	Enhance ECMP Keying	Global	On
Advertise OMP	Connected	Global	On
	Aggregate	Global	On
	Aggregate/Prefix	Device Specific	vpn1_omp_aggregate_prefix
	Aggregate/ Aggregate Only	Global	On

BR_VPN1_Static_Routing

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN

Template Name: BR_VPN1_Static_Routing

Description: Branch VPN1 Static Routing Configuration

Table 103. Branch VPN 1 static routing feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	Service VPN
	Enhance ECMP Keying	Global	On
Advertise OMP	Static	Global	On
	Network	Global	On
	Prefix	Device Specific	vpn1_omp_network_lo_addr/ maskbits
IPv4 Route	Prefix	Device Specific	vpn1_br_static_route_prefix/maskbits
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn1_next_hop_ip_addr

BR_LAN_INT1

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT1

Description: Branch LAN Interface 1

Table 104. Branch VPN 1 interface 1 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int1_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10

BR_LAN_INT2

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT2

Description: Branch LAN Interface 2

Table 105. Branch VPN 1 interface 2 feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1_lan_int2_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10

BR_LAN_INT1_VRRP

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT1_VRRP

Description: Branch LAN Interface 1 VRRP

Table 106. Branch VPN 1 interface 1 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int1_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP (Select New VRRP)	Group ID	Global	1
	Priority	Device Specific	vpn1_vrrp_priority1
	Track OMP	Global	On
	Track Prefix List	Global	default-route
	IP Address	Device Specific	vpn1_vrrp_ip_addr1

BR_LAN_INT2_VRRP

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_INT2_VRRP

Description: Branch LAN Interface 2 VRRP

Table 107. Branch VPN 1 interface 2 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int2_shutdown
	Interface Name	Device Specific	vpn1_lan_int2_gex/x_or_gex/x.VLAN
	Description	Device Specific	vpn1_lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP (Select New VRRP)	Group ID	Global	2
	Priority	Device Specific	vpn1_vrrp_priority2
	Track OMP	Global	On
	Track Prefix List	Global	default-route
	IP Address	Device Specific	vpn1_vrrp_ip_addr2

BR_LAN_Parent_INT

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: VPN Interface Ethernet

Template Name: BR_LAN_Parent_INT

Description: Branch LAN Parent Interface

Table 108. Branch VPN1 LAN parent interface feature template

Section	Parameter	Type	Variable/value
Basic configuration	Shutdown	Device Specific	vpn1_lan_parent_int_shutdown
	Interface Name	Device Specific	vpn1_lan_parent_int_gex/x
	Description	Global	LAN Parent Interface
Advanced	IP MTU	Global	1504

BR_LAN_DATA_DHCP_Server

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: DHCP Server

Template Name: BR_LAN_DATA_DHCP_Server

Description: Branch LAN DHCP Server for Data VLAN

Table 109. Branch VPN1 LAN DHCP server for data VLAN feature template

Section	Parameter	Type	Variable/value
Basic configuration	Address Pool	Device Specific	data_dhcp_address_pool/maskbits
	Exclude Addresses	Device Specific	data_dhcp_address_exclude_range
Advanced	Domain Name	Global	cisco.local
	Default Gateway	Device Specific	data_dhcp_default_gateway
	DNS Servers	Global	10.4.48.10

BR_LAN_VOICE_DHCP_Server

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: DHCP Server

Template Name: BR_LAN_VOICE_DHCP_Server

Description: Branch LAN DHCP Server for Voice VLAN

Table 110. Branch VPN1 LAN DHCP server for voice VLAN feature template

Section	Parameter	Type	Variable/value
Basic configuration	Address Pool	Device Specific	voice_dhcp_address_pool/maskbits
	Exclude Addresses	Device Specific	voice_dhcp_address_exclude_range
Advanced	Domain Name	Global	cisco.local
	Default Gateway	Device Specific	voice_dhcp_default_gateway
	DNS Servers	Global	10.4.48.10
	TFTP Servers	Global	10.4.48.19

BR_VPN1_OSPF

Devices: vEdge 100B, vEdge 100M, vEdge 100WM, vEdge 1000

Template: OSPF

Template Name: BR_VPN1_OSPF

Description: Branch LAN VPN 1 OSPF

Table 111. Branch VPN1 OSPF feature template

Section	Parameter	Type	Variable/value
Basic configuration	Router ID	Device Specific	vpn1_ospf_router_id
Redistribute	Protocol	Global	omp
Area	Area Number	Global	0
	Interface/ Interface Name	Device Specific	vpn1_ospf_interface_gex/x
	Interface/ Interface Cost	Device Specific	vpn1_ospf_interface_cost
	Interface/ Advanced/OSPF Network Type	Global/drop-down	point-to-point
	Interface/ Authentication/ Authentication Type	Global/drop-down	message-digest
	Interface/ Message Digest/ Message Digest Key ID	Global	22
	Interface/ Message Digest/ Message Digest Key	Device Specific	vpn1_ospf_message_digest_key
Area range	Address	Device Specific	vpn1_ospf_area_range_address_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Global	On

Data center device template

Table 112. Data center device template: DC_Hybrid_TypeA_BGP

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		DC_VPN0
	VPN Interface	DC_MPLS_Int
	VPN Interface	DC_INET_Int
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		DC_VPN1
	BGP	DC_VPN1_BGP
	VPN Interface	DC_VPN1_Int1
	VPN Interface	DC_VPN1_Int2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		DC_Policy
SNMP		SNMP_Template

Branch device templates

Device Model: vEdge 1000

Template Name: Branch_A_MPLS_BGP_TLOC_VRRP

Description: Branch Dual vEdge Hybrid TLOC with MPLS BGP and LAN-side Trunk and VRRP

Table 113. Branch_A_MPLS_BGP_TLOC_VRRP device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_VRRP_INT1
	VPN Interface	BR_LAN_VRRP_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_A_INET_TLOC_VRRP

Device Model: vEdge 1000

Template Name: Branch_A_INET_TLOC_VRRP

Description: Branch Dual vEdge Hybrid TLOC with INET and LAN-side Trunk and VRRP

Table 114. Branch_A_INET_TLOC_VRRP device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_VRRP_INT1
	VPN Interface	BR_LAN_VRRP_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_B_INET(DHCP)

Device Model: vEdge 100 WM

Template Name: Branch_B_INET(DHCP)

Description: Branch Single vEdge Hybrid Internet DHCP address and No Switch

Table 115. Branch_B_INET(DHCP)

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_MPLS_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface	BR_LAN_INT2
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_C_INET(DHCP)_LAN_DHCPServer

Device Model: vEdge 100 B

Template Name: Branch_C_INET(DHCP)_LAN_DHCPServer

Description: Branch Single vEdge Hybrid Internet DHCP address with LAN Trunk and DHCP Server

Table 116. Branch_C_INET(DHCP)_LAN_DHCPServer device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface>DHCP Server	BR_LAN_DATA_DHCP_Server
	VPN Interface	BR_LAN_INT2
	VPN Interface>DHCP Server	BR_LAN_VOICE_DHCP_Server
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_D_MPLS_BGP_TLOC_SubInt_OSPF

Device Model: vEdge 100 B

Template Name: Branch_D_MPLS_BGP_TLOC_SubInt_OSPF

Description: Branch Dual vEdge Hybrid TLOC SubInts with MPLS BGP and LAN-side OSPF

Table 117. Branch_D_MPLS_BGP_TLOC_Subint_OSPF device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_INET_SUBINT
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_D_INET_TLOC_SubInt_OSPF

Device Model: vEdge 100 B

Template Name: Branch_D_INET_TLOC_SubInt_OSPF

Description: Branch Dual vEdge Hybrid TLOC SubInts with INET and LAN-side OSPF

Table 118. Branch_D_INET_TLOC_SubInt_OSPF device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_SUBINT
	VPN Interface	BR_TLOC_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_E_MPLS_CE_LAN_Static_Routing

Device Model: vEdge 100 B

Template Name: Branch_E_MPLS_CE_LAN_Static_Routing

Description: Branch Single vEdge Hybrid with MPLS CE and Static Routing for LAN

Table 119. Branch_E_MPLS_CE_LAN_Static_Routing device template

Template type	Template sub-type	Template name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0
	VPN Interface	BR_INET_INT
	VPN Interface	BR_MPLS_INT
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_Base
	VPN Interface	BR_LAN_INT1
	VPN Interface	VPN1_Lo0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Data center variable values

DC1-VE1

Table 120. Dc1-ve1 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	dc1-ve1
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG3,Primary
System IP(system_system_ip)	10.255.241.101
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
Address(vpn0_mpls_next_hop_ip_addr)	10.4.1.1
Address(vpn0_inet_next_hop_ip_addr)	10.4.1.5
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.4.1.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.4.1.6/30
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000

Variable	Value
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	1000000
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.167/23
AS Number(bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(bgp_router_id)	10.255.241.101
Address(bgp_neighbor_address1)	10.4.1.9
Address(bgp_neighbor_address2)	10.4.1.13
Description(bgp_neighbor1_description)	Agg-Switch1
Description(bgp_neighbor2_description)	Agg-Switch2
Remote AS(bgp_neighbor1_remote_as)	65112
Remote AS(bgp_neighbor2_remote_as)	65112
Password(bgp_neighbor1_password)	cisco123
Password(bgp_neighbor2_password)	cisco123
Interface Name(vpn1_lan_int1_gex/x)	ge0/4
Description(vpn1_lan_int1_description)	To DC1-SW1 G1/0/11
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(vpn1_lan_int1_ip_addr/maskbits)	10.4.1.10/30
Interface Name(vpn1_lan_int2_gex/x)	ge0/5
Description(vpn1_lan_int2_description)	To DC1-SW2 G1/0/11
IPv4 Address(vpn1_lan_int2_ip_addr/maskbits)	10.4.1.14/30
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(vpn1_lo0_int_ip_addr/maskbits)	10.255.241.101/32
Shutdown(snmp_shutdown)	☐

Variable	Value
Name of Device for SNMP(snmp_device_name)	DC1-VE1
Location of Device(snmp_device_location)	Datacenter 1
vEdgePolicy/bgp_metric	50

DC1-VE2

Table 121. Dc1-ve2 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	dc1-ve2
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG2,Secondary
System IP(system_system_ip)	10.255.241.102
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
Address(vpn0_mpls_next_hop_ip_addr)	10.4.2.1
Address(vpn0_inet_next_hop_ip_addr)	10.4.2.5
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.4.2.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.4.2.6/30

Variable	Value
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	1000000
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.168/23
AS Number(bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(bgp_router_id)	10.255.241.102
Address(bgp_neighbor_address1)	10.4.2.9
Address(bgp_neighbor_address2)	10.4.2.13
Description(bgp_neighbor1_description)	Agg-Switch1
Description(bgp_neighbor2_description)	Agg-Switch2
Remote AS(bgp_neighbor1_remote_as)	65112
Remote AS(bgp_neighbor2_remote_as)	65112
Password(bgp_neighbor1_password)	cisco123
Password(bgp_neighbor2_password)	cisco123
Interface Name(vpn1_lan_int1_gex/x)	ge0/4
Description(vpn1_lan_int1_description)	To DC1-SW1 G1/0/12
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(vpn1_lan_int1_ip_addr/maskbits)	10.4.2.10/30
Interface Name(vpn1_lan_int2_gex/x)	ge0/5
Description(vpn1_lan_int2_description)	To DC1-SW2 G1/0/12
IPv4 Address(vpn1_lan_int2_ip_addr/maskbits)	10.4.2.14/30

Variable	Value
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(vpn1_lo0_int_ip_addr/maskbits)	10.255.241.102/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-VE2
Location of Device(snmp_device_location)	Datacenter 1
vEdgePolicy/bgp_metric	100

Branch variable values

BR1-VE1: Branch_A_MPLS_BGP_TLOC_VRRP

Table 122. Branch 1 vEdge 1 device template variable values

Variable	Value
Password(user_admin_password)	admin
Hostname(system_host_name)	br1-ve1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,v1000,US,West,UG5,Primary
System IP(system_system_ip)	10.255.241.11
Site ID(system_site_id)	112002
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	192.168.101.1
Address(vpn0_inet_next_hop_ip_addr)	10.101.2.2
AS Number(vpn0_bgp_as_num)	65201
Shutdown(vpn0_bgp_shutdown)	☐
Router ID(vpn_bgp_router_id)	10.255.241.11

Variable	Value
Address(vpn0_bgp_neighbor_address)	192.168.101.1
Description(vpn0_bgp_neighbor_description)	MPLS BGP Service Provider
Shutdown(vpn0_bgp_neighbor_shutdown)	☐
Remote AS(vpn0_bgp_neighbor_remote_as)	102
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.101.2.1/30
NAT	☐
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	192.168.101.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000
Interface Name(vpn0_tloc_int_gex/x_or_gex/x.VLAN)	ge0/7
IPv4 Address(vpn0_tloc_int_ip_addr/maskbits)	10.101.1.1/30
TLOC Extension(vpn0_tloc_wan_int_gex/x)	ge0/2
Shutdown(vpn0_tloc_int_shutdown)	☐
Interface Name(vpn1_lan_parent_int_gex/x)	ge0/4
Shutdown(vpn1_lan_parent_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0

Variable	Value
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.159/23
Prefix(vpn1_omp_aggregate_prefix)	10.101.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/4.10
Description(vpn1_int1_description)	Data Vlan
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.101.10.2/24
Shutdown(vpn1_lan_int1_shutdown)	☐
Priority(vpn1_vrrp_priority1)	200
IP Address(vpn1_vrrp_ip_addr1)	10.101.10.1
Interface Name(vpn_lan_int2_gex/x_or_gex/x.VLAN)	ge0/4.20
Description(vpn1_int2_description)	Voice Vlan
IPv4 Address(vpn_int2_ip_addr/maskbits)	10.101.20.2/24
Shutdown(vpn1_lan_int2_shutdown)	☐
Priority(vpn_vrrp_priority2)	200
IP Address(vpn_vrrp_ip_addr2)	10.101.20.1
IPv4 Address(vpn1_lo0_ip_addr/maskbits)	10.255.241.11/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-VE1
Location of Device(snmp_device_location)	Branch 1
vedgePolicy/bgp_tloc_ext_prefix_to_advertise	10.101.1.0/30
vedgePolicy/ospf_metric	0

BR1-VE2: Branch_A_INET_TLOC_VRRP

Table 123. Branch 1 vEdge 2 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br1-ve2
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,v1000,US,West,UG4,Secondary
System IP(system_system_ip)	10.255.241.12
Site ID(system_site_id)	112002
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	10.101.1.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.101.1
Interface Name(vpn0_inet_int_gex/x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	64.100.101.2/28
NAT	☑
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_mpls_int_gex/x_or_gex/x.VLAN)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.101.1.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000

Variable	Value
Interface Name(vpn0_tloc_int_gex/x_or_gex/x.VLAN)	ge0/7
IPv4 Address(vpn0_tloc_int_ip_addr/maskbits)	10.101.2.2/30
TLOC Extension(vpn0_tloc_wan_int_gex/x)	ge0/0
Shutdown(vpn0_tloc_int_shutdown)	☐
Interface Name(vpn1_lan_parent_int_gex/x)	ge0/4
Shutdown(vpn1_lan_parent_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.160/23
Prefix(vpn1_omp_aggregate_prefix)	10.101.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/4.10
Description(vpn1_int1_description)	Data Vlan
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.101.10.3/24
Shutdown(vpn1_lan_int1_shutdown)	☐
Priority(vpn1_vrrp_priority1)	100
IP Address(vpn1_vrrp_ip_addr1)	10.101.10.1
Interface Name(vpn_lan_int2_gex/x_or_gex/x.VLAN)	ge0/4.20
Description(vpn1_int2_description)	Voice Vlan
IPv4 Address(vpn_int2_ip_addr/maskbits)	10.101.20.3/24
Shutdown(vpn1_lan_int2_shutdown)	☐
Priority(vpn_vrrp_priority2)	100
IP Address(vpn_vrrp_ip_addr2)	10.101.20.1
IPv4 Address(vpn0_lo0_ip_addr/maskbits)	10.255.241.12/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-VE2
Location of Device(snmp_device_location)	Branch 1

BR2-VE1: Branch_B_INET(DHCP)

Table 124. Branch 2 vEdge 1 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br2-ve1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-97.335
Device Groups(system_device_groups)	BRANCH,v100,US,West,UG4,Primary
System IP(system_system_ip)	10.255.241.21
Site ID(system_site_id)	111002
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	192.168.102.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.102.1
Interface Name(vpn0_inet_int_gex/x)	ge0/4
Preference(vpn0_inet_tunnel_ipsec_preference)	0
NAT	☐
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	100000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	200000
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	192.168.102.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	100000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	200000

Variable	Value
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.159/23
Prefix(vpn1_omp_aggregate_prefix)	10.102.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/0
Description(vpn1_int1_description)	To Host 1
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.102.10.1/30
Shutdown(vpn1_lan_int1_shutdown)	☐
Interface Name(vpn_lan_int2_gex/x_or_gex/x.VLAN)	ge0/3
Description(vpn1_int2_description)	To Host 2
IPv4 Address(vpn_int2_ip_addr/maskbits)	10.102.20.1/30
Shutdown(vpn1_lan_int2_shutdown)	☐
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR2-VE1
Location of Device(snmp_device_location)	Branch 2

BR3-VE1: Branch_C_INET(DHCP)_LAN_DHCPServer

Table 125. Branch 3 vEdge 1 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br3-ve1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,v100,US,West,UG5,Primary
System IP(system_system_ip)	10.255.241.31
Site ID(system_site_id)	113003

Variable	Value
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	192.168.103.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.103.1
Interface Name(vpn0_inet_int_gex/x)	ge0/4
NAT	☐
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	192.168.103.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000
Interface Name(vpn1_lan_parent_int_gex/x)	ge0/0
Shutdown(vpn1_lan_parent_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.153/23
Prefix(vpn1_omp_aggregate_prefix)	10.103.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/0.10
Description(vpn1_int1_description)	Data Vlan
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.103.10.1/24

Variable	Value
Shutdown(vpn1_lan_int1_shutdown)	☐
data_dhcp_address_pool_maskbits	10.103.10.0/24
data_dhcp_address_exclude_range	10.103.10.1-10.103.10.50,10.103.10.101-10.103.10.255
data_dhcp_default_gateway	10.103.10.1
Interface Name(vpn_lan_int2_gex/x_or_gex/x.VLAN)	ge0/0.20
Description(vpn1_int2_description)	Voice Vlan
IPv4 Address(vpn_int2_ip_addr/maskbits)	10.103.20.1/24
Shutdown(vpn1_lan_int2_shutdown)	☐
voice_dhcp_address_pool_maskbits	10.103.20.0/24
voice_dhcp_address_exclude_range	10.103.20.1
voice_dhcp_default_gateway	10.103.20.1
IPv4 Address(vpn0_lo0_ip_addr/maskbits)	10.255.241.31/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR3-VE1
Location of Device(snmp_device_location)	Branch 3

BR4-VE1: Branch_D_MPLS_BGP_TLOC_SubInt_OSPF

Table 126. Branch 4 vEdge 1 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br4-ve1
Latitude(system_latitude)	33.754
Longitude(system_longitude)	-84.386
Device Groups(system_device_groups)	BRANCH,v100,US,East,UG5,Primary
System IP(system_system_ip)	10.255.242.41
Site ID(system_site_id)	122004
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	192.168.104.1
Address(vpn0_inet_next_hop_ip_addr)	10.104.2.2
AS Number(vpn0_bgp_as_num)	65204
Shutdown(vpn0_bgp_shutdown)	☐
Router ID(vpn_bgp_router_id)	10.255.242.41
Address(vpn0_bgp_neighbor_address)	192.168.104.1
Description(vpn0_bgp_neighbor_description)	MPLS BGP Service Provider
Shutdown(vpn0_bgp_neighbor_shutdown)	☐
Remote AS(vpn0_bgp_neighbor_remote_as)	102
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	192.168.104.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000

Variable	Value
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000
Interface Name(vpn0_inet_int_gex/x.VLAN)	ge0/4.102
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	10.104.2.1/30
NAT	☐
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_wan_parent_int_gex/x)	ge0/4
Shutdown(vpn0_wan_parent_int_shutdown)	☐
Interface Name(vpn0_tloc_int_gex/x_or_gex/x.VLAN)	ge0/4.102
IPv4 Address(vpn0_tloc_int_ip_addr/maskbits)	10.104.1.1/30
TLOC Extension(vpn0_tloc_wan_int_gex/x)	ge0/2
Shutdown(vpn0_tloc_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.154/23
Prefix(vpn1_omp_aggregate_prefix)	10.104.0.0/16
Router ID(vpn1_ospf_router_id)	10.255.242.41
Interface Name(vpn1_ospf_interface_gex/x)	ge0/0
Interface Cost(vpn1_ospf_interface_cost)	1
Message Digest Key(vpn1_ospf_message_digest_key)	cisco123
Address(ospf_area_range_address_0)	10.104.0.0/16
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/0
Description(vpn1_int1_description)	To LAN-SW

Variable	Value
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.104.0.2/30
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(vpn0_lo0_ip_addr/maskbits)	10.255.242.41/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR4-VE1
Location of Device(snmp_device_location)	Branch 4
vedgePolicy/bgp_tloc_ext_prefix_to_advertise	10.104.1.0/30
vedgePolicy/ospf_metric	10

BR4-VE2: Branch_D_INET_TLOC_SubInt_OSPF

Table 127. Branch 4 vEdge 2 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br4-ve2
Latitude(system_latitude)	33.754
Longitude(system_longitude)	-84.386
Device Groups(system_device_groups)	BRANCH,v100,US,East,UG4,Secondary
System IP(system_system_ip)	10.255.242.42
Site ID(system_site_id)	122004
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	10.104.1.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.104.1
Interface Name(vpn0_inet_int_gex/x_or_gex/x.VLAN)	ge0/4
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	64.100.104.2/28
NAT	☑

Variable	Value
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	☐
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	500000
Interface Name(vpn0_mpls_int_gex/x.VLAN)	ge0/2.101
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.104.1.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	500000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000
Interface Name(vpn0_tloc_int_gex/x_or_gex/x.VLAN)	ge0/2.102
IPv4 Address(vpn0_tloc_int_ip_addr/maskbits)	10.104.2.2/30
TLOC Extension(vpn0_tloc_wan_int_gex/x)	ge0/4
Shutdown(vpn0_tloc_int_shutdown)	☐
Interface Name(vpn0_wan_parent_int_gex/x)	ge0/2
Shutdown(vpn0_wan_parent_int_shutdown)	☐
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.155/23
Prefix(vpn1_omp_aggregate_prefix)	10.104.0.0/16
Router ID(vpn1_ospf_router_id)	10.255.242.42
Interface Name(vpn1_ospf_interface_gex/x)	ge0/0
Interface Cost(vpn1_ospf_interface_cost)	1
Message Digest Key(vpn1_ospf_message_digest_key)	cisco123
Address(ospf_area_range_address_0)	10.104.0.0/16
IPv4 Address(vpn0_lo0_ip_addr/maskbits)	10.255.242.42/32

Variable	Value
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/0
Description(vpn1_int1_description)	To LAN-SW
IPv4 Address(vpn_int1_ip_addr/maskbits)	10.104.0.6/30
Shutdown(vpn1_lan_int1_shutdown)	☐
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR4-VE2
Location of Device(snmp_device_location)	Branch 4
vedgePolicy/bgp_tloc_ext_prefix_to_advertise	10.104.1.0/30
vedgePolicy/ospf_metric	20

BR5-VE1: Branch_E_MPLS_CE_LAN_Static_Routing

Table 128. Branch 5 vEdge 1 device template variable values

Variable	Value
Password (user_admin_password)	admin
Hostname(system_host_name)	br5-ve1
Latitude(system_latitude)	37.6461
Longitude(system_longitude)	-77.511
Device Groups(system_device_groups)	BRANCH,v100,US,East,UG1,Primary
System IP(system_system_ip)	10.255.242.51
Site ID(system_site_id)	121005
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Address(vpn0_mpls_next_hop_ip_addr)	10.105.1.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.105.1

Variable	Value
Interface Name(vpn0_inet_int_gex/x)	ge0/4
IPv4 Address(vpn0_inet_int_ip_addr/maskbits)	64.100.105.2/28
NAT	
Preference(vpn0_inet_tunnel_ipsec_preference)	0
Shutdown(vpn0_inet_int_shutdown)	
Bandwidth Upstream(vpn0_inet_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_inet_int_bandwidth_down)	3000000
Interface Name(vpn0_mpls_int_gex/x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr/maskbits)	10.105.1.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference	0
Shutdown(vpn0_mpls_int_shutdown)	
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	3000000
Address(vpn512_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_mgmt0_or_gex/x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr/maskbits)	192.168.255.156/23
Prefix(vpn1_br_static_route_prefix/maskbits)	10.105.0.0/16
Address(vpn1_br_next_hop_ip_addr)	10.105.0.1
Prefix(vpn1_omp_network_lo_addr/maskbits)	10.255.242.51/32
Interface Name(vpn_lan_int1_gex/x_or_gex/x.VLAN)	ge0/0
Description(vpn1_lan_int1_description)	To LAN-SW
IPv4 Address(vpn_lan_int1_ip_addr/maskbits)	10.105.0.2/30
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(vpn0_lo0_ip_addr/maskbits)	10.255.241.11/32
Shutdown (snmp_shutdown)	
Name of Device for SNMP(snmp_device_name)	BR5-VE1
Location of Device(snmp_device_location)	Branch 5

Appendix F: vEdge router CLI-equivalent configuration

DC1-VE1

```
system
 host-name               dc1-ve1
 gps-location latitude 37.409284
 gps-location longitude -121.928528
 device-groups           DC Primary UG3 US West v5000
 system-ip               10.255.241.101
 site-id                 110001
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    "ENB-Solutions - 21615"
 organization-name       "ENB-Solutions - 21615"
 no port-hop
 vbond vbond-21615.cisco.net
 aaa
  auth-order local
  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 [admin password]
  !
```

```
 !
 logging
  disk
   enable
  !
  server 10.4.48.13
   vpn              1
   source-interface loopback0
  exit
 !
 ntp
  server time.nst.gov
   version 4
  exit
 !
!
bfd color mpls
 no pmtu-discovery
!
bfd color biz-internet
 no pmtu-discovery
!
bfd app-route poll-interval 120000
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
!
security
 ipsec
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
```

```
!
snmp
 no shutdown
 name     DC1-VE1
 location "Datacenter 1"
 view isoALL
  oid 1.3.6.1
 !
 community c1sco123
  view          isoALL
  authorization read-only
 !
 trap group SNMP-GRP
  all
   level critical major minor
  exit
 exit
!
banner
 motd "This is a private network. It is for authorized use only."
!
vpn 0
 name "Transport VPN"
 dns 64.100.100.125 primary
 dns 64.100.100.126 secondary
 ecmp-hash-key layer4
 interface ge0/0
  description          "INET Interface"
  ip address 10.4.1.6/30
  tunnel-interface
   encapsulation ipsec preference 100
   color biz-internet
   no allow-service bgp
   no allow-service dhcp
```

```
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
 !
 clear-dont-fragment
 tcp-mss-adjust       1350
 no shutdown
 bandwidth-upstream   1000000
 bandwidth-downstream 1000000
!
interface ge0/2
 description          "MPLS Interface"
 ip address 10.4.1.2/30
 tunnel-interface
  encapsulation ipsec preference 100
  color mpls restrict
  no allow-service bgp
  no allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
 !
 clear-dont-fragment
 tcp-mss-adjust       1350
 no shutdown
 bandwidth-upstream   1000000
```

```
  bandwidth-downstream 1000000
 !
 ip route 0.0.0.0/0 10.4.1.1
 ip route 0.0.0.0/0 10.4.1.5
!
vpn 1
 name "Service VPN 1"
 ecmp-hash-key layer4
 router
  bgp 65113
   router-id        10.255.241.101
   propagate-aspath
   address-family ipv4-unicast
    network 10.255.241.101/32
    maximum-paths paths 2
    redistribute omp route-policy BGP_VEDGE_PREFER
   !
   neighbor 10.4.1.9
    description Agg-Switch1
    no shutdown
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$0zvgy7IA7Bmm1otKZzk2/r52Svkap9e6CqbE6XZ+GNY=
    address-family ipv4-unicast
     route-policy BGP-POLICY-IN in
    !
   !
   neighbor 10.4.1.13
    description Agg-Switch2
    no shutdown
    remote-as   65112
```

```
      timers
       keepalive 3
       holdtime  9
      !
      password    $8$b83R94gYWNpmDLF4BUhKlWcprt+7F/WBaonoSqUSzbA=
      address-family ipv4-unicast
       route-policy BGP-POLICY-IN in
      !
     !
    !
   !
  interface ge0/4
   description "To DC1-SW1 G1/0/11"
   ip address 10.4.1.10/30
   no shutdown
  !
  interface ge0/5
   description "To DC1-SW2 G1/0/11"
   ip address 10.4.1.14/30
   no shutdown
  !
  interface loopback0
   ip address 10.255.241.101/32
   no shutdown
  !
  omp
   advertise bgp
  !
 !
 vpn 512
  name "Management VPN"
  interface mgmt0
   description "Management Interface"
   ip address 192.168.255.167/23
```

```
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.255.1
!
policy
 app-visibility
 flow-visibility
 lists
  prefix-list MPLS-Transport
   ip-prefix 10.4.1.0/30
   ip-prefix 10.4.2.0/30
   ip-prefix 10.101.1.0/30
   ip-prefix 10.104.1.0/30
   ip-prefix 10.105.1.0/30
   ip-prefix 192.168.0.0/16 le 32
  !
  as-path-list Local-Routes
   as-path ^65112$
  !
  community-list Non-SD-WAN-Sites
   community 101:101
  !
 !
 route-policy BGP-POLICY-IN
  sequence 10
   match
    address MPLS-Transport
   !
   action reject
   !
  !
  sequence 20
   match
    community Non-SD-WAN-Sites
```

```
    !
    action accept
    !
   !
   sequence 30
    match
     as-path Local-Routes
    !
    action accept
     set
      community 1:100
     !
    !
   !
   default-action reject
  !
  route-policy BGP_VEDGE_PREFER
   sequence 10
    action accept
     set
      metric 50
     !
    !
   !
   default-action reject
  !
```

BR1-VE1 (partial)

```
vpn 0
 name "Transport VPN"
 dns 64.100.100.125 primary
 dns 64.100.100.126 secondary
 ecmp-hash-key layer4
 router
  bgp 65201
```

```
    router-id 10.255.241.11
    address-family ipv4-unicast
     maximum-paths paths 2
     redistribute connected
    !
    neighbor 192.168.101.1
     description "MPLS BGP Service Provider"
     no shutdown
     remote-as   102
     address-family ipv4-unicast
      route-policy DENY-ALL in
      route-policy TLOC-EXT-PREFIX-ONLY out
     !
    !
   !
```

BR1-VE1 (partial)

```
vpn 0
 name "Transport VPN"
 dns 64.100.100.125 primary
 dns 64.100.100.126 secondary
 ecmp-hash-key layer4
 router
  bgp 65201
   router-id 10.255.241.11
   address-family ipv4-unicast
    maximum-paths paths 2
    redistribute connected
   !
   neighbor 192.168.101.1
    description "MPLS BGP Service Provider"
    no shutdown
    remote-as   102
    address-family ipv4-unicast
     route-policy DENY-ALL in
```

```
    route-policy TLOC-EXT-PREFIX-ONLY out
   !
  !
 !
!
interface ge0/0
 description          "Internet Interface"
 ip address 10.101.2.1/30
 tunnel-interface
  encapsulation ipsec preference 100
  color biz-internet
  no allow-service bgp
  no allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
 !
 clear-dont-fragment
 tcp-mss-adjust       1350
 no shutdown
 qos-map              QOS
 rewrite-rule QOS-REWRITE
 bandwidth-upstream   500000
 bandwidth-downstream 500000
!
interface ge0/2
 description          "MPLS Interface"
 ip address 192.168.101.2/30
 tunnel-interface
  encapsulation ipsec preference 100
```

```
    color mpls restrict
    allow-service bgp
    no allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    allow-service ntp
    no allow-service ospf
    no allow-service stun
   !
   clear-dont-fragment
   tcp-mss-adjust       1350
   no shutdown
   qos-map              QOS
   rewrite-rule QOS-REWRITE
   bandwidth-upstream   500000
   bandwidth-downstream 500000
  !
  interface ge0/4
   description "LAN Parent Interface"
   mtu         1504
   no shutdown
  !
  interface ge0/7
   description    "TLOC Interface"
   ip address 10.101.1.1/30
   tloc-extension ge0/2
   no shutdown
  !
  ip route 0.0.0.0/0 10.101.2.2
  ip route 0.0.0.0/0 192.168.101.1
 !
 vpn 1
```

```
 name "Service VPN"
 ecmp-hash-key layer4
 interface ge0/4.10
  description "Data Vlan"
  ip address 10.101.10.2/24
  dhcp-helper 10.4.48.10
  no shutdown
  vrrp 1
   priority          200
   track-prefix-list default-route
   ipv4 10.101.10.1
  !
 !
 interface ge0/4.20
  description "Voice Vlan"
  ip address 10.101.20.2/24
  dhcp-helper 10.4.48.10
  no shutdown
  vrrp 2
   priority          200
   track-prefix-list default-route
   ipv4 10.101.20.1
  !
 !
 interface loopback0
  ip address 10.255.241.11/32
  no shutdown
 !
 omp
  advertise connected
  advertise aggregate 10.101.0.0/16 aggregate-only
 !
!
policy
```

```
app-visibility
flow-visibility
lists
 prefix-list default-route
  ip-prefix 0.0.0.0/0
 !
 prefix-list tloc-ext-prefix
  ip-prefix 10.101.1.0/30
 !
!
route-policy DENY-ALL
 sequence 10
  action reject
  !
 !
 default-action reject
!
route-policy OSPF_VEDGE_PREFER
 sequence 10
  action accept
   set
    metric 0
   !
  !
 !
 default-action reject
!
route-policy TLOC-EXT-PREFIX-ONLY
 sequence 10
  match
   address tloc-ext-prefix
  !
  action accept
  !
```

```
 !
 default-action reject
!
class-map
 class VOICE queue 0
 class CRITICAL-DATA queue 1
 class BULK queue 2
 class CLASS-DEFAULT queue 3
 class INTERACTIVE-VIDEO queue 4
 class CONTROL-SIGNALING queue 5
!
rewrite-rule QOS-REWRITE
 class BULK low dscp 10
 class BULK high dscp 10
 class CLASS-DEFAULT low dscp 0
 class CLASS-DEFAULT high dscp 0
 class CONTROL-SIGNALING low dscp 18
 class CONTROL-SIGNALING high dscp 18
 class CRITICAL-DATA low dscp 18
 class CRITICAL-DATA high dscp 18
 class INTERACTIVE-VIDEO low dscp 34
 class INTERACTIVE-VIDEO high dscp 34
!
qos-scheduler QOS-BULK-DATA
 class              BULK
 bandwidth-percent  10
 buffer-percent     10
 drops             red-drop
!
qos-scheduler QOS-CLASS-DEFAULT
 class             CLASS-DEFAULT
 bandwidth-percent 20
 buffer-percent    20
 drops             red-drop
```

```
!
qos-scheduler QOS-CONTROL-SIGNALING
 class             CONTROL-SIGNALING
 bandwidth-percent 10
 buffer-percent    10
!
qos-scheduler QOS-CRITICAL-DATA
 class             CRITICAL-DATA
 bandwidth-percent 30
 buffer-percent    30
 drops             red-drop
!
qos-scheduler QOS-INTERACTIVE-VIDEO
 class             INTERACTIVE-VIDEO
 bandwidth-percent 20
 buffer-percent    20
 drops             red-drop
!
qos-scheduler QOS-VOICE
 class             VOICE
 bandwidth-percent 10
 buffer-percent    10
 scheduling        llq
!
qos-map QOS
 qos-scheduler QOS-BULK-DATA
 qos-scheduler QOS-CLASS-DEFAULT
 qos-scheduler QOS-CONTROL-SIGNALING
 qos-scheduler QOS-CRITICAL-DATA
 qos-scheduler QOS-INTERACTIVE-VIDEO
 qos-scheduler QOS-VOICE
!
```

BR3-VE1 (partial)

```
interface ge0/4
  description          "Internet Interface"
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec preference 0
   color biz-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
  !
  clear-dont-fragment
  tcp-mss-adjust       1350
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
  bandwidth-upstream   500000
  bandwidth-downstream 500000
!
!
 ip route 0.0.0.0/0 64.100.103.1
 ip route 0.0.0.0/0 192.168.103.1
!
vpn 1
 name "Service VPN"
 ecmp-hash-key layer4
 interface ge0/0.10
  description "Data Vlan"
```

```
 ip address 10.103.10.1/24
 dhcp-helper 10.4.48.10
 no shutdown
 dhcp-server
  address-pool 10.103.10.0/24
  exclude      10.103.10.1-10.103.10.50 10.103.10.101-10.103.10.255
  offer-time   600
  lease-time   86400
  admin-state  up
  options
   domain-name     cisco.local
   default-gateway 10.103.10.1
   dns-servers     10.4.48.10
  !
 !
!
interface ge0/0.20
 description "Voice Vlan"
 ip address 10.103.20.1/24
 dhcp-helper 10.4.48.10
 no shutdown
 dhcp-server
  address-pool 10.103.20.0/24
  exclude      10.103.20.1
  offer-time   600
  lease-time   86400
  admin-state  up
  options
   domain-name     cisco.local
   default-gateway 10.103.20.1
   dns-servers     10.4.48.10
   tftp-servers    10.4.48.19
  !
 !
```

```
 !
 interface loopback0
  ip address 10.255.241.31/32
  no shutdown
 !
 omp
  advertise connected
  advertise aggregate 10.103.0.0/16 aggregate-only
 !
```

BR1-VE4 (partial)

```
interface ge0/2
  description          "MPLS Interface"
  ip address 192.168.104.2/30
  tunnel-interface
   encapsulation ipsec preference 100
   color mpls restrict
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
  !
  clear-dont-fragment
  tcp-mss-adjust       1350
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
  bandwidth-upstream   500000
  bandwidth-downstream 500000
```

```
!
interface ge0/4
 description "WAN Parent Interface"
 mtu         1504
 no shutdown
!
interface ge0/4.101
 description    "TLOC Interface"
 ip address 10.104.1.1/30
 tloc-extension ge0/2
 no shutdown
!
interface ge0/4.102
 description          "Internet Interface"
 ip address 10.104.2.1/30
 tunnel-interface
  encapsulation ipsec preference 100
  color biz-internet
  no allow-service bgp
  no allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
 !
 clear-dont-fragment
 tcp-mss-adjust       1350
 no shutdown
 bandwidth-upstream   500000
 bandwidth-downstream 500000
!
```

```
 ip route 0.0.0.0/0 10.104.2.2
 ip route 0.0.0.0/0 192.168.104.1
!
vpn 1
 name "Service VPN"
 ecmp-hash-key layer4
 router
  ospf
   router-id 10.255.242.41
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp route-policy OSPF_VEDGE_PREFER
   area 0
    interface ge0/0
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5 [md5 password]
    exit
    range 10.104.0.0/16
   exit
  !
 !
 interface ge0/0
  description "To LAN-SW"
  ip address 10.104.0.2/30
  dhcp-helper 10.4.48.10
  no shutdown
 !
 interface loopback0
  ip address 10.255.242.41/32
  no shutdown
```

```
 !
 omp
  advertise connected
  advertise aggregate 10.104.0.0/16 aggregate-only
 !
```

BR5-VE1 (partial)

```
vpn 1
 name "Service VPN"
 ecmp-hash-key layer4
 interface ge0/0
  description "To LAN-SW"
  ip address 10.105.0.2/30
  dhcp-helper 10.4.48.10
  no shutdown
 !
 interface loopback0
  ip address 10.255.242.51/32
  no shutdown
 !
 ip route 10.105.0.0/16 10.105.0.1
 omp
  advertise static
  advertise network 10.255.242.51/32
 !
```

vSmart (partial)

```
policy
 sla-class SLA_BEST_EFFORT
  loss    5
  latency 750
  jitter  750
 !
```

```
sla-class SLA_BUSINESS_CRITICAL
 loss    1
 latency 300
 jitter  300
!
sla-class SLA_BUSINESS_DATA
 loss    3
 latency 500
 jitter  500
!
sla-class SLA_REALTIME
 loss    2
 latency 300
 jitter  60
!
data-policy _ALL_VPNS_qos_classify
 vpn-list ALL_VPNS
  sequence 1
   match
    dscp 46
   !
   action accept
    set
     forwarding-class VOICE
    !
   !
  !
  sequence 11
   match
    dscp 34 36 38
   !
   action accept
    set
     forwarding-class INTERACTIVE-VIDEO
```

```
    !
   !
  !
  sequence 21
   match
    dscp 10 12 14
   !
   action accept
    set
     forwarding-class BULK
    !
   !
  !
  sequence 31
   match
    app-list APPS_BULK_DATA
   !
   action accept
    set
     dscp             10
     forwarding-class BULK
    !
   !
  !
  sequence 41
   match
    dscp 24 48
   !
   action accept
    set
     forwarding-class CONTROL-SIGNALING
    !
   !
  !
```

```
sequence 51
 match
  destination-data-prefix-list MGT_Servers
  protocol                     6 17
 !
 action accept
  set
   forwarding-class CRITICAL-DATA
  !
 !
!
sequence 61
 match
  dscp 24
 !
 action accept
  set
   forwarding-class CONTROL-SIGNALING
  !
 !
!
sequence 71
 match
  destination-port 11000-11999 1300 1718 1719 1720 5060 5061
  protocol         6
 !
 action accept
  set
   dscp             24
   forwarding-class CONTROL-SIGNALING
  !
 !
!
sequence 81
```

```
    match
     dscp 16 18 20 22 26 28 30 32 40
    !
    action accept
     set
      forwarding-class CRITICAL-DATA
     !
    !
   !
   sequence 91
    match
     dscp 0 8
    !
    action accept
     set
      forwarding-class CLASS-DEFAULT
     !
    !
   !
   sequence 101
    match
     app-list APPS_SCAVENGER
    !
    action accept
     set
      dscp             0
      forwarding-class CLASS-DEFAULT
     !
    !
   !
   default-action accept
  !
 !
app-route-policy _ALL_VPNS_App-Route-Policy
```

```
vpn-list ALL_VPNS
 sequence 1
  match
   app-list APPS_SCAVENGER
  !
  action
   sla-class SLA_BEST_EFFORT strict preferred-color biz-internet
  !
 !
 sequence 11
  match
   dscp 46
  !
  action
   sla-class SLA_REALTIME preferred-color mpls
  !
 !
 sequence 21
  match
   destination-data-prefix-list MGT_Servers
  !
  action
   sla-class SLA_BUSINESS_CRITICAL
  !
 !
 sequence 31
  match
   app-list APPS_NETWORK_CONTROL
  !
  action
   sla-class SLA_BUSINESS_CRITICAL
  !
 !
 sequence 41
```

```
    match
     dscp 10 12 14 18 20 22 26 28 30 34 36 38
    !
    action
     sla-class SLA_BUSINESS_CRITICAL
    !
   !
   sequence 51
    match
     dscp 8 16 24 32 40 48 56
    !
    action
     sla-class SLA_BUSINESS_DATA
    !
   !
   sequence 61
    match
     dscp 0
    !
    action
     sla-class SLA_BEST_EFFORT preferred-color biz-internet
    !
   !
   default-action sla-class SLA_BEST_EFFORT
  !
!
lists
 vpn-list ALL_VPNS
  vpn 1-511
 !
 vpn-list Service_VPN
  vpn 1
 !
 data-prefix-list MGT_Servers
```

```
 ip-prefix 10.4.48.10/32
 ip-prefix 10.4.48.13/32
 ip-prefix 10.4.48.15/32
 ip-prefix 10.4.48.17/32
!
app-list APPS_BULK_DATA
 app ftp
 app imap
 app imaps
 app lotusnotes
 app outlook
 app pop3
 app pop3s
 app smtp
!
app-list APPS_NETWORK_CONTROL
 app ntp
 app radius
 app ssh
 app tacacs_plus
 app telnet
 app telnets
 app xmlrpc
!
app-list APPS_SCAVENGER
 app apple_update
 app facebook
 app facebook_apps
 app facebook_live
 app facebook_mail
 app facebook_messenger
 app facebook_video
 app twitter
 app youtube
```

```
  app youtube_hd
 !
 site-list ALL_SITES
  site-id 0-4294967295
 !
 site-list High_BW_East_Branches
  site-id 122000-129999
 !
 site-list High_BW_West_Branches
  site-id 112000-119999
 !
 site-list Low_BW_East_Branches
  site-id 121000-121999
 !
 site-list Low_BW_US_Sites
  site-id 111000-111999
  site-id 121000-121999
 !
 site-list Low_BW_West_Branches
  site-id 111000-111999
 !
 site-list West_DC1
  site-id 110001
 !
control-policy Filter-Low-BW-Sites
 sequence 1
  match tloc
   site-list Low_BW_US_Sites
  !
  action reject
  !
 default-action accept
!
control-policy control_-686667287
```

```
 sequence 10
  match route
   site-list West_DC1
   vpn-list  Service_VPN
  !
  action accept
  !
 sequence 20
  match tloc
   site-list West_DC1
  !
  action accept
  !
 default-action reject
!
 apply-policy
site-list ALL_SITES
 data-policy _ALL_VPNS_qos_classify from-service
 app-route-policy _ALL_VPNS_App-Route-Policy
!
site-list High_BW_East_Branches
 control-policy Filter-Low-BW-Sites out
!
site-list High_BW_West_Branches
 control-policy Filter-Low-BW-Sites out
!
site-list Low_BW_East_Branches
 control-policy control_-686667287 out
!
site-list Low_BW_West_Branches
 control-policy control_-686667287 out
!
!
```

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.