

Cisco SD-WAN End-to-End Deployment Guide

Version 18.3.5/16.9.4

July, 2019

Table of Contents

Introduction 6

SD-WAN deployment overview 8

Deployment example 10

Data center details 10

Transport side 11

Service side 11

MPLS routing 12

Branch details 13

Branch 1: Dual router/TLOC extension/layer 2 trunk LAN switch/VRRP site 13

Branch 2: Single router/Internet DHCP address/layer 2 LAN switch site 15

Branch 3: Single router/layer 2 trunk LAN switch site 16

Branch 4: Sub-interface TLOC-extension/layer 3 OSPF routing site 17

Branch 5: CE router/layer 3 switch/static LAN routing site 18

Additional details 19

Deployment details 22

Tuning controller configurations 22

Procedure 1: Verify controllers are up and ready 22

Procedure 2: Determine controller configuration mode 23

Procedure 3: Tune configuration settings (optional on all controllers) 24

Procedure 4: Retrieve the authorized WAN Edge serial number file 26

Procedure 5: Load the authorized WAN Edge serial number file 27

Preparing for software upgrades and upgrading the controllers 30

Procedure 1: Prepare and configure vManage for software upgrades 31

Procedure 2: Upgrade vManage (optional) 33

Procedure 3: Upgrade the vBond and vSmart controllers 34

Deploying the data center WAN Edge routers 35

Procedure 1: Verify the global vBond address 35

Procedure 2: Put the WAN Edge routers in staging state (optional) 36

Procedure 3: Configure the WAN Edge router via CLI to connect to the controllers 37

Procedure 4: Upgrade vEdge routers if necessary 40

Procedure 5: Configure basic information section of feature template 40

Procedure 6: Configure the transport VPN 50

Procedure 7: Configure the Management VPN (optional) 58

Procedure 8: Configure the Service VPN 59
Procedure 9: Configure additional templates (optional) 67
Procedure 10: Create a device template 72
Procedure 11: Deploy the device templates to the WAN Edge routers 75
Procedure 12: Create a localized policy 83
Procedure 13: Attach localized policy to a device template 88
Procedure 14: Add localized policy references in the feature templates 89
Procedure 15: Bring vEdge devices out of staging mode 91
Deploying remote sites 91
Procedure 1: Create a localized policy for the branches 91
Procedure 2: Configure the transport side feature templates 94
Procedure 3: Configure the service side feature templates 102
Procedure 4: Create the branch device templates 110
Procedure 5: Attach the device templates 118
Procedure 6: Bring remote vEdge routers online via ZTP 122
Procedure 7: Bring remote IOS XE SD-WAN routers online via PnP 124
Procedure 8: Bring remote IOS XE SD-WAN routers online via manual bootstrap method 124
Procedure 9: Verify the network status 126
Configuring centralized policy 129
Configuring an application-aware routing policy 137
Procedure 1: Create lists 138
Procedure 2: Create the application-aware routing policy 139
Procedure 3: Apply the policy definition 141
Configuring symmetric traffic for DPI 142
Procedure 1: Influence traffic from LAN to WAN 143
Procedure 2: Influence traffic from WAN to LAN over the overlay 148
Configuring quality of service 149
Procedure 1: Configure localized policy 151
Procedure 2: Define QoS classification access list 158
Procedure 3: Update feature templates 164
Appendices 166
Appendix A: Product list 166
Appendix B: Prepare IOS XE routers for SD-WAN deployment 166
Procedure 1: Check the hardware and software requirements 167
Procedure 2: Upgrade the rommon image 167

Procedure 3: Upgrade to the SD-WAN image 168
To revert back to IOS XE: 173
Appendix C: Plug and Play (PnP) Connect Portal 175
Procedure 1: Log into the PnP Connect portal 176
Procedure 2: Configure the controller file 176
Procedure 3: Add WAN Edge devices to the portal 178
Download the authorized serial number file 181
Appendix D: vEdge factory default settings 183
Appendix E: Manual upgrade of a WAN Edge router 186
Appendix F: Supporting network device configurations 189
Appendix G: vEdge configuration template summary 198
Shared feature templates 198
Data center feature templates 203
Branch feature templates 208
Data center device template 219
Branch device templates 219
Data center variable values 226
Branch variable values 230
Appendix H: WAN Edge router CLI-equivalent configuration 243
About this guide 287
Feedback & Discussion 287

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. This guide is not meant to exhaustively cover all deployment options. It highlights best practices and assists with a successful configuration and deployment of a Cisco SD-WAN network.

The example SD-WAN network includes one data center with two Cisco vEdge 5000 routers and five remote sites with a mix of Cisco vEdge 1000 routers, Cisco vEdge 100 routers, and Cisco ISR 4351 and 4331 routers running the SD-WAN software image. 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.

Note: Cisco ISR 4000 and 1000 and the Cisco ASR 1000 routers running the SD-WAN software image are also referred to as IOS XE SD-WAN routers. The Cisco IOS XE SD-WAN routers, along with the Cisco vEdge routers are collectively referred to as Cisco WAN Edge routers.

Prerequisites to starting deployment:

- Cisco WAN Edge routers are installed and ready to configure. The IOS XE SD-WAN routers should already be converted from IOS XE to SD-WAN code. See Appendix B for information on the conversion.
- Devices adjacent to the Cisco WAN Edge 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 at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf for background information on the SD-WAN solution.

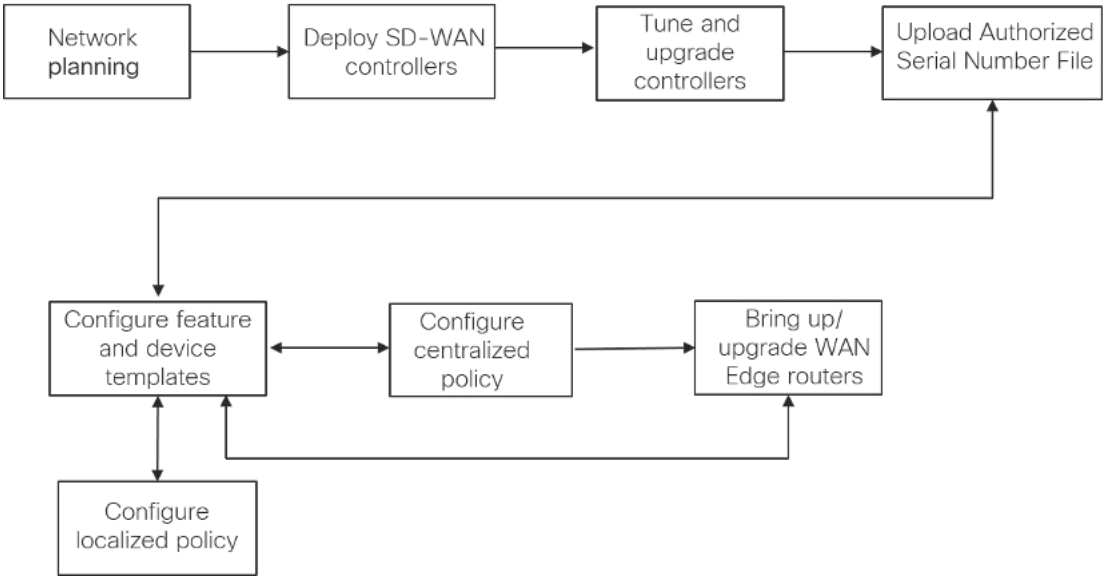
Refer to Appendix A for the hardware models and software versions used in this deployment guide. Refer to Appendix F for portions of the supporting network device configurations. Refer to Appendices G and H for summaries of the configurations for the vEdge devices.

See Design Zone at http://www.cisco.com/go/cvd for additional documentation, including the Cloud onRamp for SaaS Deployment Guide.

SD-WAN deployment overview

In order to have a fully functional SD-WAN 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 WAN Edge device configurations, policies, and code versions; and plan out supporting device configurations, including any firewall ports that must be open to accommodate WAN Edge 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.

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 necessary.

4. Upload the authorized serial number file - The authorized serial number file, which contains the serial and chassis numbers of all WAN Edge routers that are authorized to be in the network, should be uploaded to vManage. Once uploaded or synched to vManage, the file is distributed to the vBond and vSmart controllers. Note that more than one authorized serial number file can be uploaded and the duplicate device entries will be ignored.

5. Configure feature and device templates - Configure feature and device templates and attach them to the WAN Edge devices, supplying variables to parameter values as necessary. vManage builds the full configurations and pushes them out to the WAN Edge 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 WAN Edge 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 WAN Edge routers - Bring up the WAN Edge routers in order to establish control connections to the vBond, vSmart, and vManage devices. This is accomplished either through a manual bootstrap configuration or through an automatic provisioning process. Auto-provisioning includes either the Zero-Touch Provisioning (ZTP) process for vEdge routers or the Cisco Network Plug and Play (PnP) process for IOS XE SD-WAN routers. In addition, upgrade the WAN Edge routers if necessary, which can be performed manually through the vManage GUI or automatically during the auto-provisioning process.

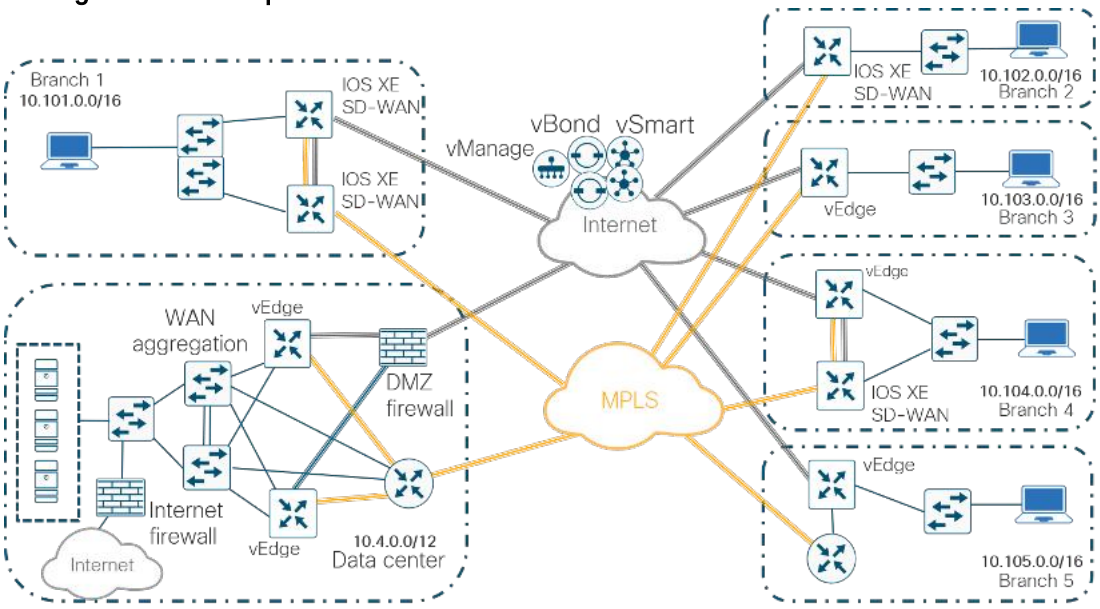
Note that the sequence of the above described steps is flexible, with the following exceptions:

- Network planning and the SD-WAN controller deployment should come first.
- When upgrading to a new code version, the vManage device should be upgraded first, followed by the vBond and vSmart controllers, and then followed by the WAN Edge routers.
- The authorized serial number file needs to be uploaded before any WAN Edge routers are successfully brought online.
- Device templates must be attached to WAN Edge routers in the vManage GUI before bringing them online successfully via the ZTP or PnP 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 topology described 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 WAN Edge 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 WAN Edge routers connect directly to the controllers over the Internet transport. The WAN Edge 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

In the example SD-WAN network, two Cisco vEdge 5000 routers (labeled DC1-WE1 and DC1-WE2) are positioned in the primary data center (see Figure 3).

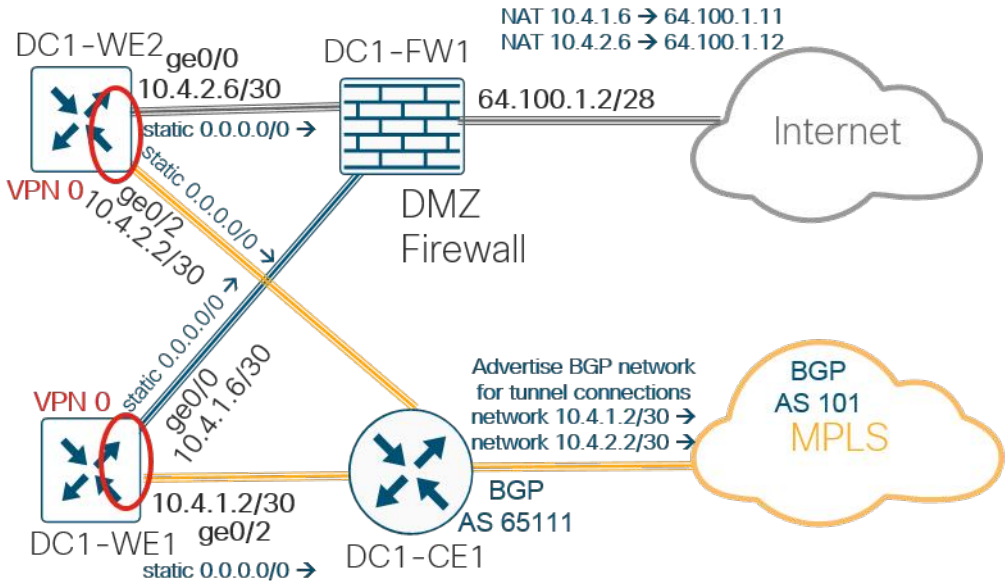
Transport side

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 (labeled DC1-FW1) using a DMZ interface. Each vEdge router's 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 (labeled DC1-CE1), 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 WAN Edge 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.

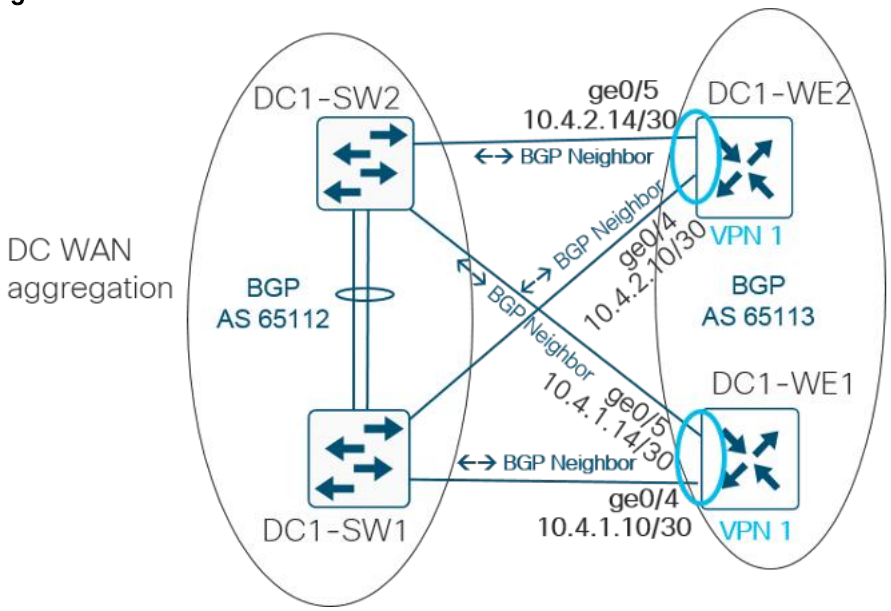
Figure 3 Data center network transport side



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 (labeled DC1-SW1) in the network, while interface ge0/5 connects to data center WAN aggregation switch 2 (labeled DC1-SW2). 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



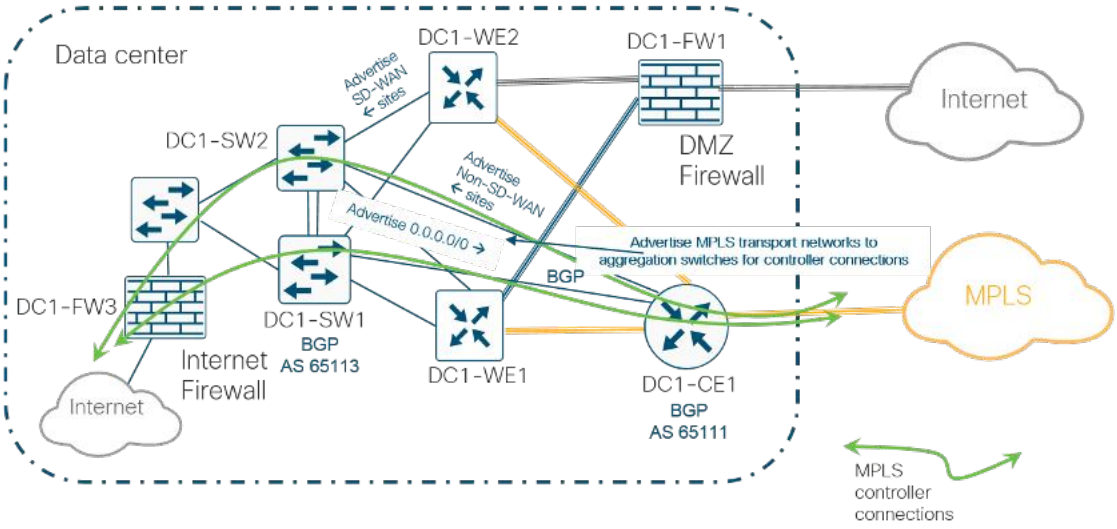
Data center Edge IP addresses

Hostname	ge0/0 Internet	ge0/2 MPLS	ge0/4 DC1-SW1	ge0/5 DC1-SW2
DC1-WE1	10.4.1.6/30	10.4.1.2/30	10.4.1.10/30	10.4.1.14/30
DC1-WE2	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 WAN Edge 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 routing



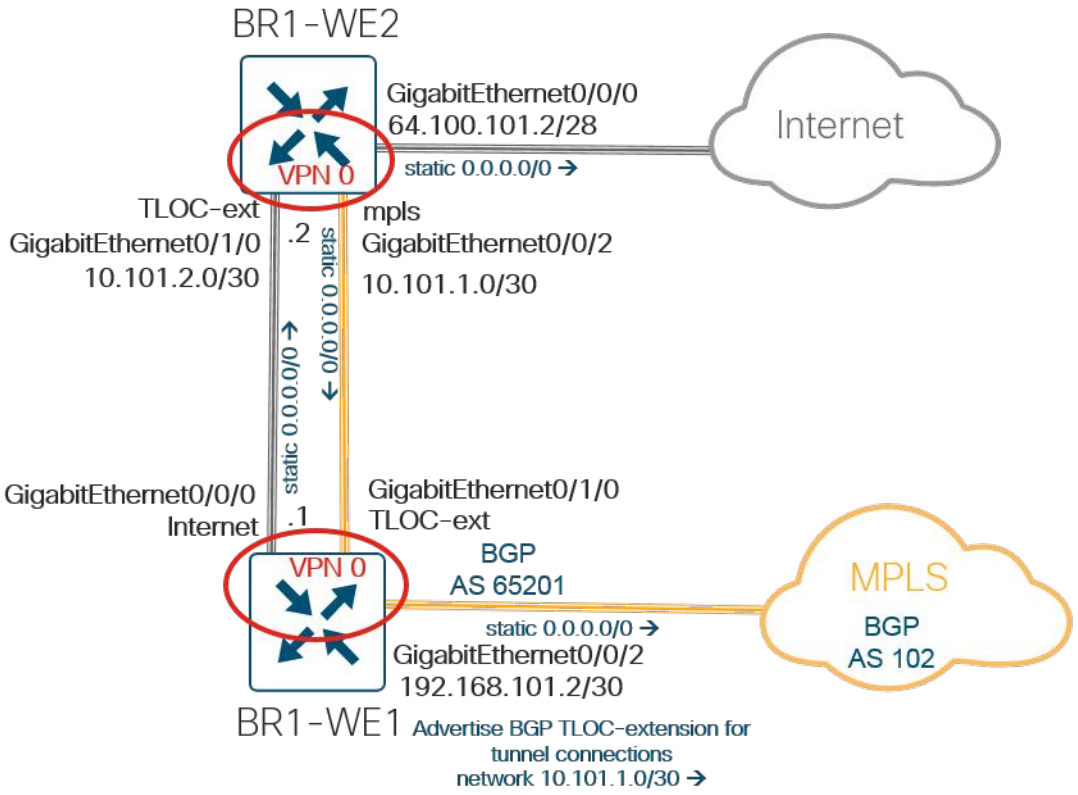
Branch details

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

Transport side

Branch 1 contains two ISR 4351 IOS XE SD-WAN routers, with each router having a direct connection to one of the transport providers. This site has TLOC-extension links between the routers to give each router access to both transports. WAN Edge 1 (labeled BR1-WE1) runs BGP in the transport VPN to communicate the TLOC extension link subnet to the MPLS cloud, so WAN Edge 2 (labeled BR1-WE2) will have reachability to the controllers through the data center and to other WAN Edge routers on the MPLS transport to form IPSec tunnels. On both routers, static default routes pointing to the next-hop gateways are configured for tunnel establishment on the MPLS (GigabitEthernet0/0/2) and Internet (GigabitEthernet0/0/0) links on both WAN Edge 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

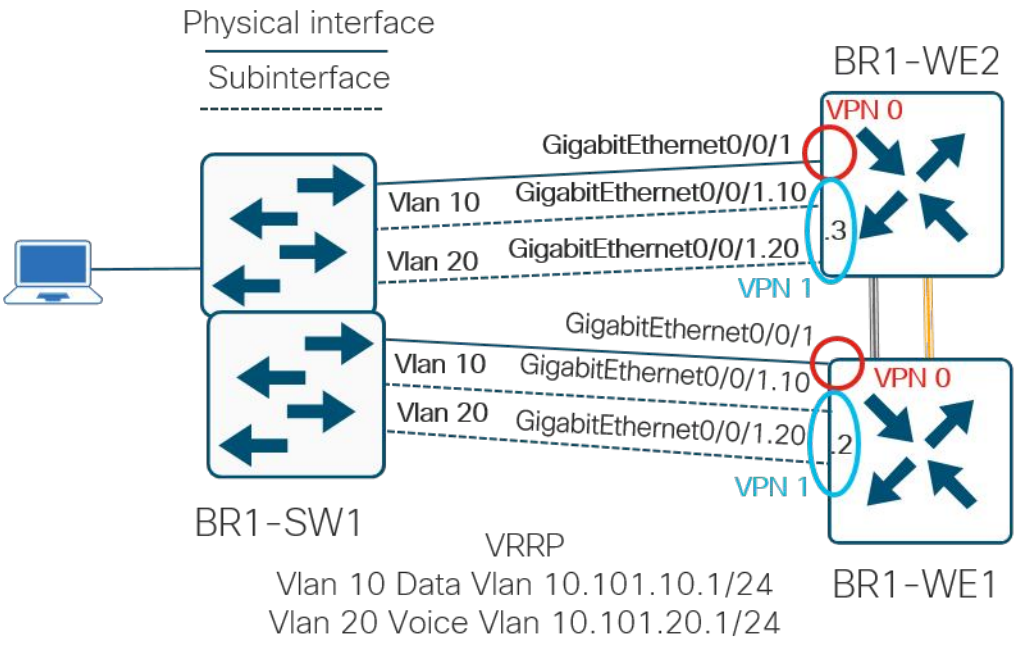


Service side

Each WAN Edge router connects to a stack of LAN switches (labeled BR1-SW1) via a trunk interface. Only one link on each WAN Edge router is attached to a single LAN switch in the stack. This simplifies the design as currently there is no support for channeling or spanning-tree, and if you configure a link from each WAN Edge 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 translate into two different sub-interfaces on each WAN Edge router. The physical link, GigabitEthernet0/0/1, 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 WAN Edge 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 respectively.

Figure 7 Branch 1 service side



Branch 1 Edge IP addresses

Host-name	Gigabit Ethernet0/0/0 Internet	Gigabit Ethernet0/0/2 MPLS	Gigabit Ethernet0/1/0 TLOC Extension	Gigabit Ethernet0/0/1 BR1-SW1 Vlan 10	Gigabit Ethernet0/0/1 BR1-SW1 Vlan 20
BR1-WE1	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-WE2	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 router/Internet DHCP address/layer 2 LAN switch site

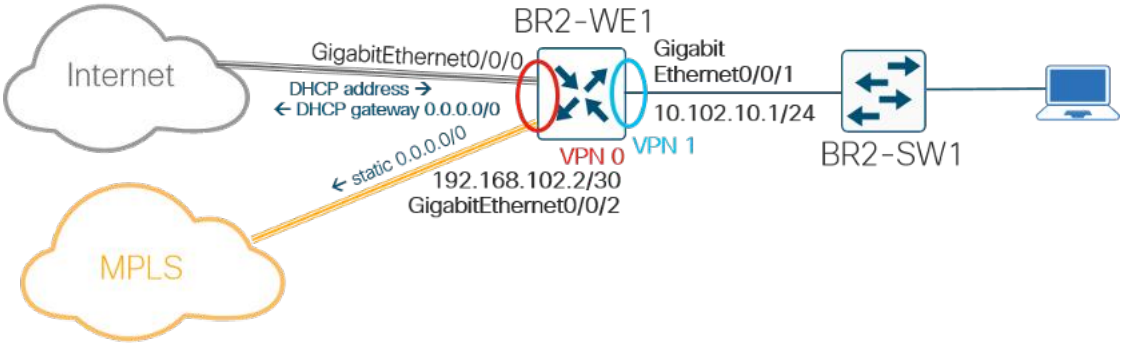
Transport side

Branch 2 contains one Cisco 4331 IOS XE SD-WAN router (labeled BR2-WE1), which connects to both the MPLS and Internet transports. The Internet transport interface (GigabitEthernet0/0/0) 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 (GigabitEthernet0/0/2).

Service side

The WAN Edge router at branch 2 connects to a layer 2 switch (labeled BR2-SW1) using GigabitEthernet0/0/1.

Figure 8 Branch 2 transport and service side



Branch 2 Edge IP addresses

Hostname	GigabitEthernet0/0/0 Internet	GigabitEthernet0/0/2 MPLS	GigabitEthernet0/0/1 BR2-SW1
BR2-WE1	DHCP (64.100.102.x/28)	192.168.102.2/30	10.102.10.1/30

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

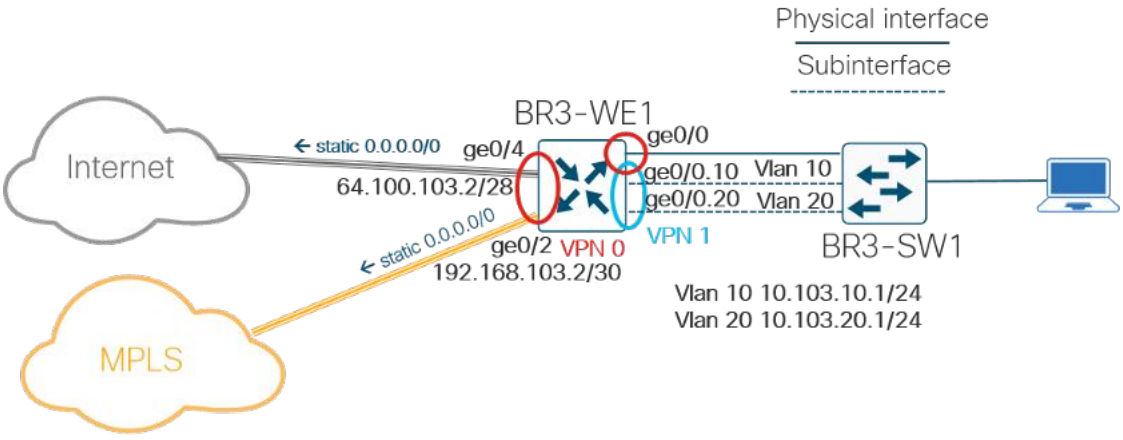
Transport side

Branch 3 contains one vEdge 100b router (labeled BR3-WE1), 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 (labeled BR3-SW1). 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



Branch 3 Edge IP addresses

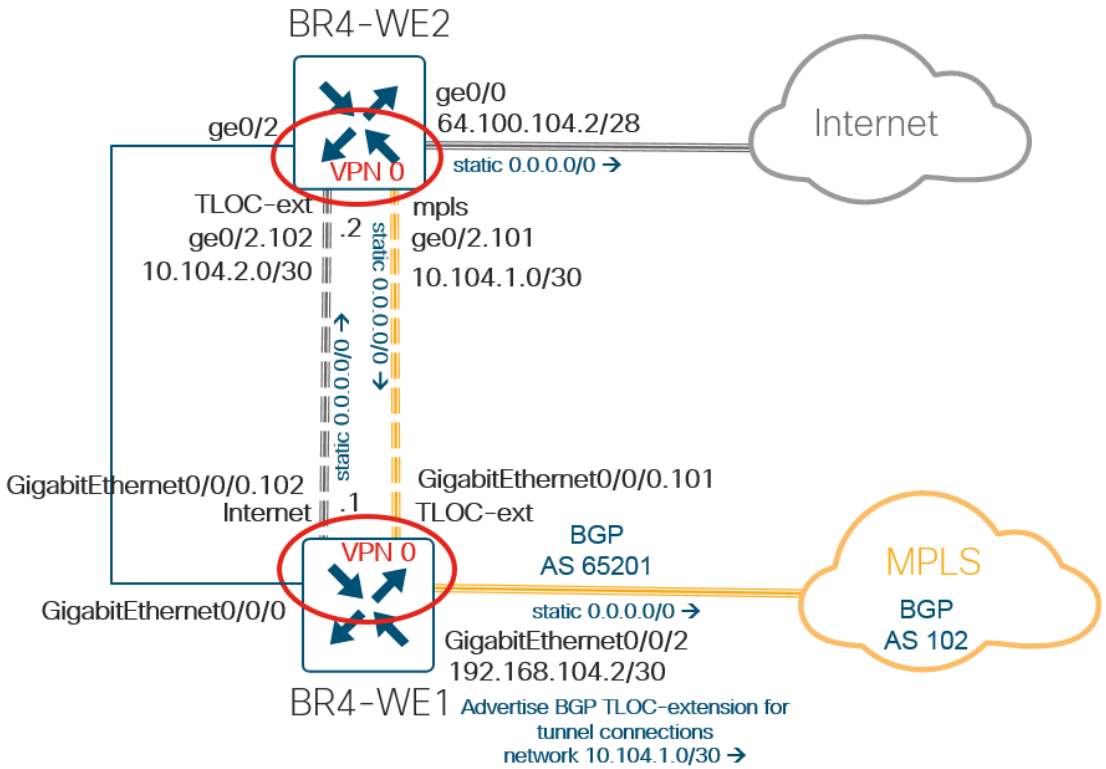
Hostname	ge0/4 Internet	ge0/2 MPLS	ge0/0 BR3-SW1 Vlan 10	ge0/0 BR3-SW1 Vlan 20
BR3-WE1	64.100.103.2/28	192.168.103.2/30	10.103.10.1/24	10.103.20.1/24

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

Transport side

Branch 4 contains a Cisco vEdge 1000 router directly connected to an Internet service provider and a Cisco ISR4351 IOS XE SD-WAN router directly connected to an MPLS service provider. This site has a TLOC-extension link between the two WAN Edge routers to give each WAN Edge router access to both transports. The TLOC-extension link utilizes sub-interfaces. The IOS XE SD-WAN router (labeled BR4-WE1) runs BGP in the transport VPN to communicate the TLOC extension link subnet to the MPLS cloud, so the vEdge router (labeled BR4-WE2) will have reachability to the controllers through the data center and to other WAN Edge routers on the MPLS transport to form IPSec tunnels. On both WAN Edge routers, static default routes pointing to the next-hop gateways are configured for tunnel establishment on the MPLS and Internet 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 on WAN Edge 1 and WAN Edge 2, as well as the sub-interfaces, are configured in VPN 0.

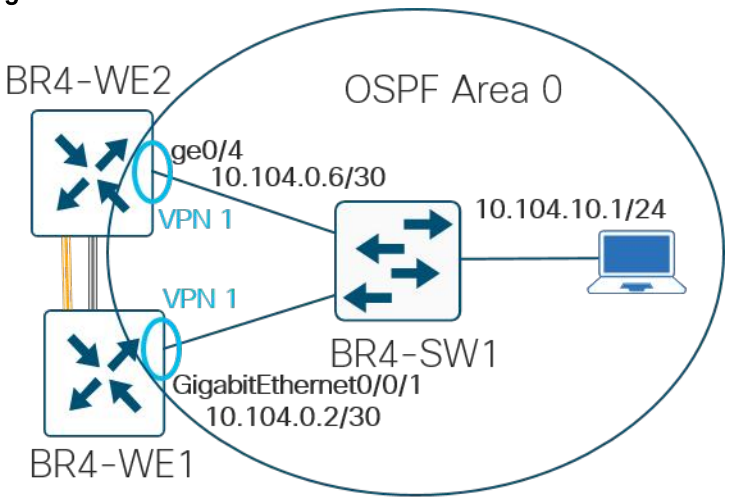
Figure 10 Branch 4 transport side



Service side

Branch 4 has two WAN Edge routers connected to a layer 3 switch (labeled BR4-SW1) and running Open Shortest Path First (OSPF) between them. All devices are in area 0. The router interfaces are configured for OSPF network point to point on each interface to the layer 3 switch.

Figure 11 Branch 4 service side



Branch 4 Edge 1 IP addresses

Host-name	Gigabit Ethernet0/0/0.102 Internet	Gigabit Ethernet0/0/2 MPLS	Gigabit Ethernet0/0/0.101 TLOC Extension	Gigabit Ethernet0/0/1 BR4-SW1
BR4-WE1	10.104.2.1/30	192.168.104.2/30	10.104.1.1/30	10.104.0.2/30

Branch 4 Edge 2 IP addresses

Host-name	ge0/0 Internet	ge0/2.101 MPLS	ge0/2.102 TLOC Extension	ge0/4 BR4-SW1
BR4-WE2	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

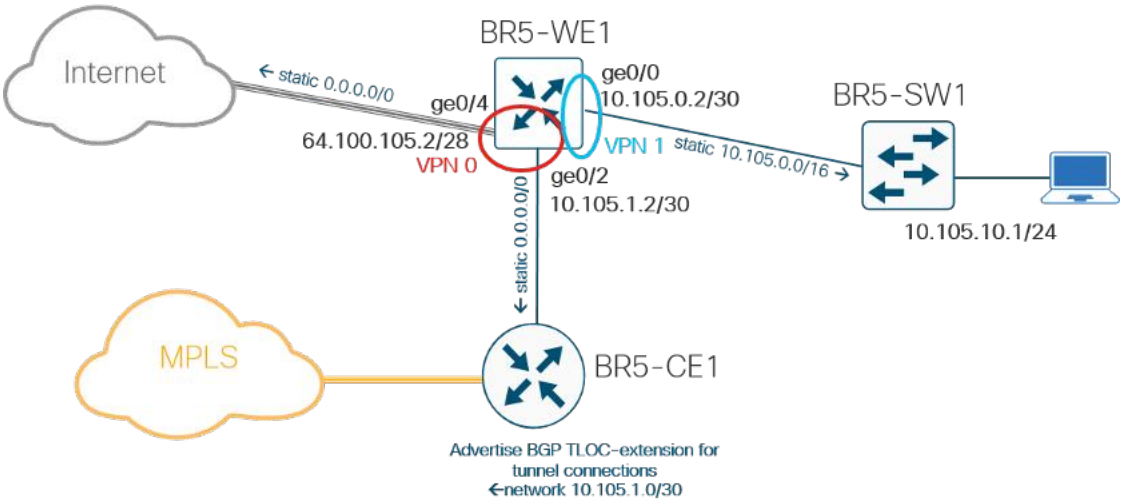
Transport side

Branch 5 has a single vEdge 100b (labeled BR5-WE1) directly connected to the Internet transport and is also connected to a CE router (labeled BR5-CE1), 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 WAN Edge 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 (labeled BR5-SW1) and there is static routing between the LAN switch and the vEdge router.

Figure 12 Branch 5 transport and service side



Branch 5 Edge IP addresses

Host-name	ge0/4 Internet	ge0/2 MPLS	ge0/0 BR5-SW1
BR5-WE1	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. PnP is not limited to a specific port on the IOS XE SD-WAN routers.

Port numbering scheme

WAN Edge Model	Internet	MPLS	LAN	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
ISR4351 IOS XE SD-WAN	Gigabit Ethernet0/0/0	Gigabit Ethernet0/0/2	Gigabit Ethernet0/0/1	Gigabit Ethernet0/1/0
ISR 4331 IOS XE SD-WAN	Gigabit Ethernet0/0/0	Gigabit Ethernet0/0/2	Gigabit Ethernet0/0/1	--

System IP addresses and site IDs

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.

Six-digit site ID example

Hostname	GigabitEthernet0/0/0 Internet	GigabitEthernet0/0/2 MPLS
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

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.

Example network site IDs and system IP addresses

Hostname	Location	Site ID	System IP
DC1-WE1	Datacenter 1/West	110001	10.255.241.101
DC1-WE2	Datacenter 1/West	110001	10.255.241.102
BR1-WE1	Branch 1/West	112001	10.255.241.11
BR1-WE2	Branch 1/West	112001	10.255.241.12
BR2-WE1	Branch 2/West	111002	10.255.241.21
BR3-WE1	Branch 3/West	113003	10.255.241.31
BR4-WE1	Branch 4/East	122004	10.255.242.41
BR4-WE2	Branch 4/East	122004	10.255.242.42

Hostname	Location	Site ID	System IP
BR5-WE1	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.

Universal design parameters

Hostname	Location
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, SNMP 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

Deployment details

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 cover:

- Tuning controller configurations – This covers verifying that the controllers are up and modifying their configurations for best practices. It also includes uploading the authorized serial file.
- Preparing for software upgrades and upgrading the controllers.
- Deploying the data center WAN Edge routers - This covers the bootstrapping of the WAN Edge routers to get them connected to the controllers, code upgrades, device and feature template configurations, and localized policy.
- Deploying the remote site WAN Edge routers - This covers the ZTP and PnP process in getting the WAN Edge 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).

Tuning controller configurations

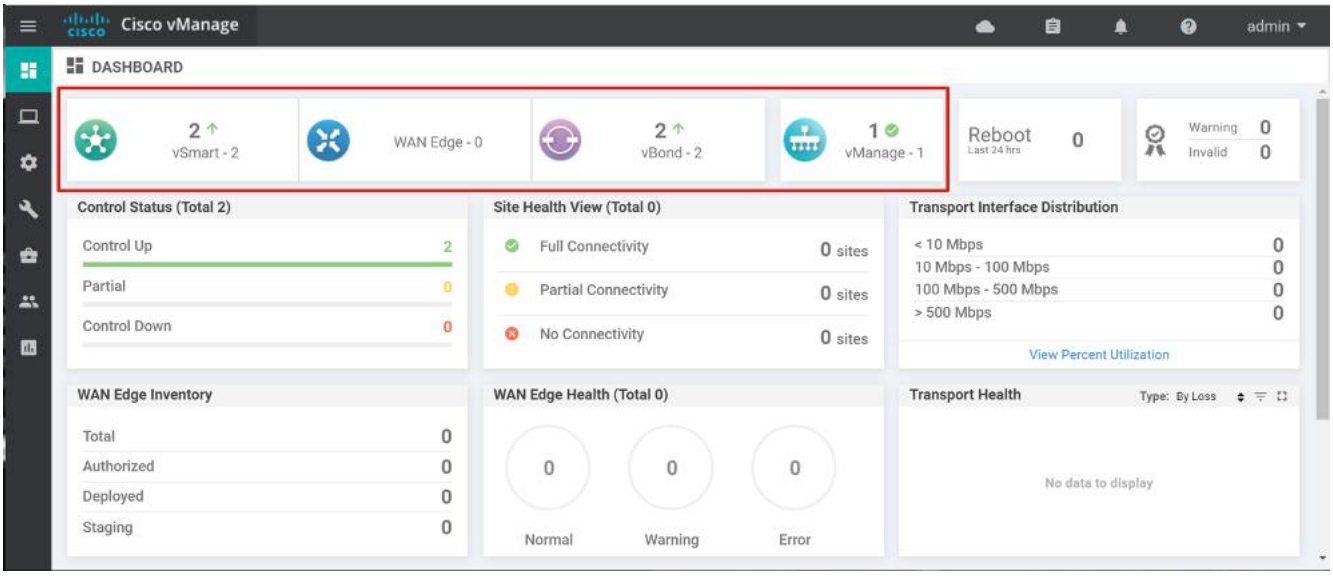
The controllers in this deployment consist of a vManage, two vSmart controllers, and two vBond orchestrators. The vManage and vBond orchestrators are in Command-Line Interface (CLI) mode while the vSmart controllers are in vManage mode using CLI-based templates. The vManage and vBond orchestrators can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

1. Access the vManage web instance by using a web browser. For example: *https://vmanage1.cisco.com:8443/*
2. Log in with your username and password credentials.
3. The vManage dashboard will be displayed. At the top, a status indicating reachability will be displayed for all vSmart controllers, vEdge routers, and vBond orchestrators that are installed and added to vManage. Verify the controllers are all showing up before proceeding. The number of

controllers will be shown with a green up arrow (indicating reachable), or a red down arrow (indicating unreachable).

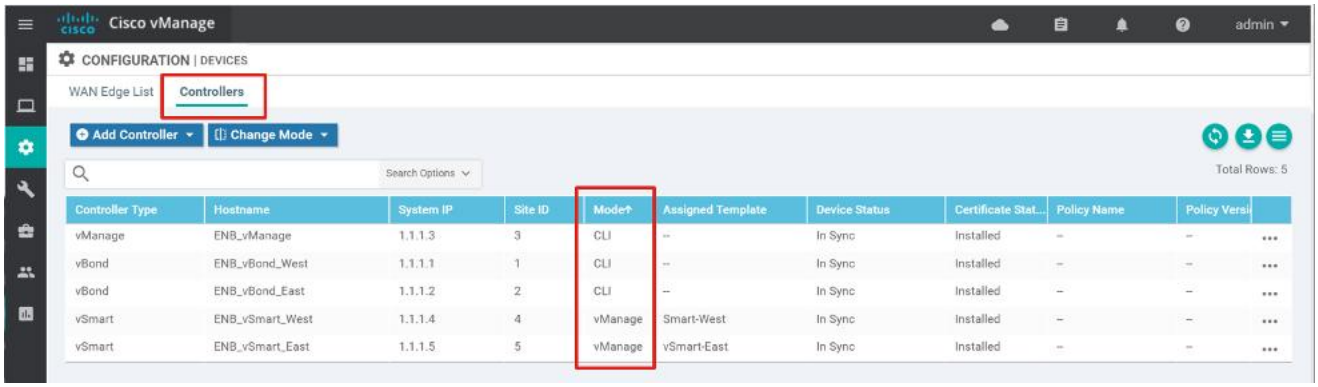


Procedure 2: Determine controller configuration mode

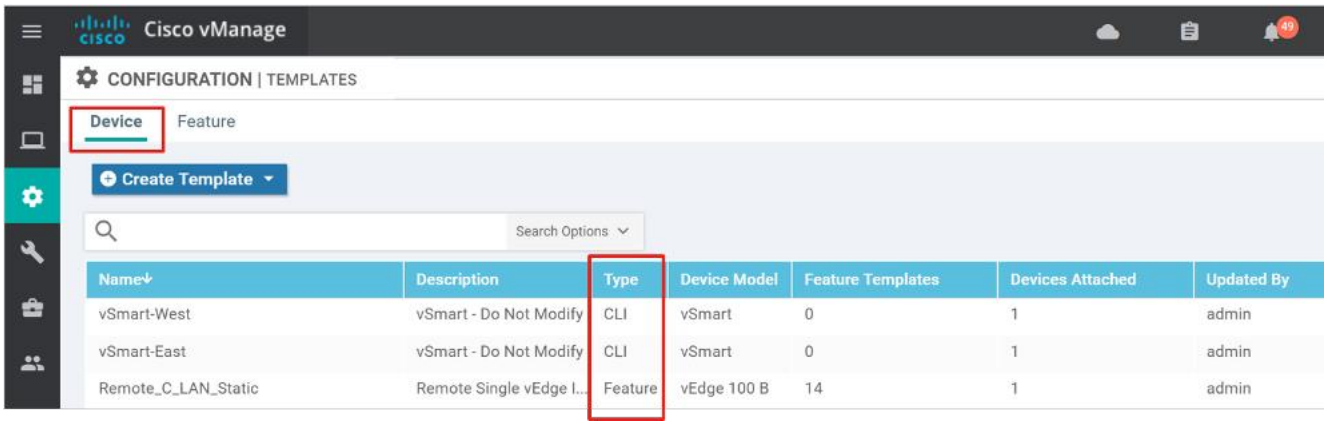
To determine the controller configuration mode, follow these steps:

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

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



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 configuration settings that you may want to modify are:

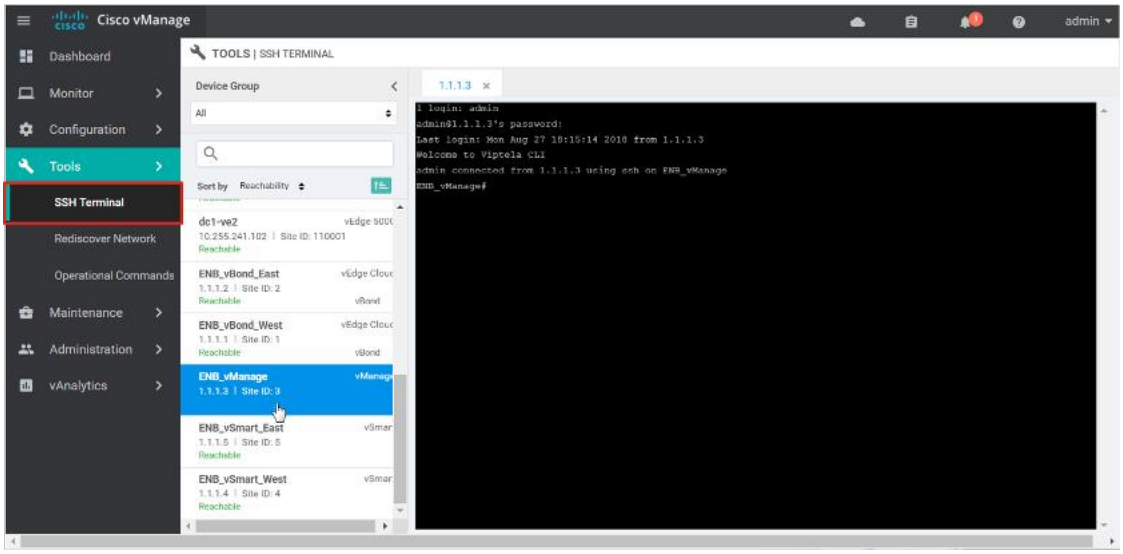
- Admin password (all controllers) - You may want to change the admin password for the controllers if you are using local authentication.
- TLS (vSmart controllers and vManage) - If possible, run Transport Layer Security (TLS) as the security protocol between vEdge and the controllers and between controllers.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

Tech tip: Note that changing the security protocol of the controllers can be extremely disruptive. The current sessions will be disrupted, so configure with caution.

- 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. When you enable 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.

To modify the configuration settings, follow these steps:

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. Select the vManage controller. An SSH window will come up in the main panel. Enter the username and password.



2. On the vManage controller, change the admin password and enable TLS by entering the following:

```
config terminal
system
 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.

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.

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

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

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. Here is a configuration snippet:

```
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.

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



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.

9. Select Update.

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

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

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

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

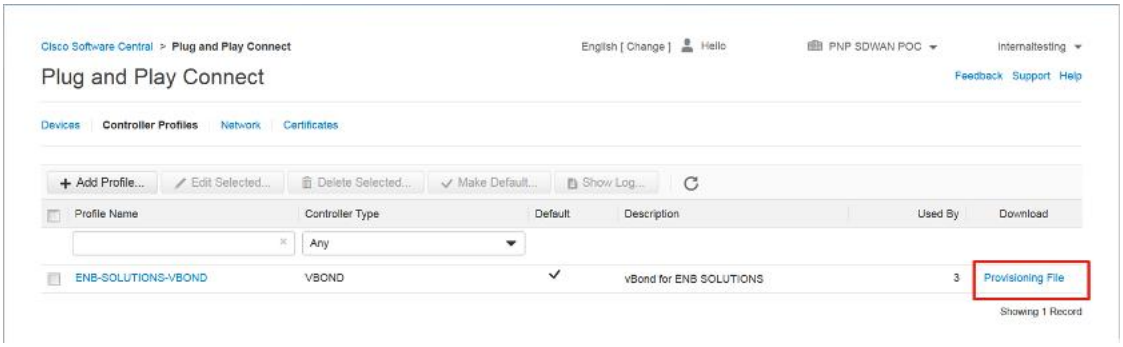
Procedure 4: Retrieve the authorized WAN Edge serial number file

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

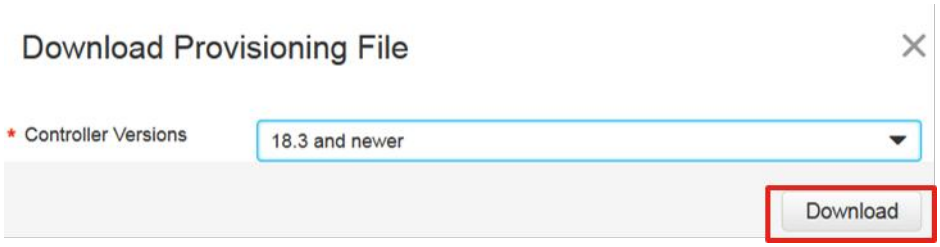
The legacy authorized serial number files for vEdge routers were located at the Cisco SD-WAN support website, but these files are now migrated to the Plug and Play (PnP) Connect portal. The authorized serial number file on the PnP Connect portal also contains IOS XE SD-WAN router information. See Appendix C for information on how to add any WAN Edge devices to the portal if needed before downloading the authorized serial number file. Note that you can upload mulitple authorized serial number files to vManage and the duplicates should be filtered.

PnP Connect portal

1. Navigate to https://software.cisco.com.
2. Under the Network Plug and Play section, click Plug and Play Connect.
3. Ensure the correct virtual account is chosen in the top right corner.
4. Click on Controller Profiles.
5. Next to the correct controller profile (ENB-SOLUTIONS-VBOND), click on the Provisioning File text.



6. In the pop-up window, select the controller versions from the drop-down box. Choose 18.3 and newer. Click Download and save the file to your computer. It is saved as serialFile.viptela by default.



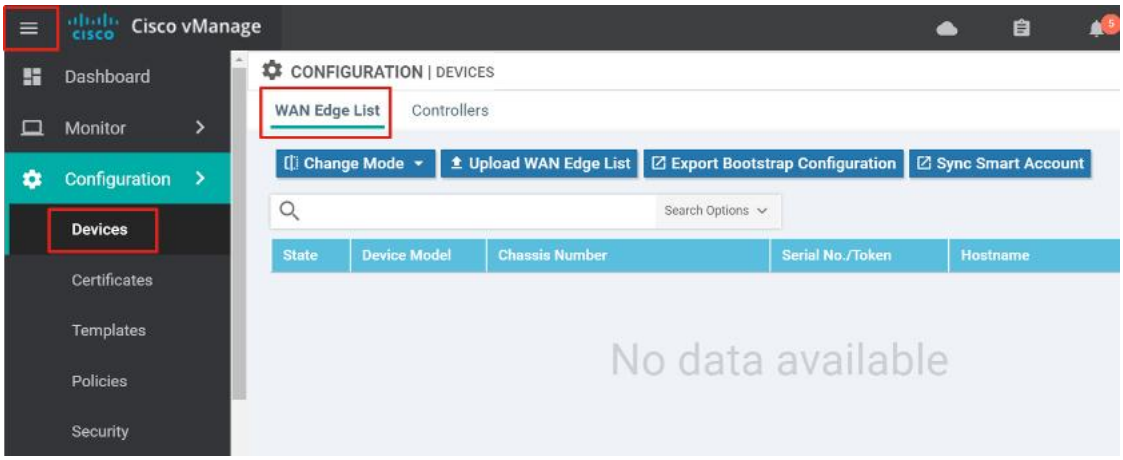
Procedure 5: Load the authorized WAN Edge serial number file

There are two ways to load the WAN Edge serial number file into vManage:

- Manually load the list into vManage
- Sync to the Smart Account on the PnP Connect portal from vManage

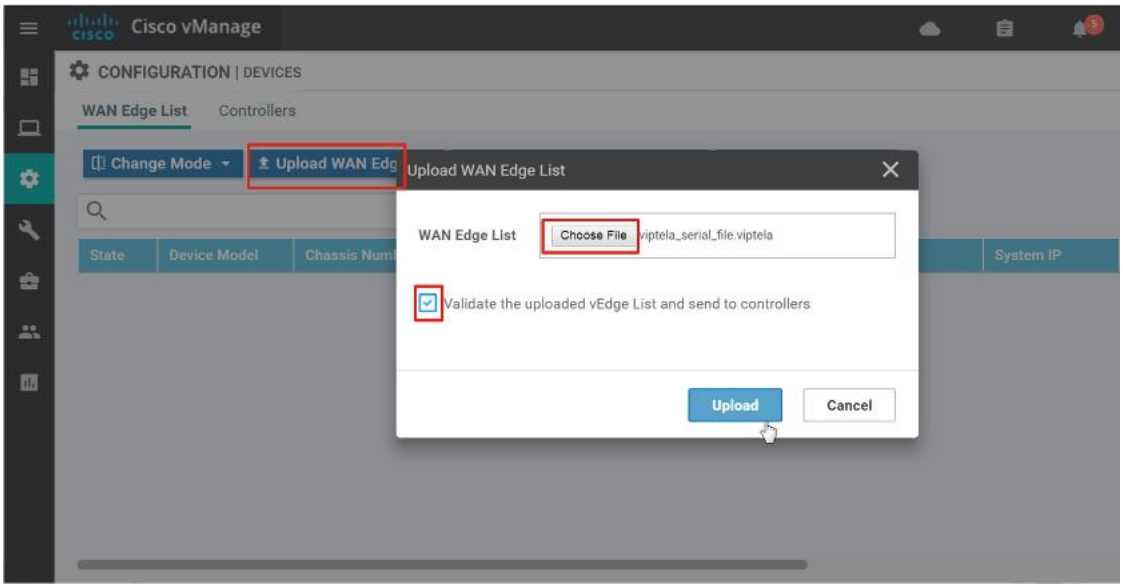
Manually load the list

1. In the vManage GUI, go to Configuration>Devices in the left pane, or alternatively, expand the left pane by selecting the three horizontal bars in the top left corner of the GUI, then select Configuration>Devices. Ensure the WAN Edge List tab is selected.



2. Select the Upload WAN Edge List button. A pop-up window appears. Select Choose File. Browse for and select the serial number file. Select Open.

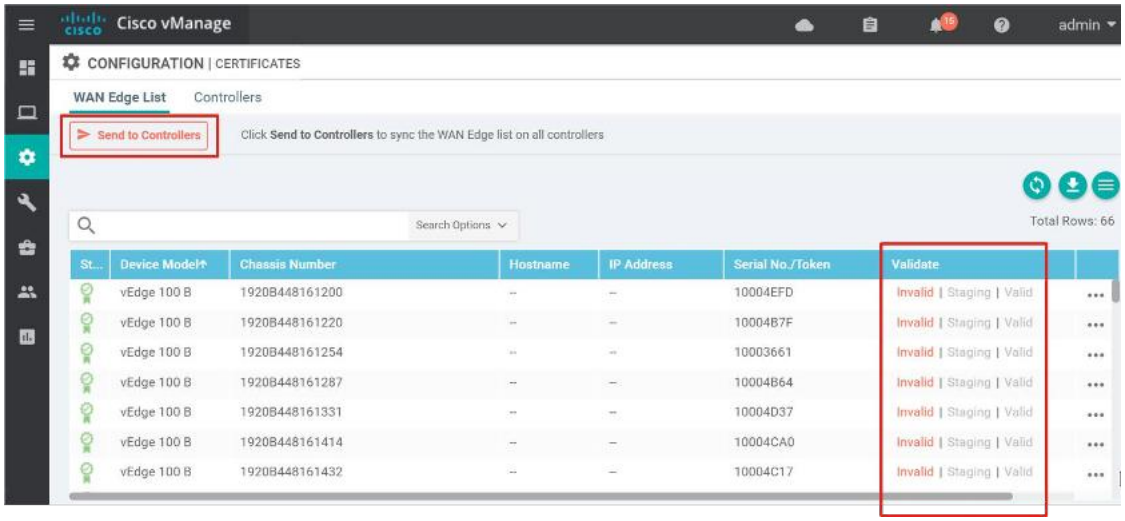
3. Now that the file is selected, select the check box in order to validate the list and send it to the controllers. Select the Upload button. If you select the check box, this will put all the devices on the list into a valid state, which means they can be brought up at any time on the network and start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



4. Select OK in the confirmation box that appears.

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

6. If you did not select the check box to validate the uploaded list to send to the controllers, you can go to Configuration>Certificates, ensure the WAN Edge 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 WAN Edge routers to all of the controllers. A page will indicate that the list has been successfully pushed out to the vBond and vSmart controllers. All devices will be in an invalid state.

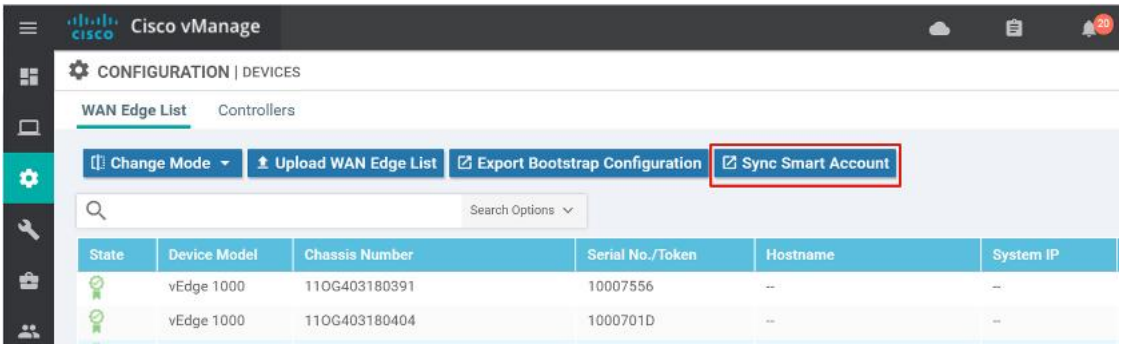


Sync to the Smart Account

Starting from version 18.3, vManage has a Sync Smart Account option, which allows vManage to automatically connect to the PnP Connect portal and pull down the authorized WAN Edge serial number file.

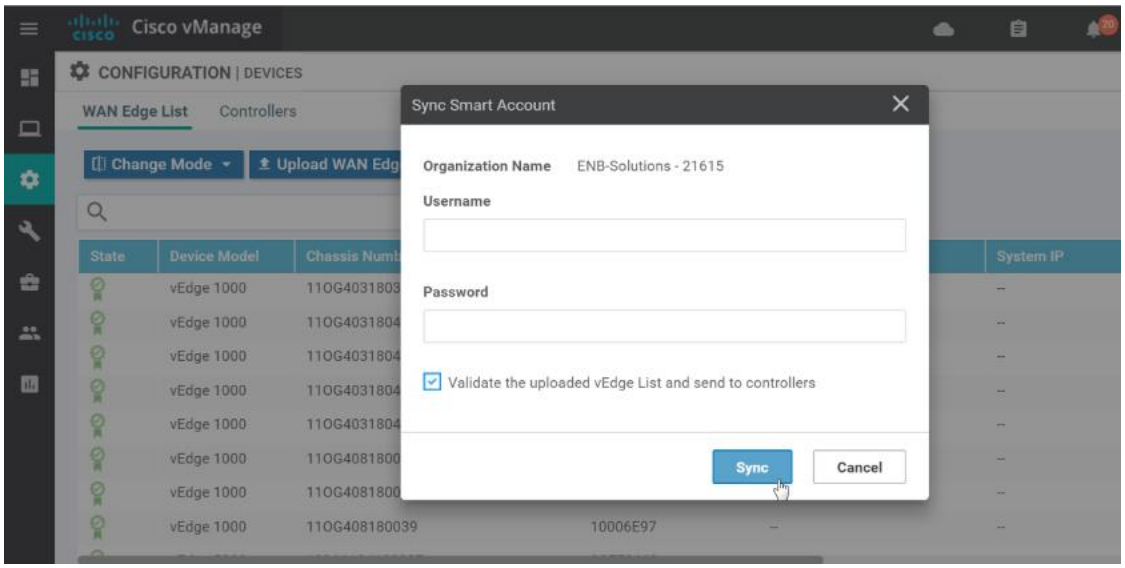
1. In the vManage GUI, go to Configuration>Devices, and ensure the WAN Edge List tab is selected.

2. Click on Sync Smart Account and a window pops up which prompts you for your Username and Password.



3. Enter your username and password for the Cisco website. The checkbox which validates the uploaded list is selected by default. Note that the list still needs to be distributed to the other controllers once synced with vManage even if the checkbox was selected.

4. Click Sync. vManage uses SSL to connect to the Cisco servers and the authorized list is downloaded using REST APIs.



5. Go to Configuration>Certificates in vManage to view the uploaded list. The devices should all be in a valid state.

6. Click the Send to Controllers button in the top left corner of the GUI in order for all of the controllers to be updated with the valid WAN Edge list. Once completed, the operation should indicate success.

Preparing for software upgrades and upgrading the controllers

SD-WAN Software may be downloaded from https://software.cisco.com, or more specifically, https://software.cisco.com/download/home/286320954.

The following are the file naming conventions for the SD-WAN products.

SD-WAN File Naming Conventions

Hostname	Location
ASR1000	asr100xx-ucmk9.16.9.3.SPA.bin
ISR1000	c1100-ucmk9.16.9.3.SPA.bin
ISR4000	isr4x00-ucmk9.16.9.3.SPA.bin
vEdge 100/vEdge 1000/vEdge 2000	viptela-18.3.4-mips64.tar.gz
vSmart/vBond/vEdge Cloud/vEdge 5000	viptela-18.3.4-x86_64.tar.gz
vManage	vmanage-18.3.4-x86_64.tar.gz

When moving to a particular code version, it is important to first upgrade code on the vManage, then on the controllers (vBonds, vSmarts), and lastly, on the WAN Edge routers. Ensure vManage and the controllers are

at the proper code version before bringing the WAN Edge routers onto the targeted code version. The WAN Edge routers can be upgraded once online or as a last part of the ZTP or PnP 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 router 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 WAN Edge 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 WAN Edge routers into the first upgrade group. In dual WAN Edge sites, put each router into a different upgrade group and do not upgrade both of them at the same time. All WAN Edge routers in an upgrade group can be upgraded in parallel (up to 32 WAN Edge 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 WAN Edge 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.

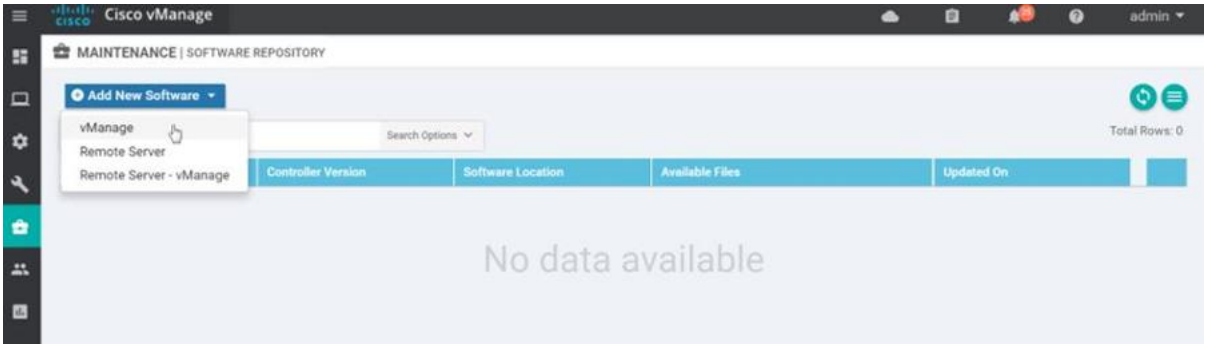
When upgrading using vManage, you can upgrade using a code image that is directly loaded onto vManage or a remote vManage, and you can also upgrade using a code image located on a remote file server.

Procedure 1: Prepare and configure vManage for software upgrades

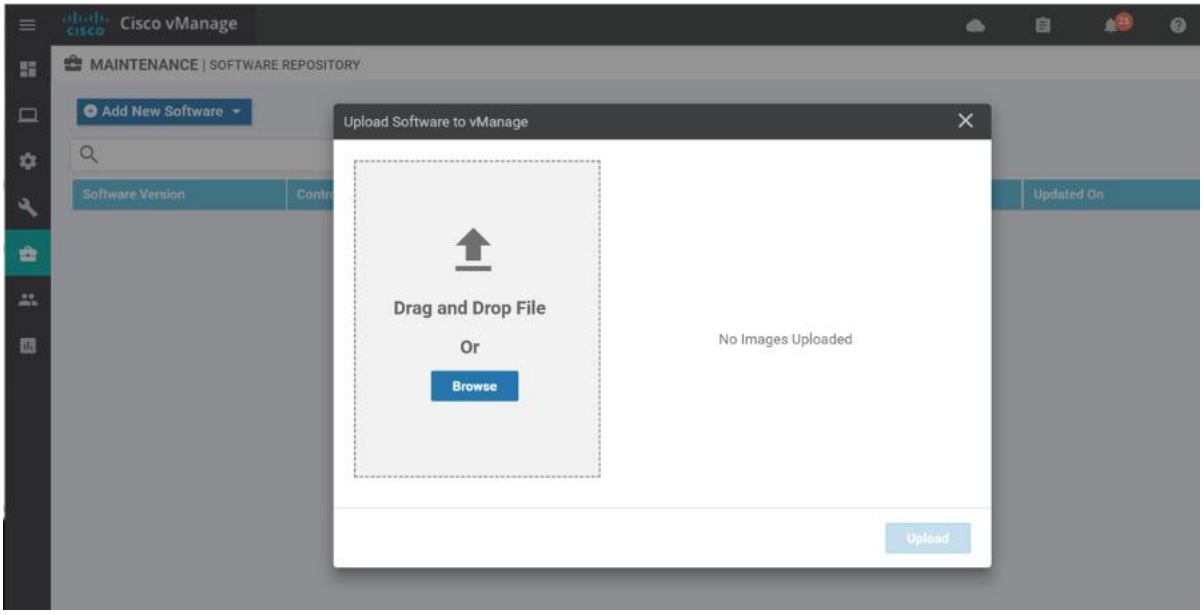
In this procedure, software for any controller and WAN Edge router is uploaded to vManage and a remote file server and the vManage software repository is configured and prepared for upgrading devices. The data center device upgrades will be performed with a remote server, while other devices will be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

1. Go to Maintenance > Software Repository. The repository stores the image locally on vManage, or indicates where to retrieve it in the case of a remote file server or remote vManage.

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

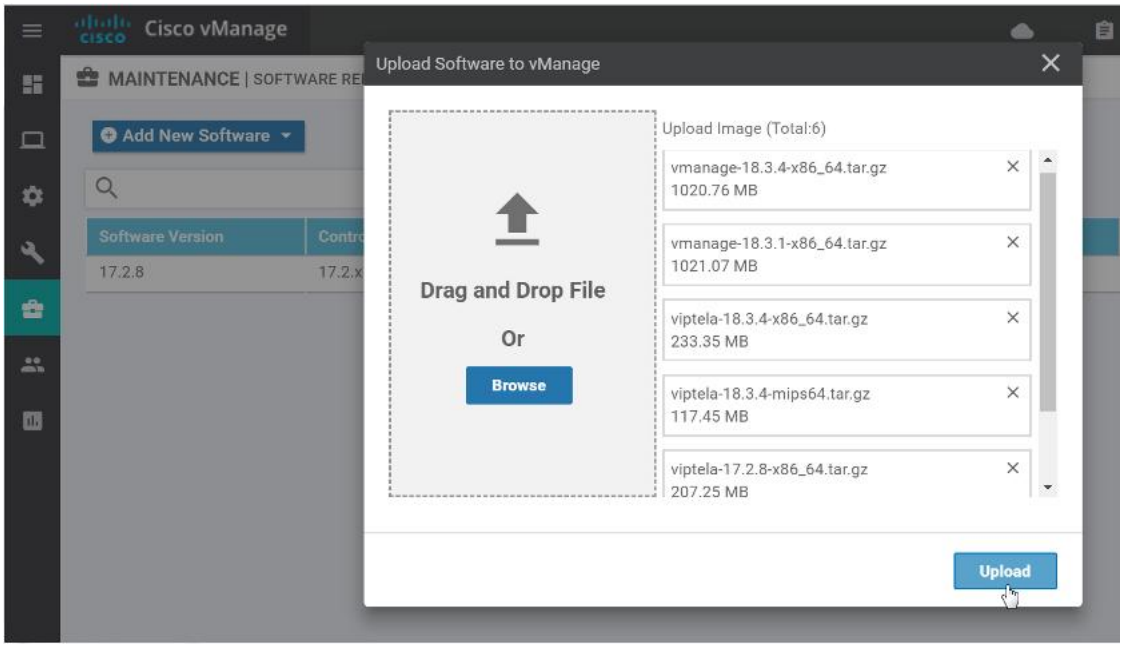


3. Select vManage. A window will appear prompting you to drop an image file or browse for an image on the local computer.



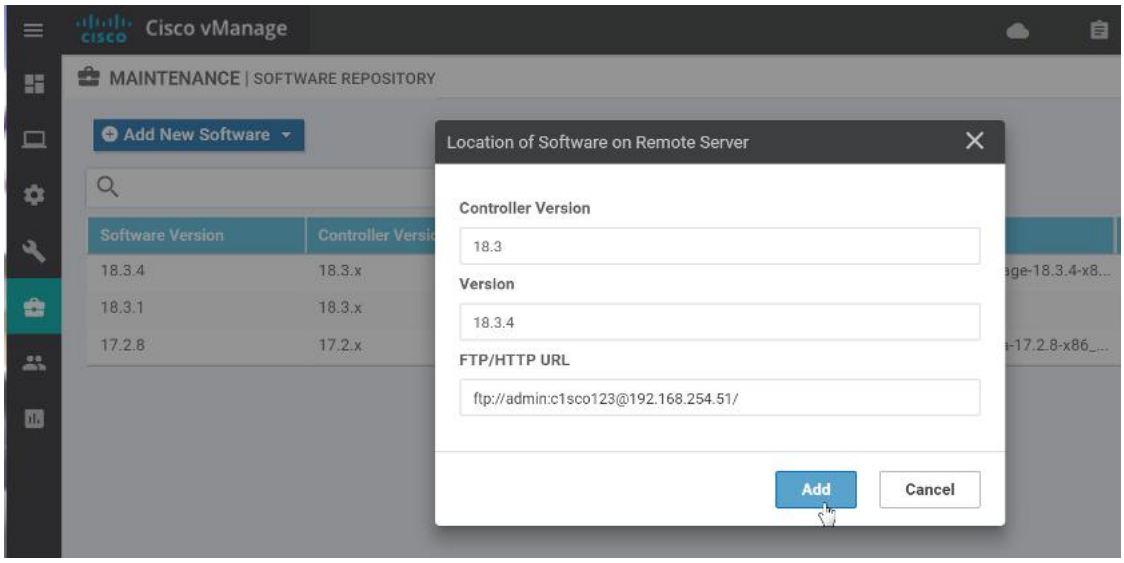
4. Load the desired images into the window, either by dropping them or clicking the Browse button to select them.

5. Click the Upload button.



A window will indicate that the code versions are being loaded to the vManage. Once completed, a message will indicate the images were uploaded successfully, and the version, software location (vmanage), and available files will be added to the repository.

6. 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. Go to Maintenance>Software Repository. Click Add New Software, then select Remote Server from the drop-down menu. A window will pop up. Fill in the Controller version (18.3), the code version of the image (18.3.4) and the FTP or HTTP URL of the file server, including authentication if needed (ftp://admin:c1sco123@192.168.254.51/). Click Add. The controller version, software 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.

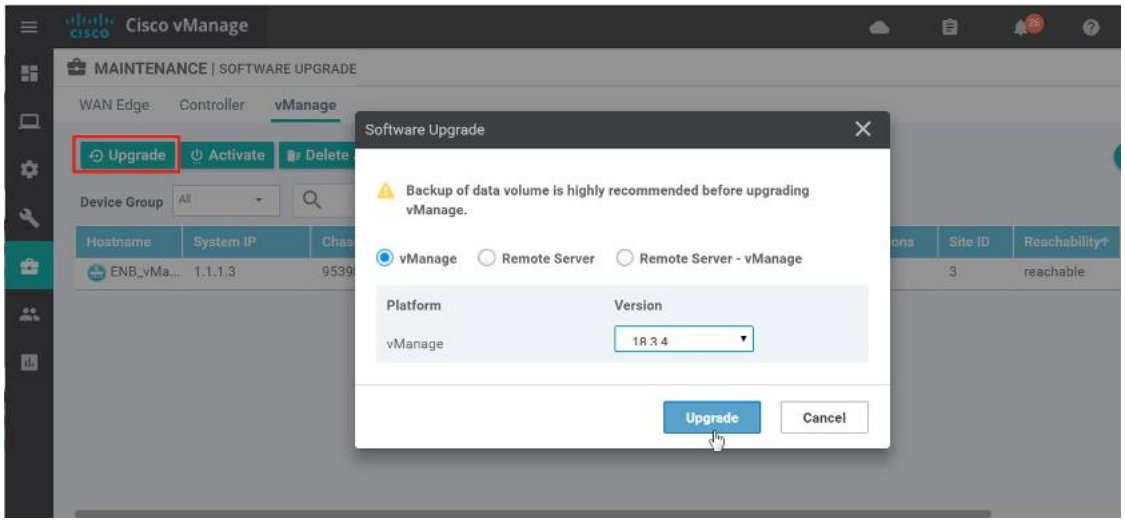
Review the release notes before upgrading: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/Release_Notes/Release_Notes_for_IOS_XE_SD-WAN_Release_16.9_and_SD-WAN_Release_18.3#Upgrade_to_SD-WAN_Software_Release_18.3

Tech tip: Once upgraded, It is not possible to downgrade vManage to a lower major release. For example, if you are running an 18.3.x release, you cannot downgrade to an 18.2,x or lower release. While you can install a lower code version onto the vManage server, you will not be able to activate it.

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

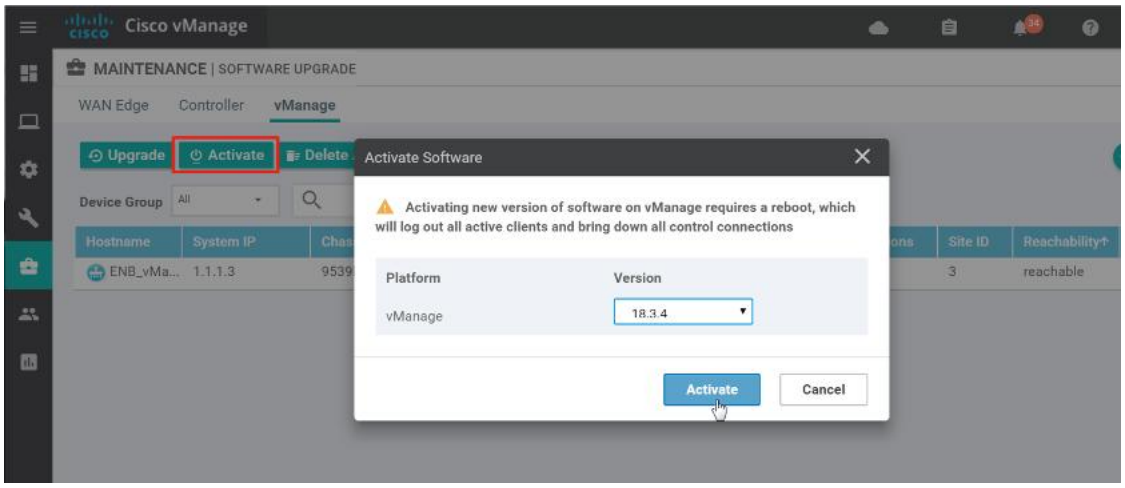
2. Select the Upgrade button in the upper left part of the page. This will cause the software to install, but vManage will not reboot and load the new software until the Activate button is used.

3. A window pops up. Choose the desired software (18.3.4) from the drop-down box. Loading the image from vManage is the default. Select Upgrade.



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

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 (18.3.4) from the drop-down box and select Activate.



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

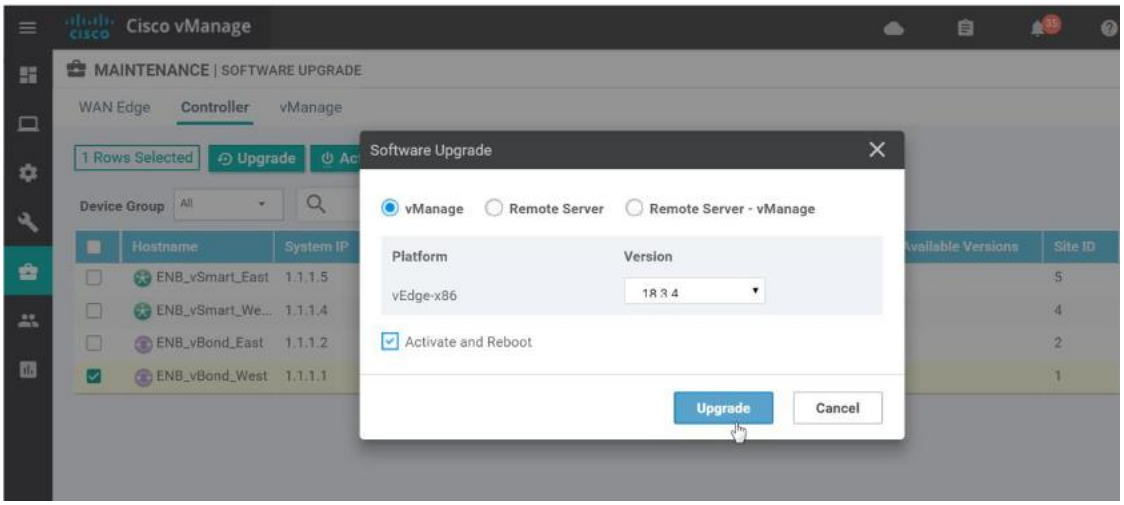
In this procedure, the controllers are upgraded directly from an image on the vManage.

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

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.

3. A window pops up. Choose the software version (18.3.4) and leave the vManage radio button selected.

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.



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

Deploying the data center WAN Edge routers

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

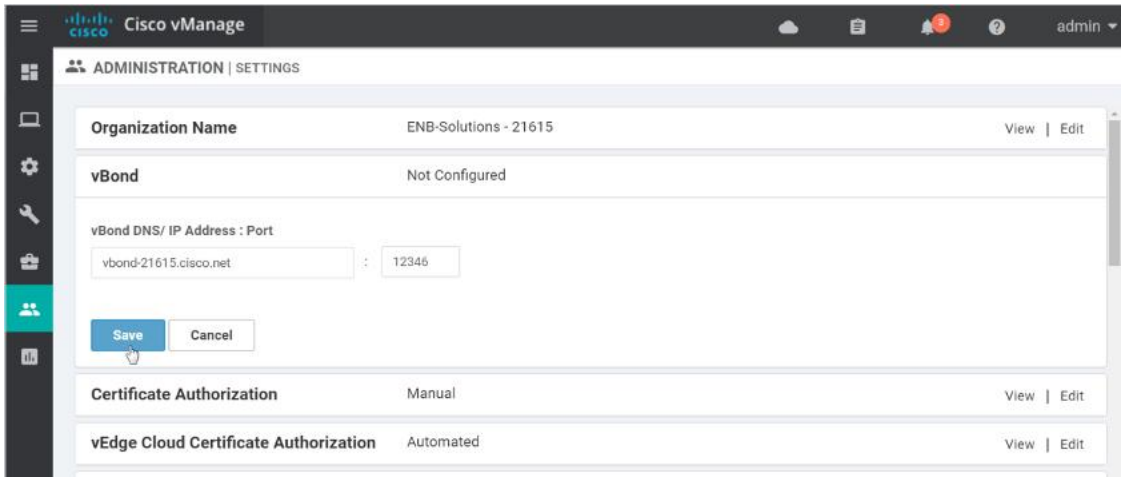
Even though ZTP can be performed, the vEdge routers in the data center will be manually bootstrapped for connectivity to the vBond orchestrator.

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 WAN Edge 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.

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*.

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 WAN Edge routers in staging state (optional)

Before bringing the WAN Edge 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 WAN Edge 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.

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 router itself, or by executing a show hardware inventory on the vEdge router console:

```
vedge# show hardware inventory

hardware inventory Chassis 0

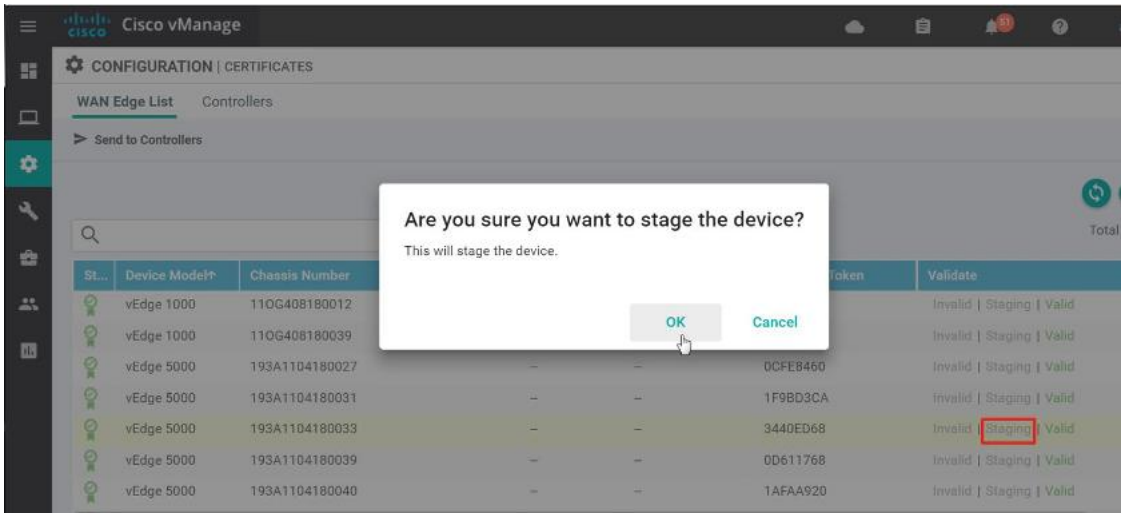
 version         1.1

 part-number     vEdge-5000

 serial-number   193A1104180033

 hw-description "vEdge-5000. CPLD rev: 0x0, PCB rev: A."
```

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.



3. Repeat step 2 for the other vEdge router.

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

Procedure 3: Configure the WAN Edge router via CLI to connect to the controllers

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

Tech tip: 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. If you have issues, you can manually upgrade the vEdge router to at least 17.2.8 or greater before attempting to bring the vEdge onto the network. See Appendix E for manual upgrade steps.

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 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
  tunnel-interface
   encapsulation ipsec
```

```
   color biz-internet
vpn 512
interface mgmt0
ip address 192.168.255.167/23
commit and-quit
```

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
```

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 the following CLI:

```
config t
system
 host-name dc1-we1
 system-ip 10.255.241.101
 site-id 110001
 organization-name "ENB-Solutions - 21615"
 vbond vbond-21615.cisco.net
commit and-quit
```

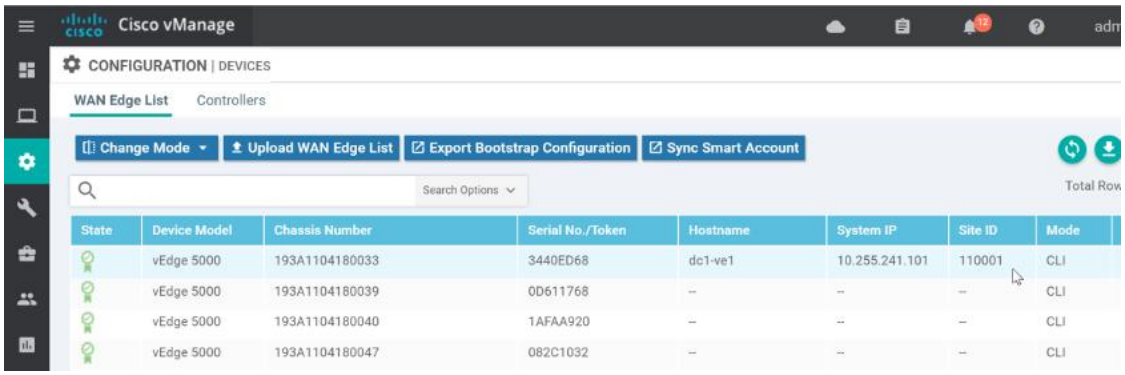
5. Verify the control connections. A show control summary will initially show four connections–one to the vBond orchestrator, one to vManage and one to each of the vSmart controllers. Then the vBond connection will terminate and connections to vManage and the vSmart controllers remain up.

```
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.



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
  tunnel-interface
   encapsulation ipsec
   color biz-internet
vpn 512
interface mgmt0
ip address 192.168.255.168/23
system
 host-name dc1-we2
 system-ip 10.255.241.102
 site-id 110001
 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.

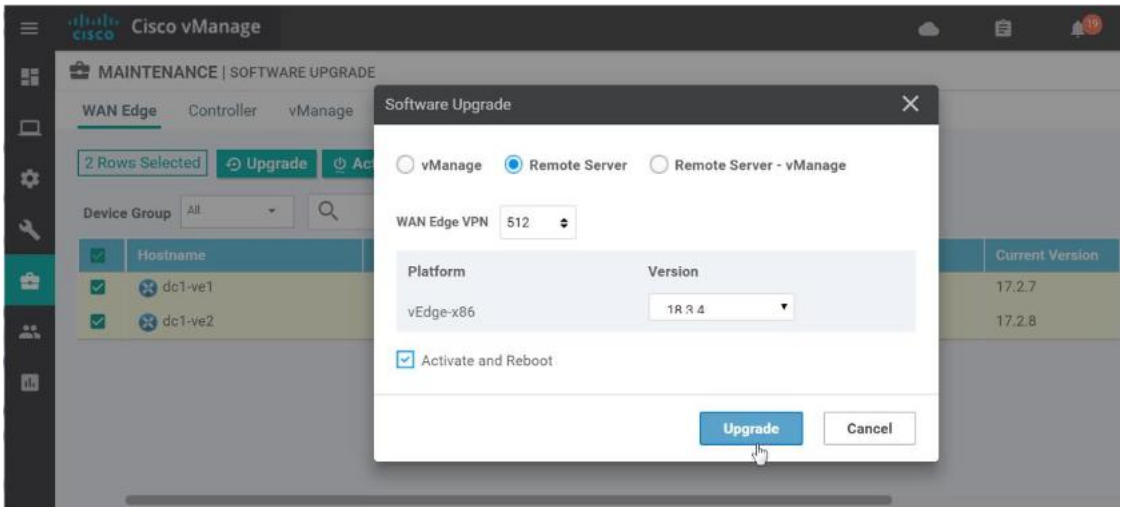
Procedure 4: Upgrade vEdge routers if necessary

Tech tip: Once you upgrade a vEdge router to 18.3.0 or greater, you will not be able to install an image which is 18.2.0 or older. If an image already exists on the vEdge before the upgrade, then you will be able to activate the older image already there (for one week). Once you install and activate Release 18.3.1 or later on a vEdge router, after one week, all Release 18.1 and earlier software images are removed from the router and you cannot reinstall them. See the release notes at https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/Release_Notes/Release_Notes_for_IOS_XE_SD-WAN_Release_16.9_and_SD-WAN_Release_18.3

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

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

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.

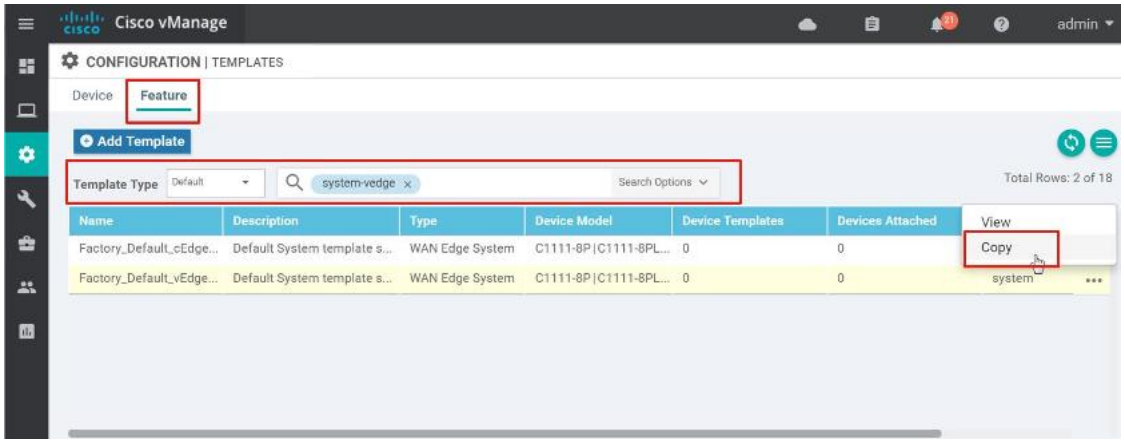
System

The following steps show a system template being created by copying the default system template for a WAN Edge device. You create variables for different parameters, including latitude and longitude, so that the

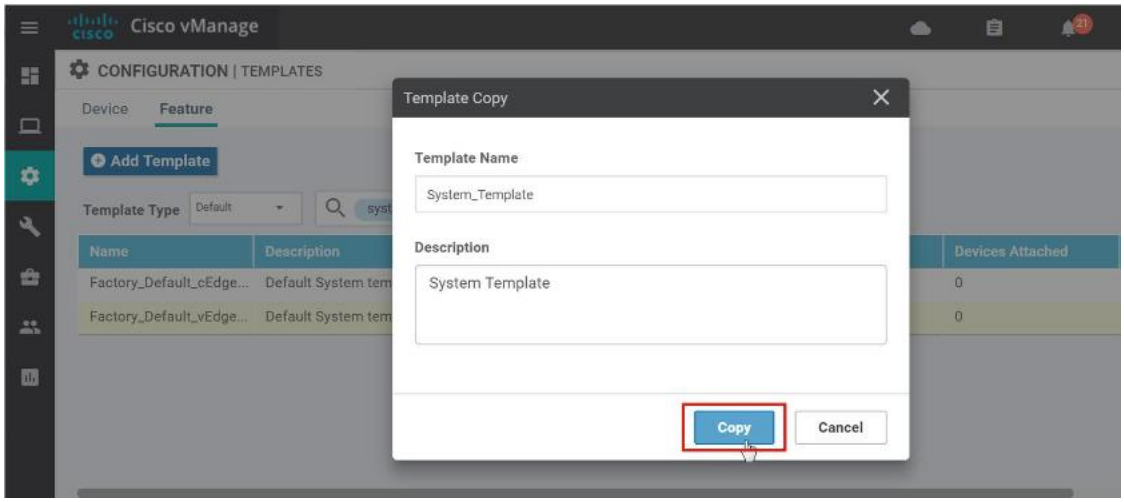
feature template can be used across most WAN Edge devices. Latitude and longitude values allow us to view the WAN Edge location on the vManage map located at Monitor > Geography on the vManage GUI.

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.

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.

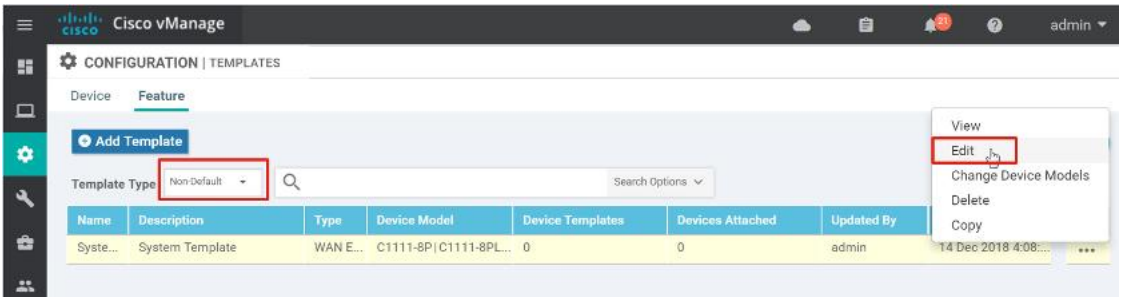


3. In the pop-up window, enter the template name System_Template and description System Template and select Copy.



4. 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.

5. 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 are 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).

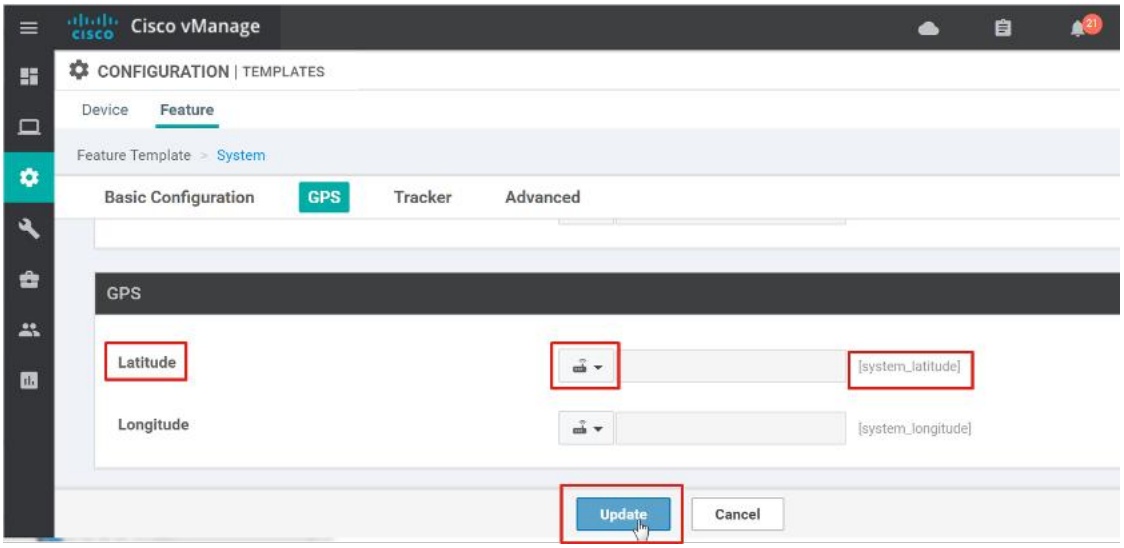
6. Device groups can help organize and group common WAN Edge routers when using the vManage GUI for upgrading and monitoring. For example, you can organize WAN Edge routers according to type or location, and put them into various upgrade groups during upgrade procedures. Next to Device Groups, choose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

7. Next to Console Baud Rate (bps), choose Device Specific from the drop-down box. Use the variable name system_console_baud_rate. The default baud rates are different for the IOS XE SD-WAN routers (9600 bps) and the vEdge routers (115200 bps).

8. 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).

9. 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, including Timezone (UTC).

10. Select Update.



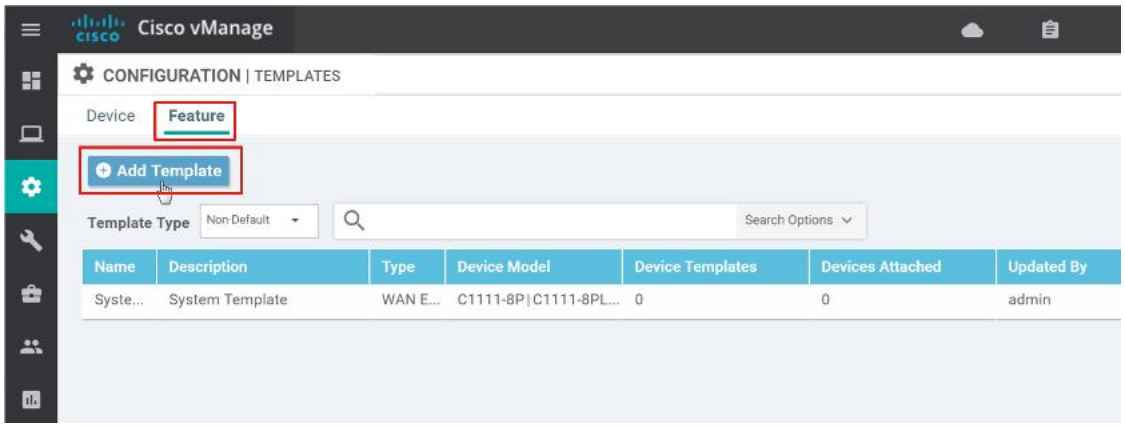
The following table summarizes the parameters configured in the system feature template:

System feature template settings

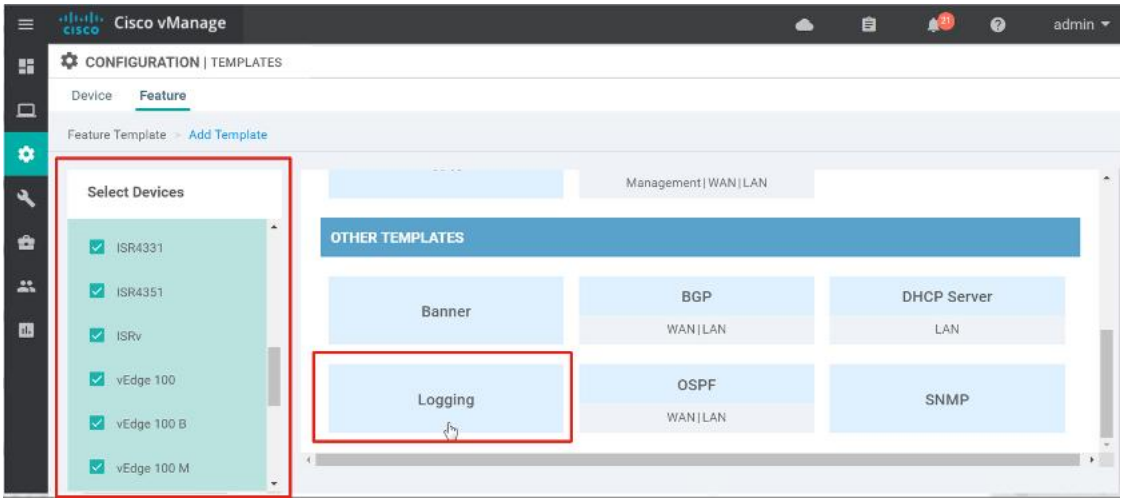
Section	Parameter	Type	Variable/value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_hostname
	Device Groups	Device Specific	system_device_groups
	Console Baud Rate (bps)	Device Specific	system_console_baud_rate
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

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



12. Select the devices this template will apply to from the left side. Select the checkboxes for all devices except for vManage and vSmart. Select the Logging template block under the Other Templates category on the right.

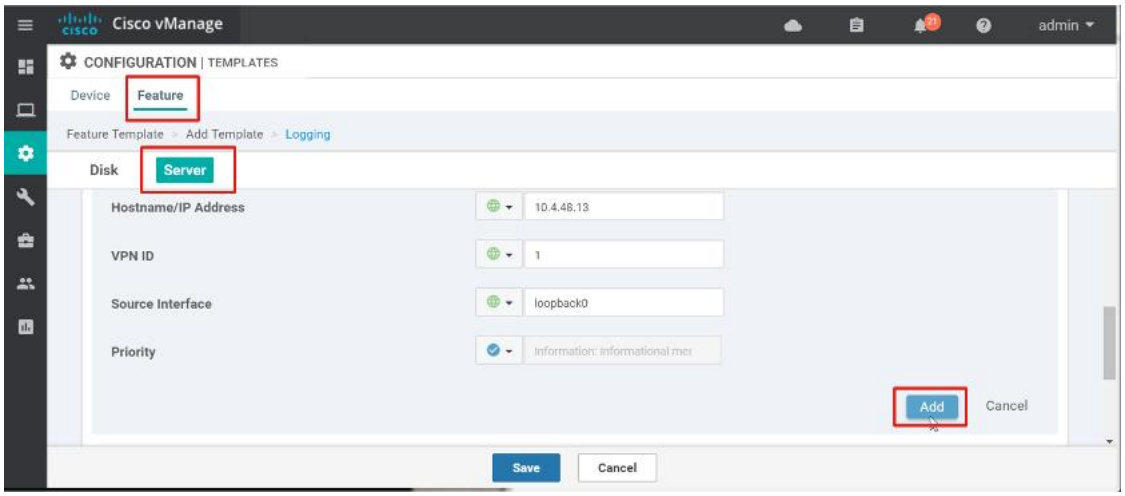


13. The Logging template is presented. Fill in the Template Name (Logging_Template) and Description (Logging Template)

14. 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.

15. 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.

16. 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 you can better correlate the events which appear 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.

17. 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.

18. Select the Save button to complete template.

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

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

Network Time Protocol (NTP)

In the NTP template, the devices will use an NTP server located on the Internet, time.nist.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.

19. 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: All except vManage and vSmart

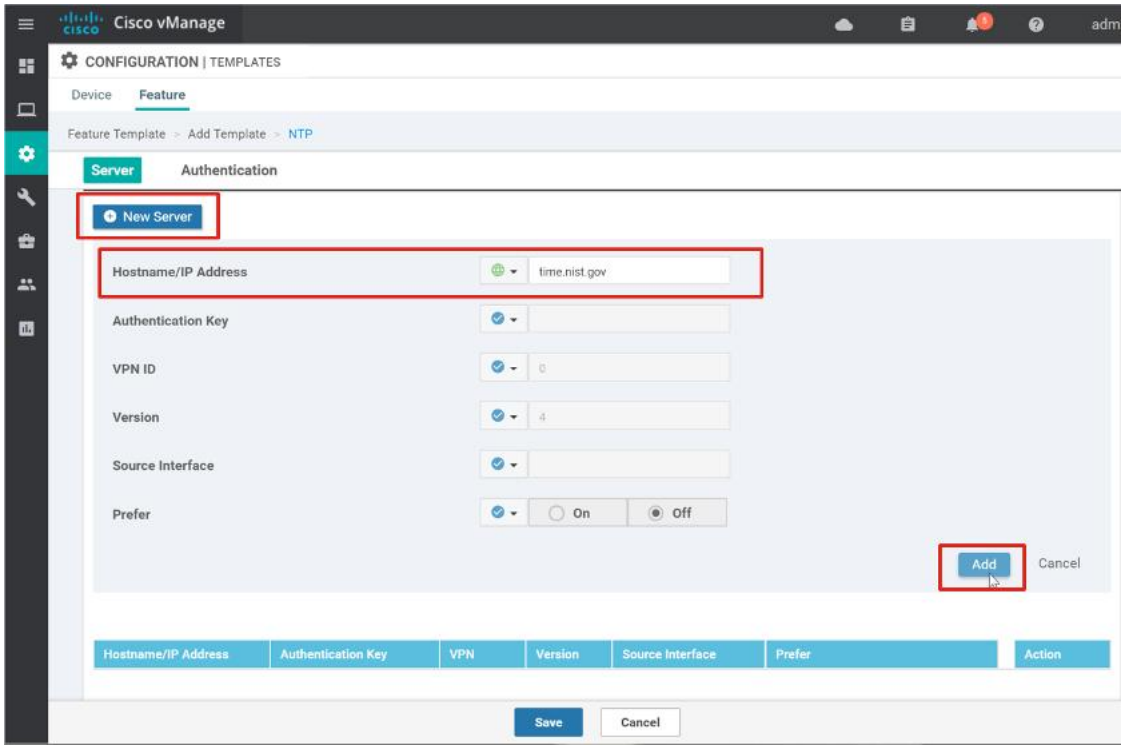
    Template: Basic Information/NTP

    Template Name: NTP_Template

    Description: NTP Template

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

21. 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.

22. Select Save to complete the template.

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

NTP feature template settings

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

AAA

In the AAA feature template, define local authentication and create additional users, an operator with read-only privileges and a netadmin user who can perform all operations. Note that this controls access when users use ssh to access the devices. Different users under different groups can be separately configured in vManage to control access to the vMangage GUI (under Administration>Manage Users).

23. 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: All except vManage and vSmart

    Template: Basic Information/AAA

Template Name: AAA_Template

Description: AAA Template

24. 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.

25. Under the Local authentication section, click the New User button.

26. Next to Name enter oper1. Next to Password, enter a password. Next to User Groups, select operator from the drop-down text box.

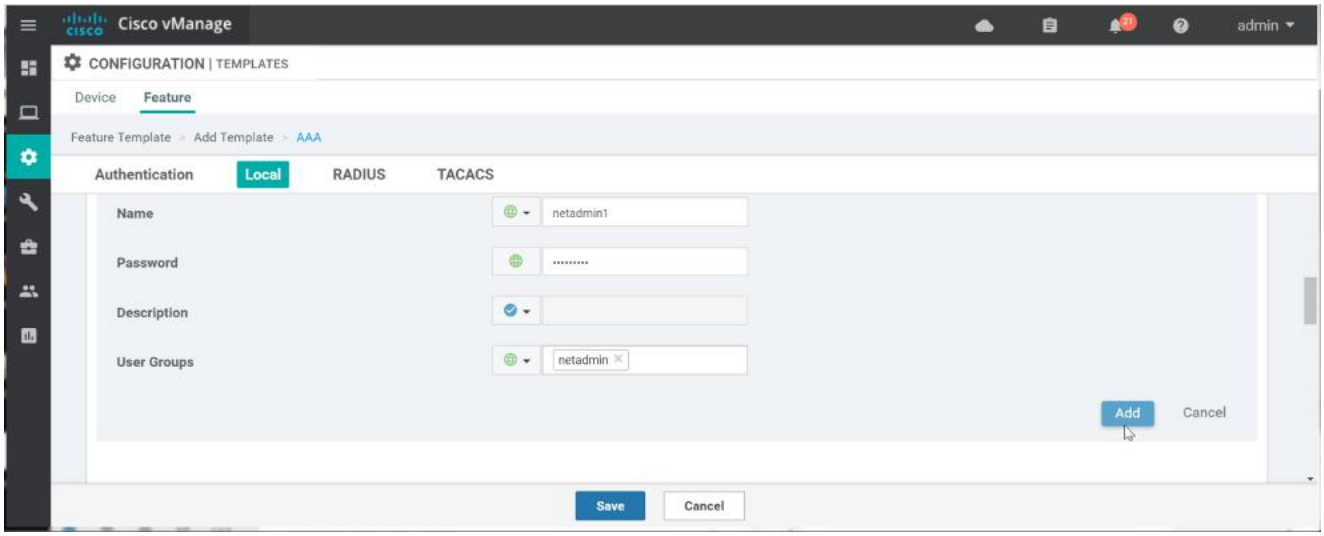
27. Click Add.

28. Click the New User botton to add the second new user.

29. Next to Name enter oper1. Next to Password, enter a password. Next to User Groups, select operator from the drop-down text box.

30. Next to Name, enter netadmin1. Next to Password, enter a password. Next to User Groups, select netadmin from the drop-down text box.

31. Click Add.



32. Select Save to complete the template.

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

AAA feature template settings

Section	Parameter	Type	Variable/value
Authentication	Authentication Order	Drop-down	local
Local/New User	Name/Password/User Groups	Global	oper1/oper1/operator

	Name/Password/User Groups	Global	netadmin1/netadmin1/net admin

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.

33. 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: **All except vManage and vSmart**

    Template: Basic Information/OMP

    Template Name: **OMP_Template**

    Description: OMP Template

34. Configure the following parameters:

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

35. Select Save to complete the template.

Bidirectional Forwarding Detection (BFD)

BFD is used by application-aware routing to calculate delay, loss, and jitter for the SLA classes. It is also used on the tunnel transports to detect link failures. It is on by default and you cannot disable it.

In the BFD feature template, the app-aware routing BFD poll interval is modified to 120000 milliseconds. The Color section in the template allows you to change the default BFD timers on the transports to detect tunnel failures and to turn on or off Path MTU Discovery (PMTUD). PMTUD is enabled by default.

36. 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:

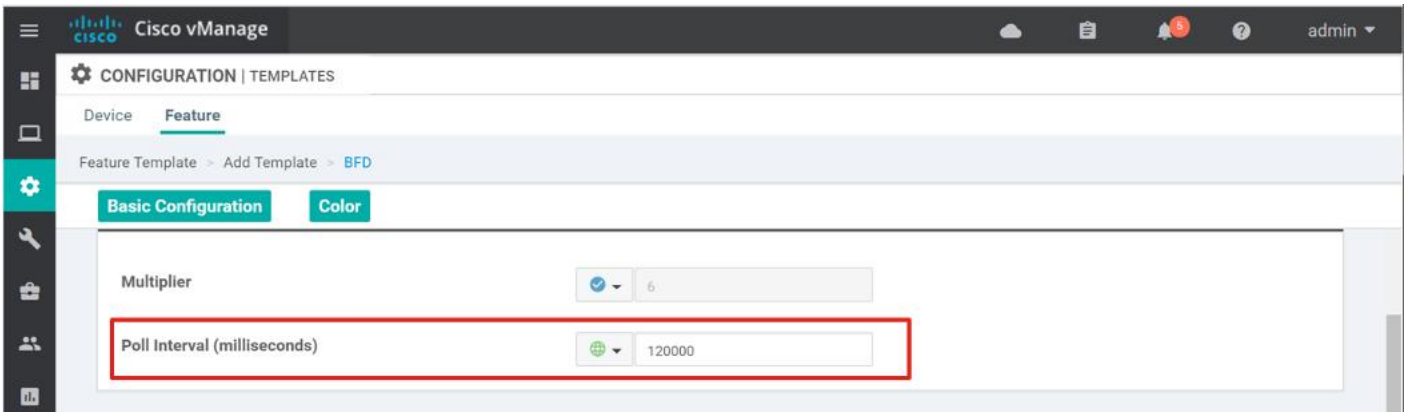
    Select Devices: All except vManage and vSmart

    Template: Basic Information/BFD

Template Name: BFD_Template

Description: BFD Template

37. Under Basic Configuration next to Poll Interval, select Global and type in 120000 in the text box.



38. Select Save to complete the template.

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

BFD feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Poll Interval	Global	120000

Security

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

39. 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: All except vManage and vSmart

    Template: Basic Information/Security

    Template Name: Security_Template

    Description: Security Template

40. Configure the following parameters:

Security feature template settings

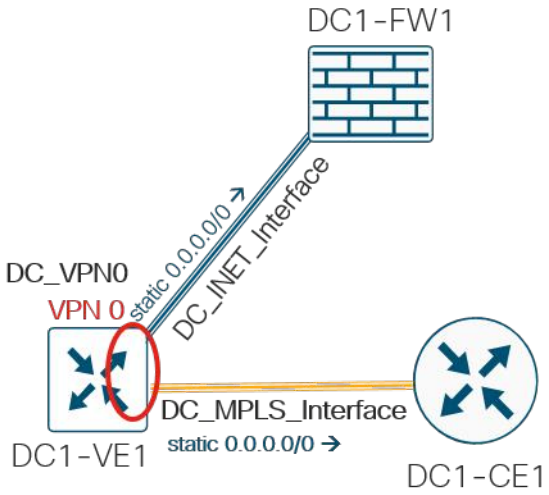
Section	Parameter	Type	Variable/value
Basic Configuration	Replay Window	Global/drop-down	4096

41. 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



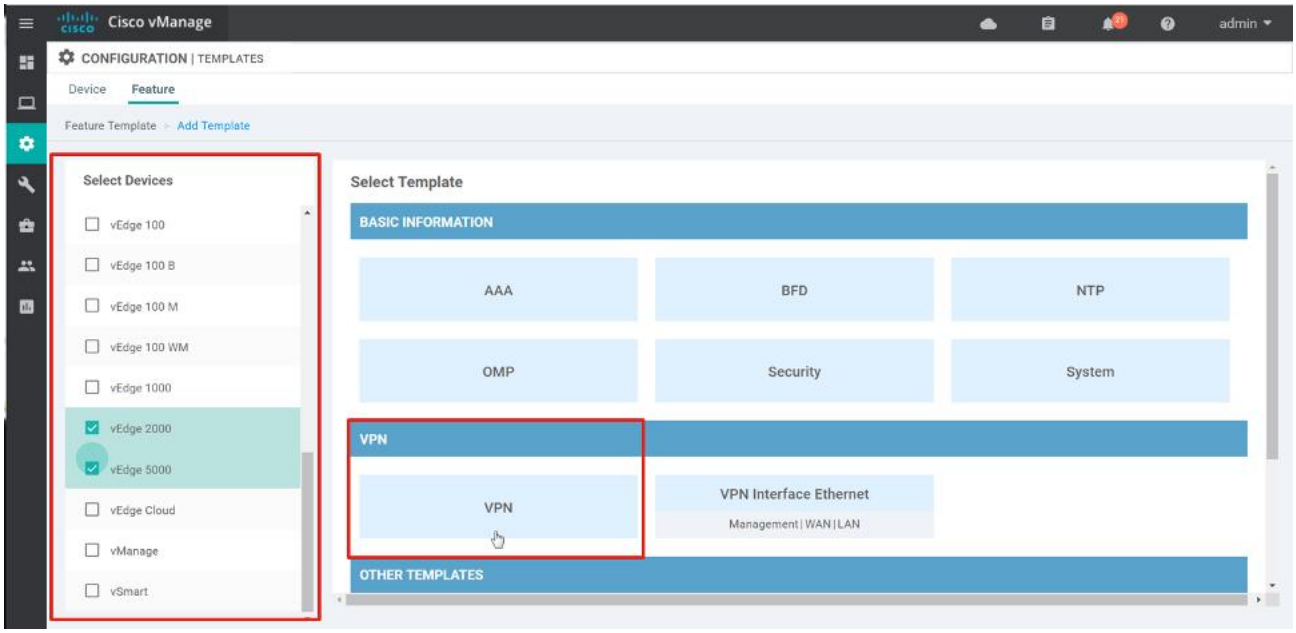
Transport VPN (VPN 0)

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

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.

3. Under the Select Devices column, choose ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000, and any additional WAN Edge device types that may reside at the data center. Select the VPN template block under the VPN section on the right.



4. Configure the Template Name and Description:

   Template Name: DC _VPN0

   Description: DC Transport VPN 0

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

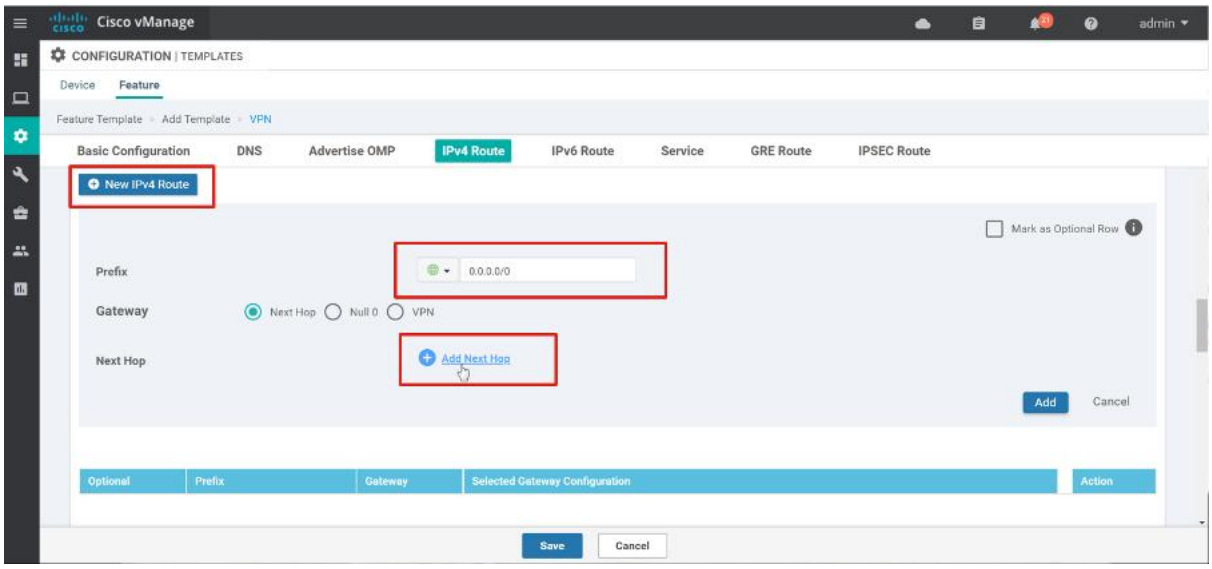
6. Next to Name, select Global from the drop-down menu, and type Transport VPN, a description for the VPN.

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.

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 so the tunnel endpoints can peer with neighboring sites. Multiple default routes can exist because the WAN Edge uses the physical tunnel endpoint source as well as the destination when making a routing decision.

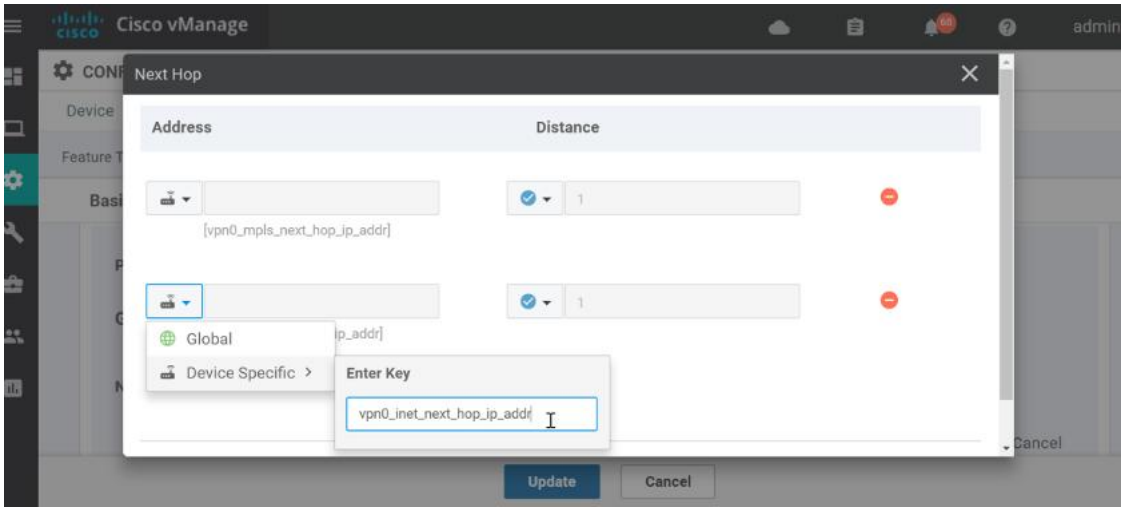
9. Under the IPv4 Route section, click the New IPv4 Route button. Add 0.0.0.0/0 in the Prefix box and select Add Next Hop.



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

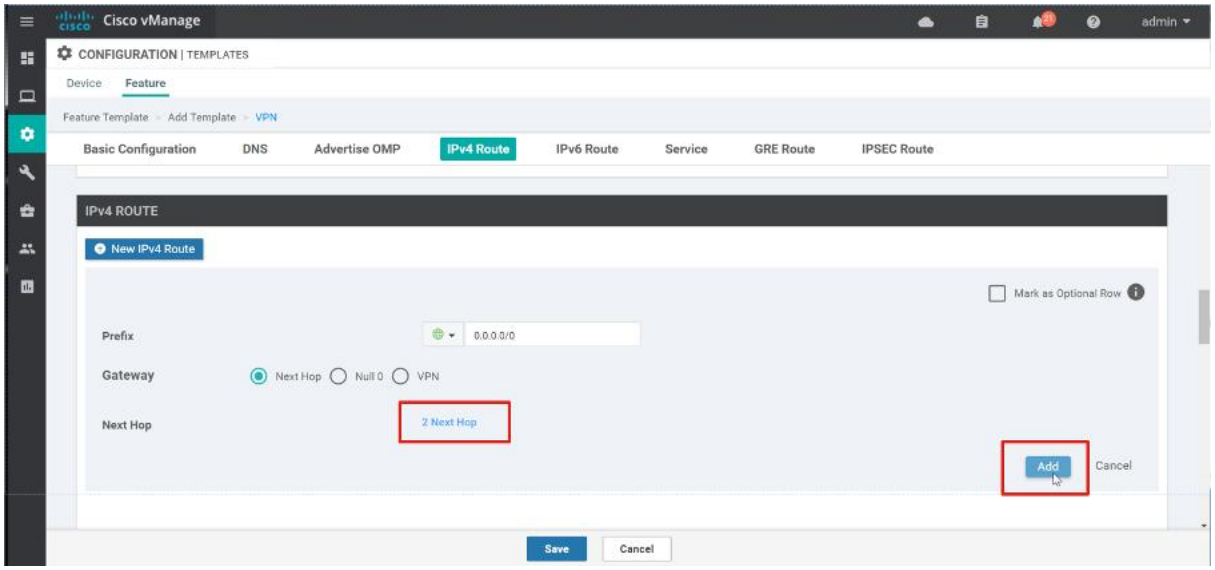
11. Since this template applies to more than one WAN Edge, the next hop parameters are variables instead of global values. On the pop-up window, under Address, select Device Specific from the drop-down menu, and type in the next-hop IP address variable for the MPLS transport in the text box (vpn0_mpls_next_hop_ip_addr).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

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 Internet transport in the text box (vpn0_inet_next_hop_ip_addr).



13. Select Add at the bottom of the popup. This stores both next hops for the prefix 0.0.0.0/0. You will return to the feature template page.

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, along with the next-hop information for that prefix.



15. Select Save to create the template.

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

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
	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

Next, configure the interfaces under the transport VPN.

VPN interface (MPLS)

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: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

    Template: VPN/VPN Interface Ethernet

Template Name: DC_ MPLS_Interface

Description: DC MPLS Interface

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.

18. Under the Basic Configuration section next to Interface Name, select Device Specific and type in the variable name vpn0_mpls_int_x|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.

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

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.

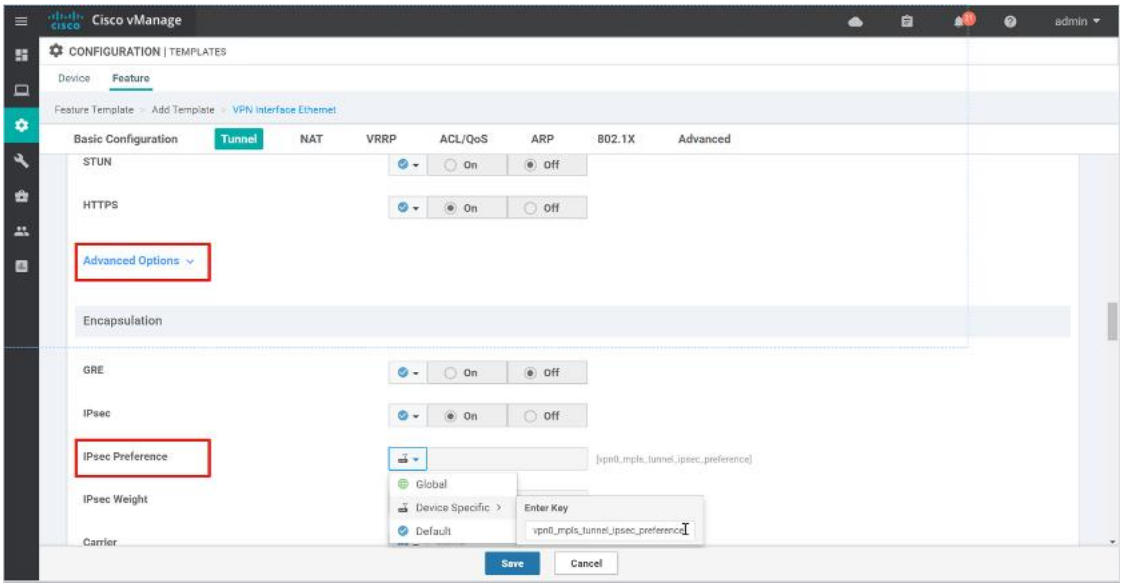
21. Under Basic Configuration, next to Bandwidth Upstream, select Device Specific and type in the variable name vpn0_mpls_int_bandwidth_up. Next to Bandwidth Downstream, select Device Specific and type in the variable name vpn0_mpls_int_bandwidth_down. These two parameters cause vManage notifications,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

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 WAN Edge. In addition, other services can be enabled and accepted into the physical interface unencrypted - this includes DNS, DHCP, HTTPS, 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.

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

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.



25. 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.

26. Press the Save button to create the template.

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

VPN 0 VPN Interface Ethernet feature template settings (MPLS)

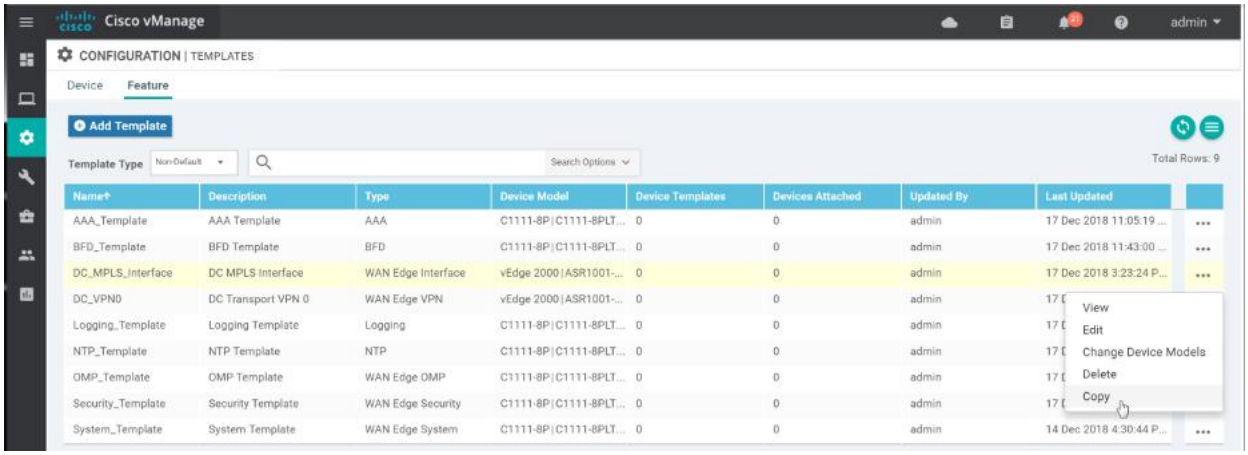
Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_x|x
	Description	Global	MPLS Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr|maskbits
	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	Clear-Dont-Fragment	Global	On

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

VPN interface (Internet)

27. 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.

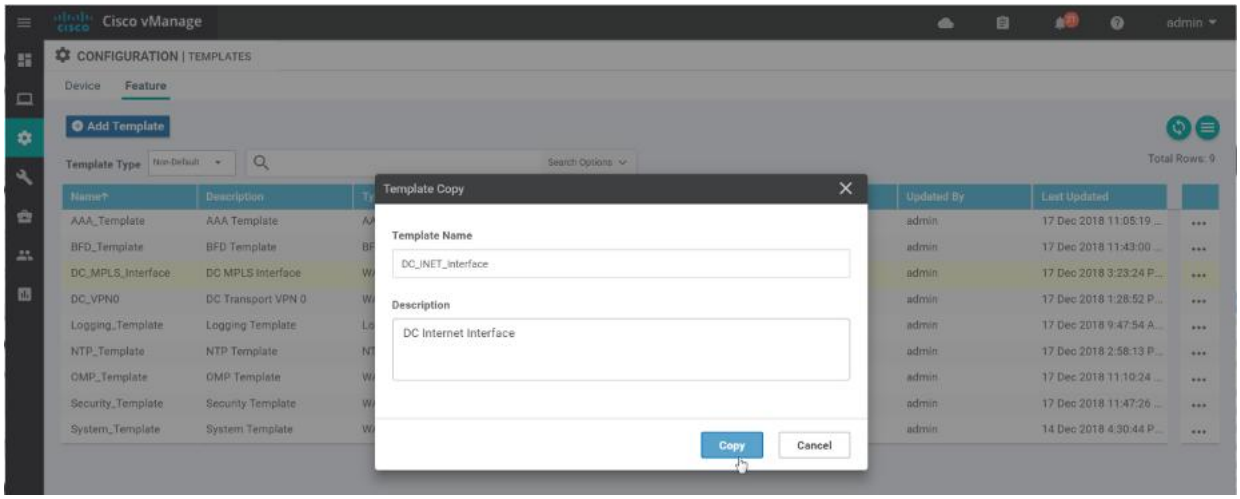


28. On the pop-up window, define the template name and description as:

    Template Name: DC_INET_Interface

    Description: DC Internet Interface

29. Select the Copy button. The feature template is created and is now in the list with the other created feature templates.



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

31. Modify the interface description, variables, and tunnel color.

The following table summarizes the parameters in the feature template.

VPN 0 VPN 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_x|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	Clear-Don't-Fragment	Global	On

32. 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 WAN Edge router.

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: All except vManage and vSmart

   Template: VPN/VPN

   Template Name: VPN512_Template

   Description: VPN 512 Out-of-Band Management

2. Configure the parameters in the following table.

VPN512 feature template settings

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

3. Select Save to create the feature template.

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

VPN interface (VPN512)

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

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

   Select Devices: All except vManage and vSmart

   Template: VPN/VPN Interface Ethernet

   Template Name: VPN512_Interface

Description: VPN 512 Management Interface

6. Configure the parameters in the following table.

VPN512 interface feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgt_int_x|x
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_mgt_int_ip_addr|maskbits

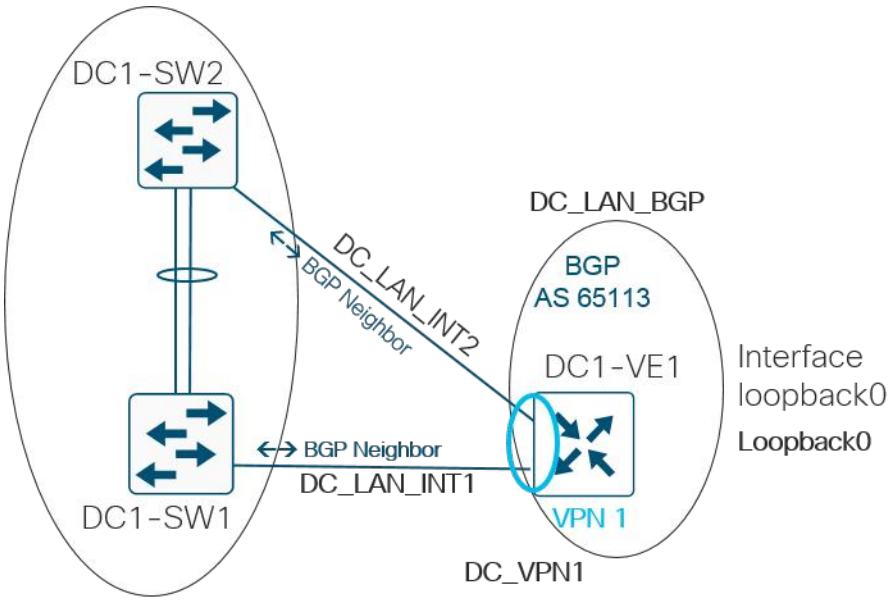
By defining the interface name as a variable, only one template is needed and can be applied to multiple types of WAN Edge devices because different model types use different management port interfaces. For example, the vEdge 1000, 2000, and 5000 routers all use the built-in mgmt0, the vEdge 100 uses a normal Ethernet port (ge0/1 in the example network), and the IOS XE SD-WAN routers use GigabitEthernet0.

7. Press the Save button to create the template.

Procedure 8: Configure the Service VPN

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. BGP is redistributed into OMP so that remote sites can have reachability into the data center.

Figure 14 Data center vEdge service templates



Service VPN 1

1. Select Configuration>Templates, and select the Feature tab. Select the Add Template button.
2. Create the VPN 1 template using the following device types, template, template name, and description:

   Select Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

   Template: VPN/VPN

   Template Name: DC_VPN1

   Description: DC Service VPN 1
3. Configure the parameters in the following table.

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.

4. Select Save to create the template.

VPN interface Ethernet 1

5. Assuming that you are still on the Feature Templates page, select the Add Template button.

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

   Select Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

   Template: VPN/VPN Interface Ethernet

   Template Name: DC_LAN _INT1

   Description: DC LAN Interface 1

7. Configure the parameters in the following table.

Data center VPN interface feature template settings (Interface 1)

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x
	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits

8. Select Save to complete the template.

VPN interface Ethernet 2

9. Assuming that you are still on the Feature Templates page, find the feature template just created (DC_LAN_INT1) and select **...** to the far right. Select Copy.

10. In the pop-up window, define the Template Name and Description as:

    Template Name: DC _LAN_INT2

    Description: DC LAN Interface 2

11. Select the Copy button. The feature template is created and is now in the list with the other created feature templates.

12. Choose **...** to the right of the newly-created feature template (DC_LAN_INT2) and select Edit to modify the template.

13. Modify the interface variables.

The following table summarizes the parameters in the feature template.

Data center VPN interface feature template settings (Interface 2)

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr|maskbits

14. Once configuration changes have been made, select the Update button to save the changes in the feature template.

VPN interface Ethernet Loopback 0

A loopback0 interface is created with the system IP address so that 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.

15. Assuming that you are still on the Feature Templates page, select the Add Template button.

16. Create the loopback0 interface template using the following device types, template type, template name, and description:

    Select Devices: All except vManage and vSmart

    Template: VPN/VPN Interface Ethernet

    Template Name: Loopback0

    Description: Interface Loopback 0

17. Configure the parameters listed in the following table.

VPN 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	lo0_int_ip_addr|maskbits

18. 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. The feature setting called Propagate AS Path is enabled, which carries the BGP AS path information into OMP which can be passed to other BGP-enabled sites for loop prevention.

Tech tip: The Propagate AS Path feature is not supported on IOS XE SD-WAN software until 16.11.1.

19. Assuming that you are still on the Feature Templates page, select the Add Template button.

20. Create the BGP template using the following device types, template type, template name, and description:

    Select Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

    Template: Other Templates/BGP

    Template Name: DC_LAN_BGP

    Description: DC LAN BGP Template

21. Configure the parameters listed in the following table under the Basic Configuration section.

BGP feature template basic configuration settings

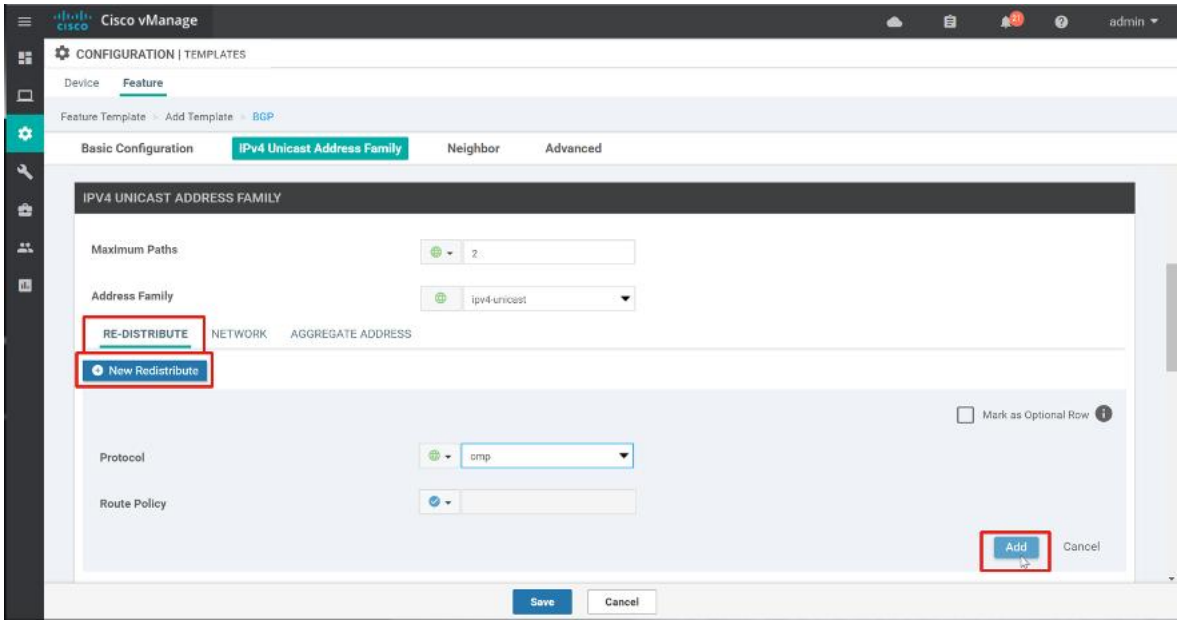
Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_bgp _shutdown
	AS Number	Device Specific	lan_bgp_as_num
	Router ID	Device Specific	lan_bgp_router_id
	Propagate AS Path	Global	On

22. Configure the IPv4 Unicast Address Family section for the BGP template. Next to Maximum Paths, select Global and enter 2 in the text box.

23. Next to Address Family, choose ipv4-unicast from the drop-down box.

24. On the Re-Distribute tab, which is the default, click on the New Redistribute button. This area of the configuration will allow multiple protocols to be redistributed into BGP. In this case, OMP will be redistributed.

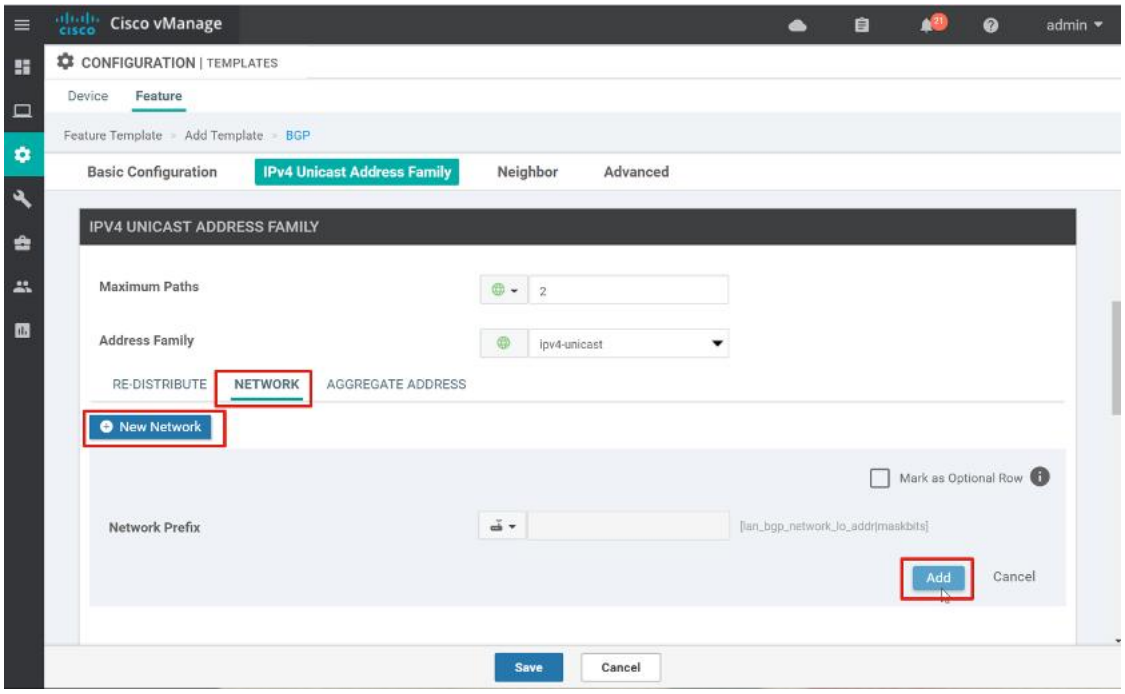
25. Next to Protocol, choose omp from the drop-down box, then click the Add button.



26. The loopback0 address in this example is advertised in BGP by configuring a network statement. Select the Network tab and click the New Network button.

27. Next to Network Prefix, select Device Specific and enter the variable name, lan_bgp_network_lo_addr|maskbits, in the text box.

28. Click the Add button.



BGP feature template IPv4 unicast address family configuration settings

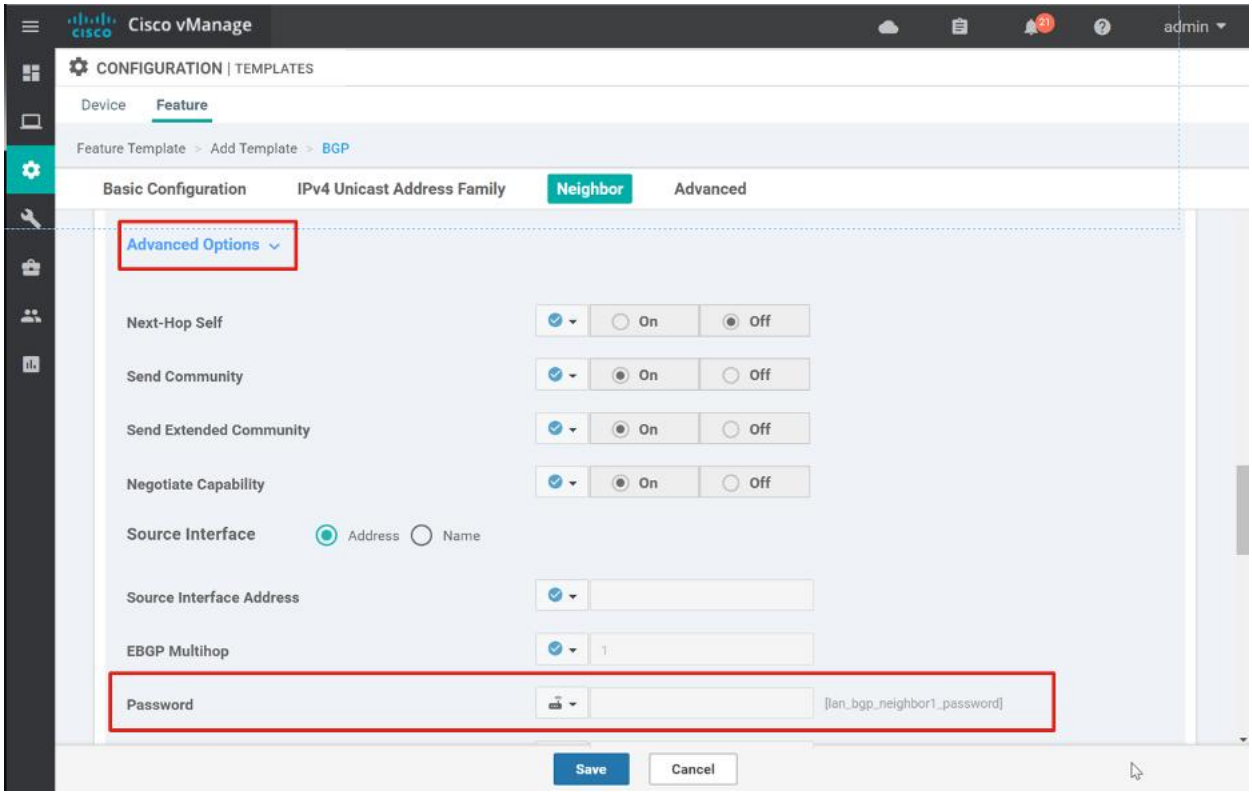
Section	Parameter	Type	Variable/value

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

29. Configure the Neighbor section for the BGP template. Click the New Neighbor button and configure the parameters listed in the following table. Click on the Advanced Options text to reveal the advanced parameter options.

BGP feature template neighbor 1 configuration settings

Section	Parameter	Type	Variable/value
Neighbor (1)	Address	Device Specific	lan_bgp_neighbor1_addr
	Description	Device Specific	lan_bgp_neighbor1_description
	Remote AS	Device Specific	lan_bgp_neighbor1_remote_as
	Address Family	Global	On
	Address Family	Global	ipv4-unicast
	Shutdown	Device Specific	lan_bgp_neighbor1_shutdown
	Advanced Options/Password	Device Specific	lan_bgp_neighbor1_password
	Advanced Options/Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9



30. Click the Add button to add the neighbor configuration to the template.

31. Repeat the previous two steps to add the configuration for the second BGP neighbor. Configure the parameters listed in the following table.

BGP feature template neighbor 2 configuration settings

Section	Parameter	Type	Variable/value
Neighbor (2)	Address	Device Specific	lan_bgp_neighbor2_addr
	Description	Device Specific	lan_bgp_neighbor2_description
	Remote AS	Device Specific	lan_bgp_neighbor2_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Shutdown	Device Specific	lan_bgp_neighbor2_shutdown
	Advanced Options/Password	Device Specific	lan_bgp_neighbor2_password
	Advanced Options/Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9

32. Click the Add button to add the neighbor configuration to the template.

33. Select Save to create the template.

Procedure 9: Configure additional templates (optional)

You can create a banner and an 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.

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

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

   Select Devices: All except vManage and vSmart

   Template: Other Templates/Banner

   Template Name: Banner_Template

   Description: Banner Template

3. Configure the parameters listed in the following table.

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.

4. Select Save to create the template.

SNMP

Tech tip: Currently, no SD-WAN-specific mibs and traps are supported on IOS-XE SD-WAN code. Only IOS mibs and traps are supported.

5. Assuming that you are still on the Feature Templates page, select the Add Template button.

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

Select Devices: All except vManage and vSmart

Template: Other Templates/SNMP

Template Name: SNMP_Template

Description: SNMP Template

7. Configure the basic configuration parameters in the following table.

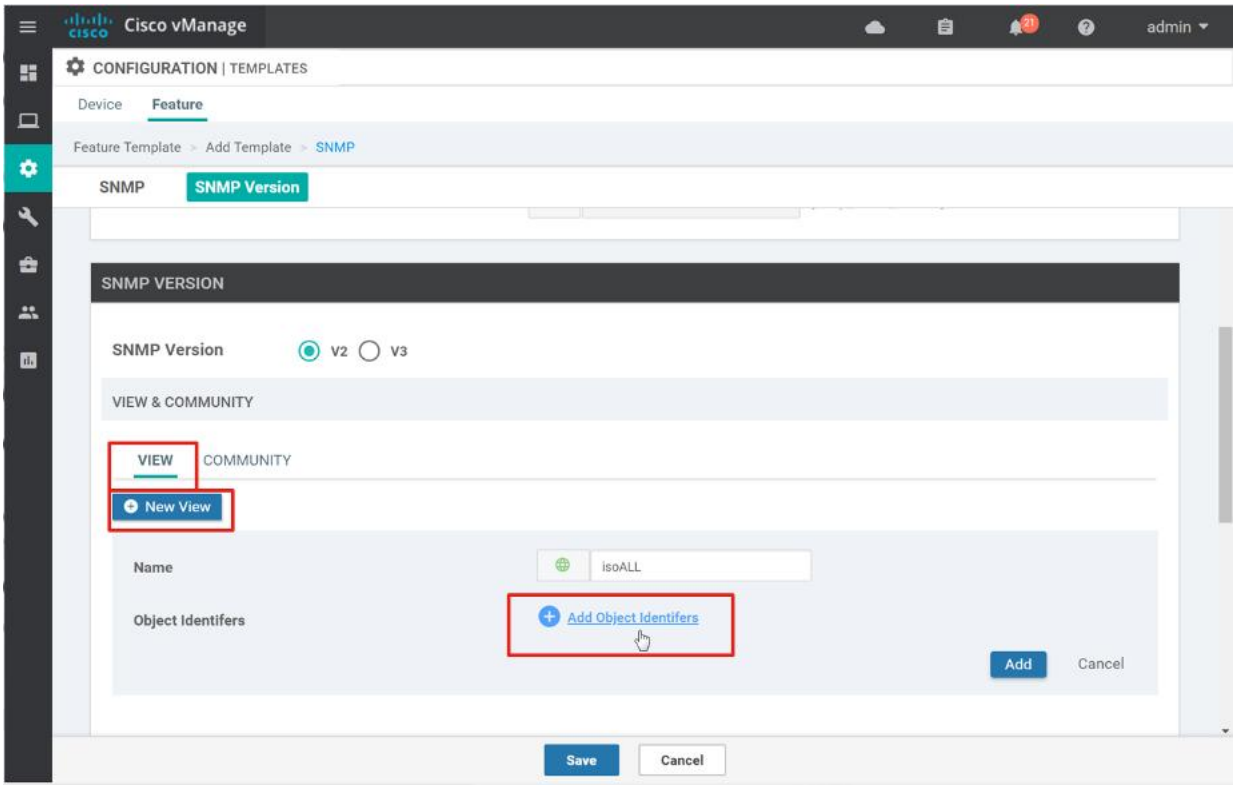
SNMP feature template basic configuration settings

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

8. Configure the SNMP Version section of the template. Next to SNMP Version, ensure V2 is selected. Under View & Community on the View tab, click the New View button.

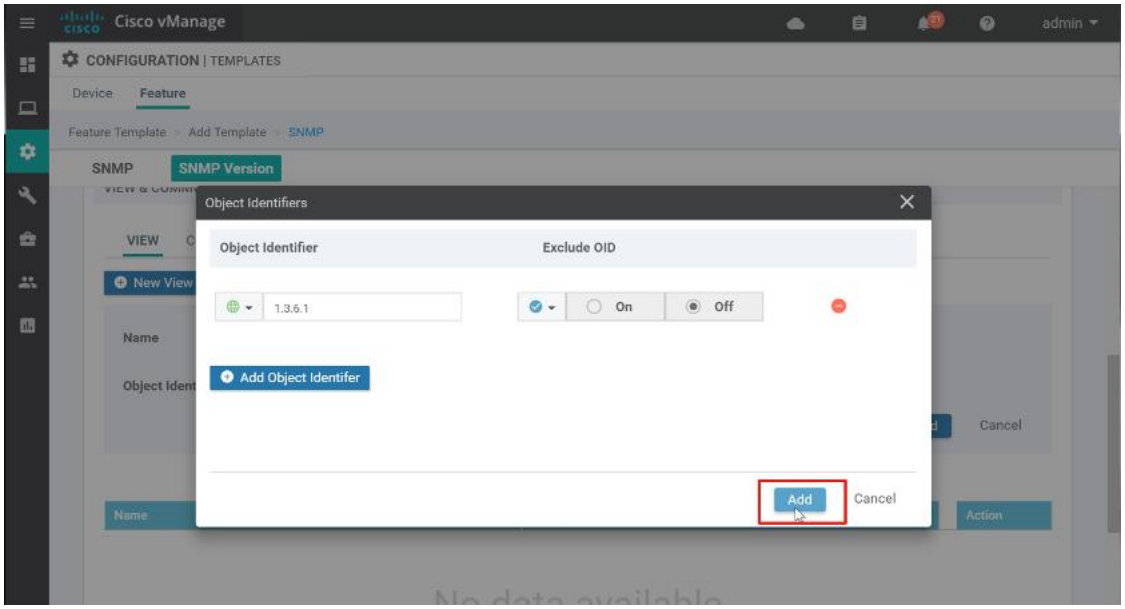
9. Next to Name, type in isoALL in the text box.

10. Click on the Add Object Identifiers text.



11. A pop-up window indicates that you should add your first object identifier. Click the Add Object Identifier button.

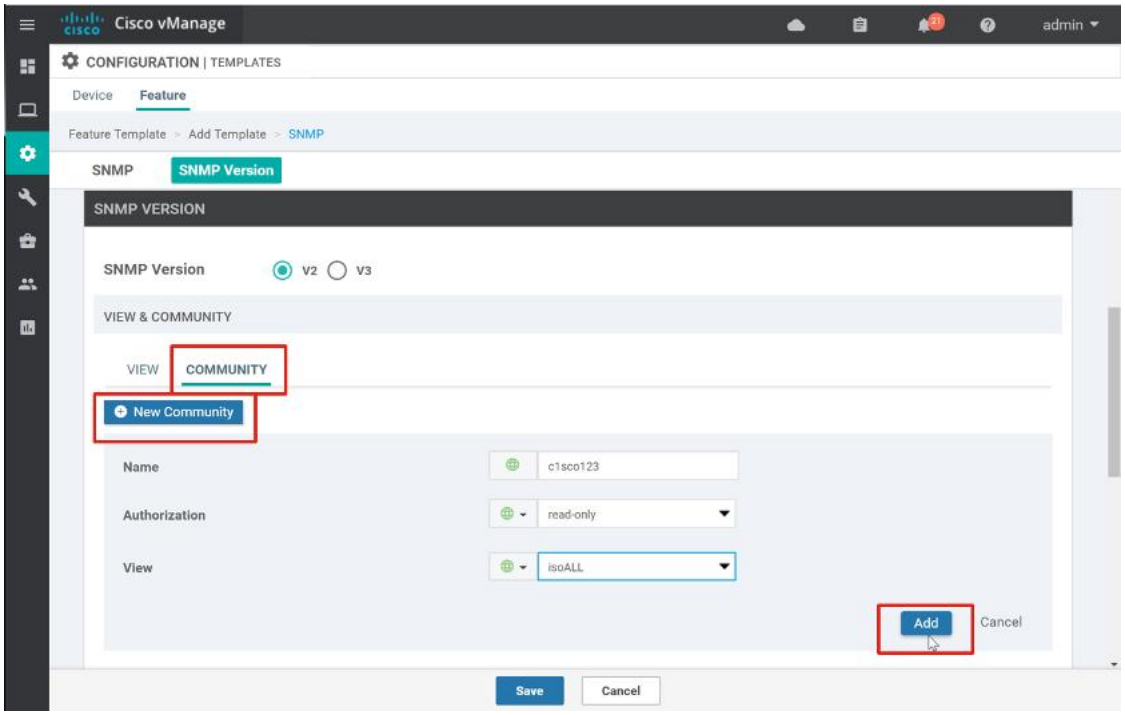
12. An Object Indentifiers pop-up window appears. In the text box, type 1.3.6.1. Then click the Add button.



13. Once on the main feature template page, click the Add button to save the isoALL view in the template.

14. Under the View & Community section, select the Community tab and click the New Community button. Enter the community Name (c1sco123), select the Authorization (read-only), and select the View just created (isoALL).

15. Click the Add button to save the community settings in the template.

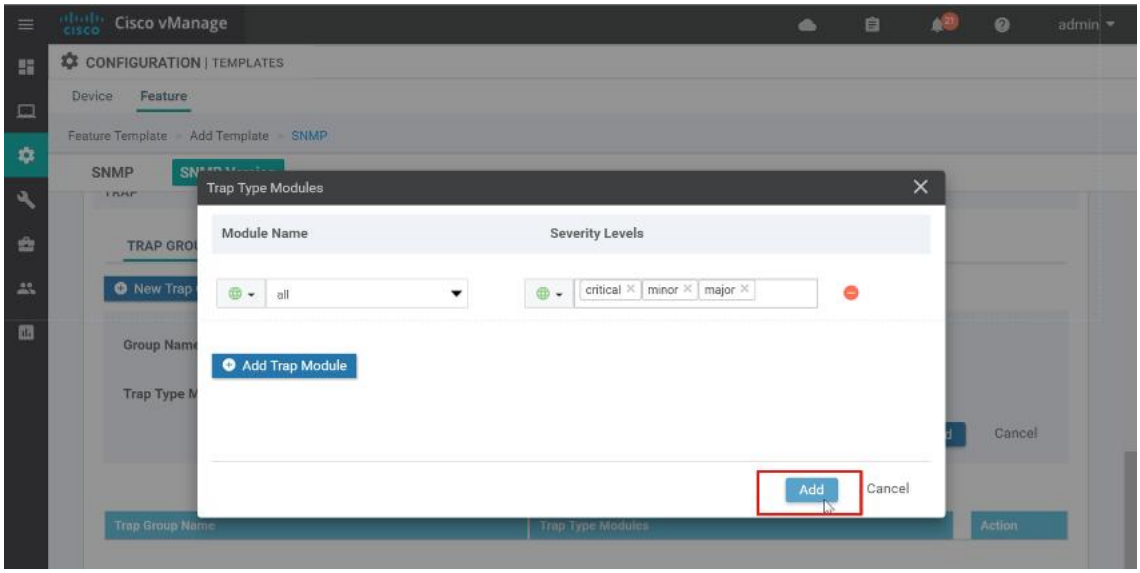


16. Under the Trap section, select the Trap Group tab and click on the New Trap Group button. Enter the Group Name (SNMP-GRP) and click on the Add Trap Type Modules text.

17. A pop-up window instructs you to add your first trap module. Click the Add Trap Module button.

18. Choose a Module Name (all) and the Severity Levels (critical, major, minor) from the drop-down boxes.

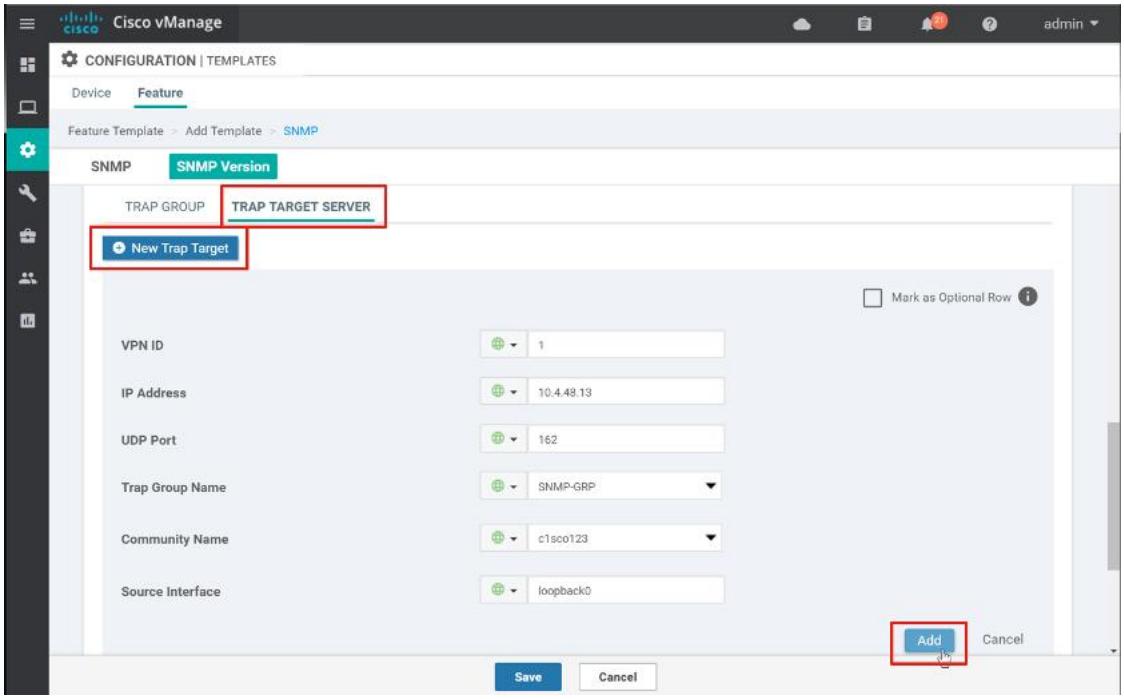
19. Click the Add button.



20. Once on the main feature template page, click the Add button to save the trap group in the template.

21. Under the Trap section, select the Trap Target Server tab and click on the New Trap Target button. Enter the VPN ID (1), the IP Address (10.4.48.13) and UDP Port (162) of the SNMP trap server, the Trap Group Name (SNMP-GRP), and the Community Name (c1sco123). Next to Source Interface, select Global from the drop-down box and enter loopback0.

22. Click the Add button.



23. Select Save to create the template.

SNMP feature template view, community, and trap settings

Section	Parameter	Type	Variable/value
SNMP Version	SNMP Version	Radio button	V2
SNMP Version/View & 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
SNMP Version/Trap	Trap Group/Group Name	Global	SNMP-GRP
	Trap Group/Trap Type Modules/Module Name	Global	all
	Trap Group/Trap Type Modules/Severity Levels	Global	critical, major, minor
	Trap Target Server/VPN	Global	1
	Trap Target Server/IP Address	Global	10.4.48.13
	Trap Target Server/UDP Port	Global	162

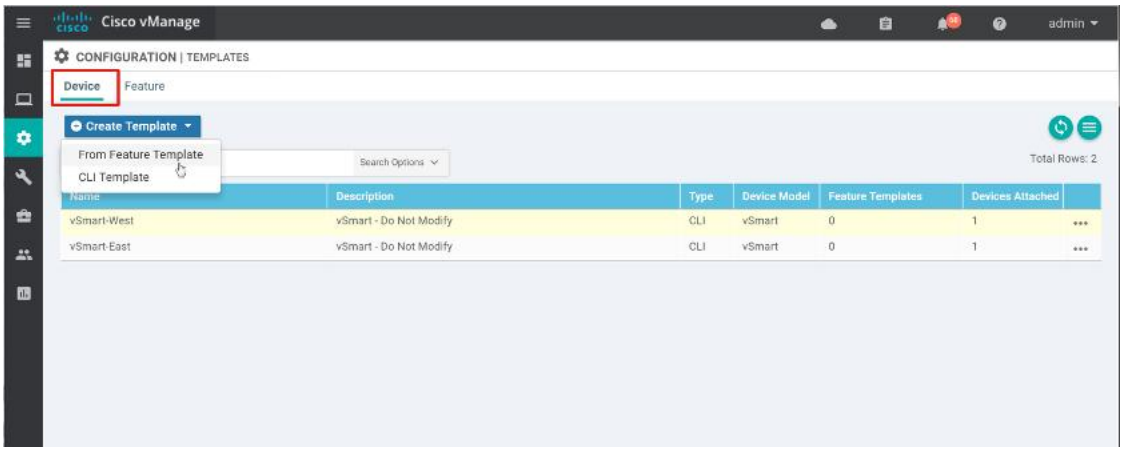
	Trap Target Server/Trap Group Name	Global	SNMP-GRP
	Trap Target Server/Community Name	Global	c1sco123
	Trap Target Server/Source Interface	Global	loopback0

Procedure 10: Create a device template

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

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

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



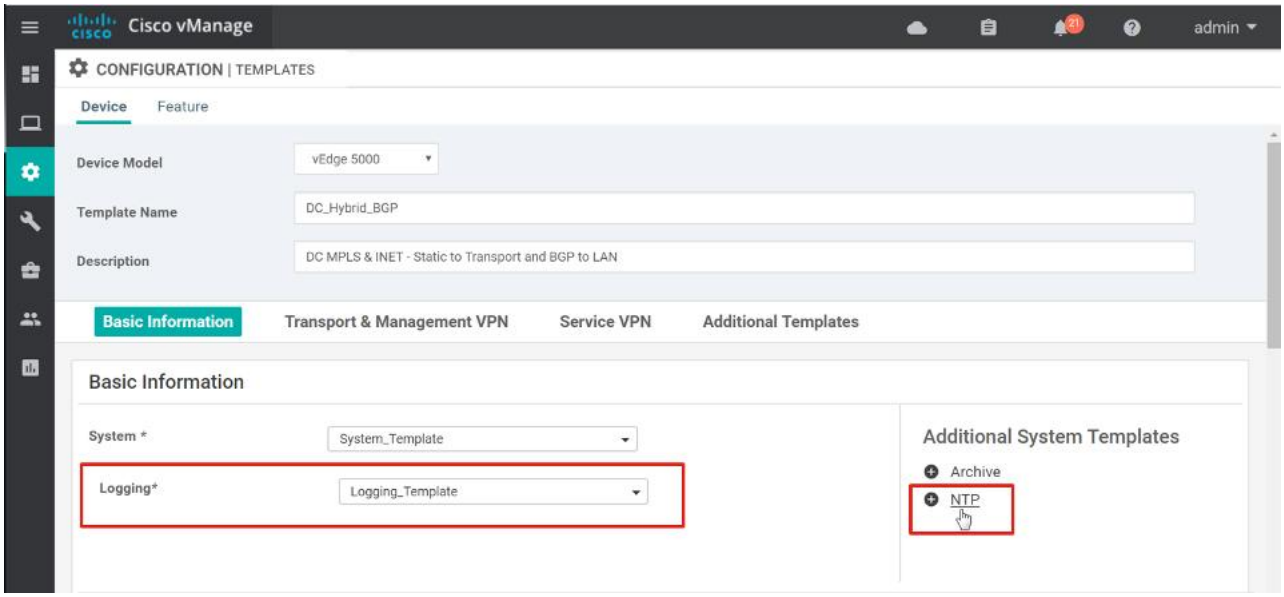
3. Select the Device Model (vEdge 5000) from the drop-down box.

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

5. Under Basic Information next to System, select the feature template, System_Template, from the drop-down box.

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

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.



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

9. Repeat the last step for BFD (BFD_Template), OMP (OMP_Template), and Security (Security_Template).

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

10. Under the Transport & 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.

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.

Transport and management VPN section of device template

Template type	Template sub-type	Template name

VPN0		DC_VPN0
	VPN Interface	DC_MPLS_Interface
	VPN Interface	DC_INET_Interface
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface

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.

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.

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

Service VPN section of device template

Template type	Template sub-type	Template name
VPN1		DC _VPN1
	BGP	DC_LAN_BGP
	VPN Interface	DC_LAN_INT1
	VPN Interface	DC_LAN_INT2
	VPN Interface	Loopback0

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. There is also no Security Policy to reference at this time.

Additional templates section of device template

Template type	Template name
Banner	Banner_Template
Policy	
Security Policy	
SNMP	SNMP_Template

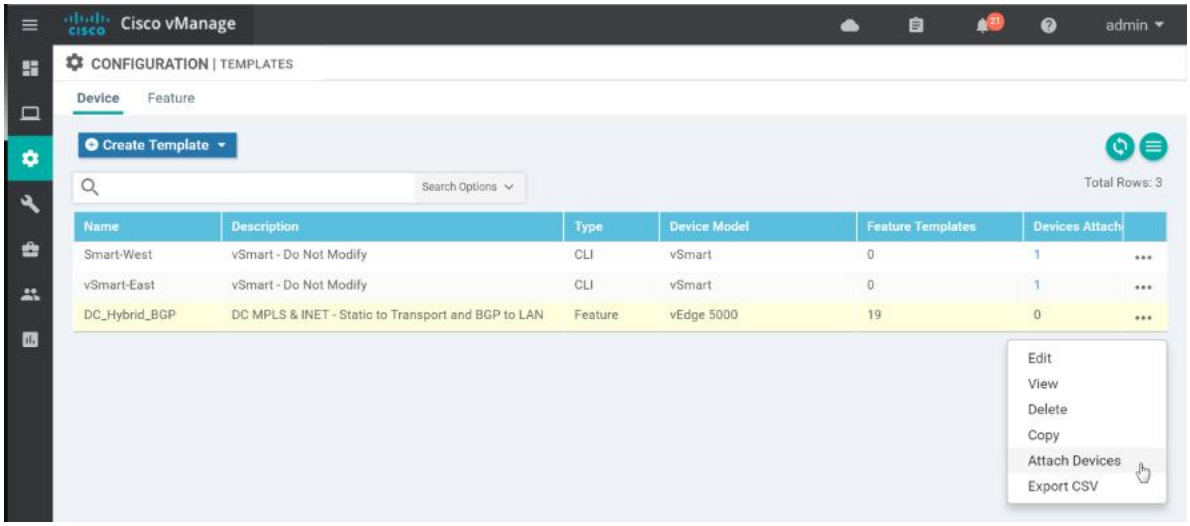
16. Select Create to create and save the device template.

Procedure 11: Deploy the device templates to the WAN Edge routers

To deploy the device template created to the WAN Edge routers, the vManage builds the full configurations based on the feature templates and then pushes them out to the designated WAN Edge 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.

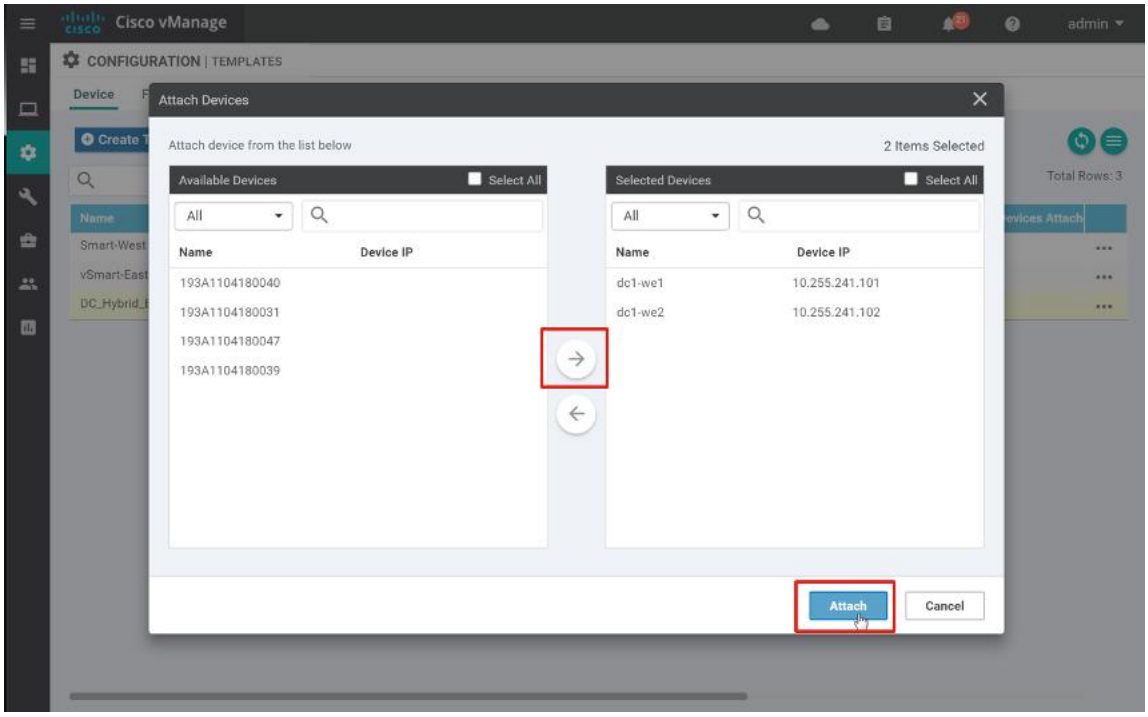
Enter values manually

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

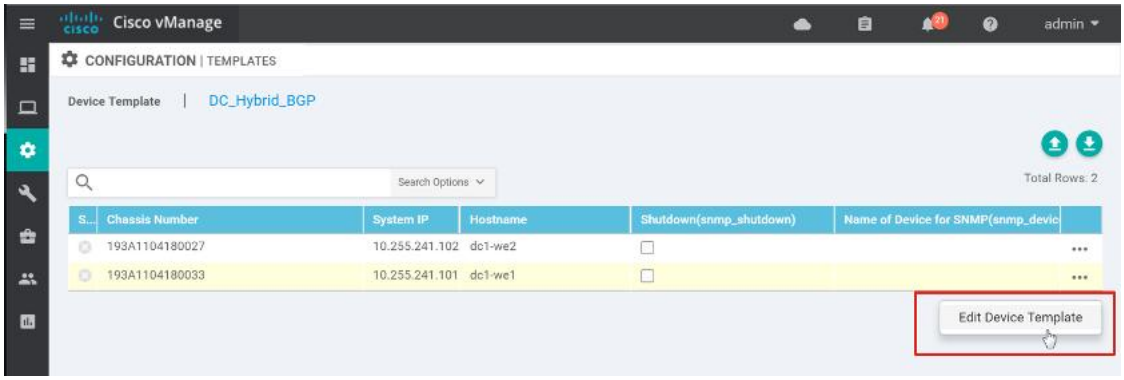


2. A window pops up listing the available devices to be attached to this configuration. The list of available devices contains either the hostname and IP address of a device if it is known through vManage, or it will contain the chassis serial number of the devices that have not yet come up on the network 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).

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.



4. There will be a page listing the devices you have selected. Find dc1-we1, and select **...** to the far right of it. Select Edit Device Template.



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. Because we did not select any optional configurations in the DC templates, all text boxes must be filled in, but check boxes can be left unchecked. 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 as listed in the following table.

Data center WAN Edge 1 device template variable values

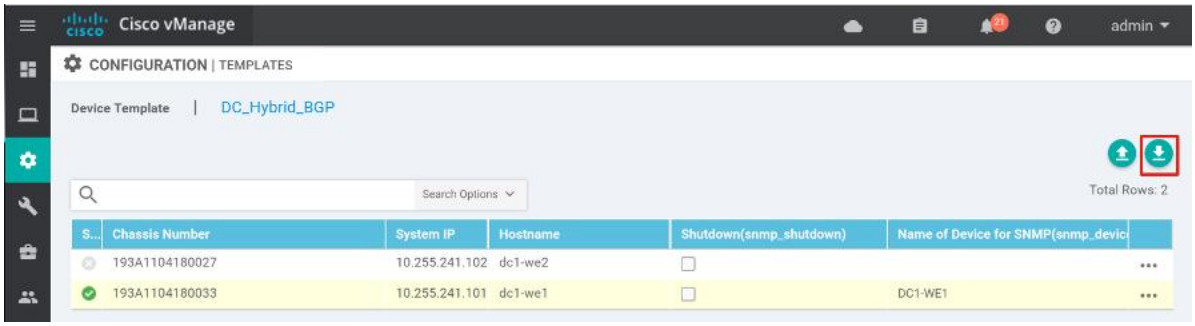
Variable	Value
Hostname(system_host_name)	dc1-we1

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)	☐
Console Baud Rate (bps) (system_console_baud_rate)	115200
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_x|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_x|x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	10.4.1.6/30
Preference(vpn_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_x|x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.167/23
AS Number(lan_bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(lan_bgp_router_id)	10.255.241.101

Network Prefix(lan_bgp_network_lo_addr|maskbits)	10.255.241.101/32
Address(lan_bgp_neighbor1_addr)	10.4.1.9
Address(lan_bgp_neighbor2_addr)	10.4.1.13
Description(lan_bgp_neighbor1_description)	Agg-Switch1
Description(lan_bgp_neighbor2_description)	Agg-Switch2
Shutdown(lan_bgp_neighbor1_shutdown)	☐
Shutdown(lan_bgp_neighbor2_shutdown)	☐
Remote AS(lan_bgp_neighbor1_remote_as)	65112
Remote AS(lan_bgp_neighbor2_remote_as)	65112
Password(lan_bgp_neighbor1_password)	cisco123
Password(lan_bgp_neighbor2_password)	cisco123
Interface Name(lan_int1_x|x)	ge0/4
Description(lan_int1_description)	To DC1-SW1 G1/0/11
Shutdown(lan_int1_shutdown)	☐
IPv4 Address(lan_int1_ip_addr|maskbits)	10.4.1.10/30
Interface Name(lan_int2_x|x)	ge0/5
Description(lan_int2_description)	To DC1-SW2 G1/0/11
IPv4 Address(lan_int2_ip_addr|maskbits)	10.4.1.14/30
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.101/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-WE1
Location of Device(snmp_device_location)	Datacenter 1

6. Select Update.

7. 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 you entered earlier will not be available and you will need to enter them 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

8. 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_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-we1 device was already filled out manually, those values are already populated in the spreadsheet.

9. Fill out the variable values for dc1-we2, then save the .csv file. Keep it in .csv format when saving. Fill in the variable values as listed in the following table.

Data center WAN Edge 2 device template variable values

Variable	Value
Hostname(system_host_name)	dc1-we2
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)	☐
Console Baud Rate (bps)(system_console_baud_rate)	115200
Address(vpn0_mpls_next_hop_ip_addr)	10.4.2.1
Address(vpn0_inet_next_hop_ip_addr)	10.4.2.5

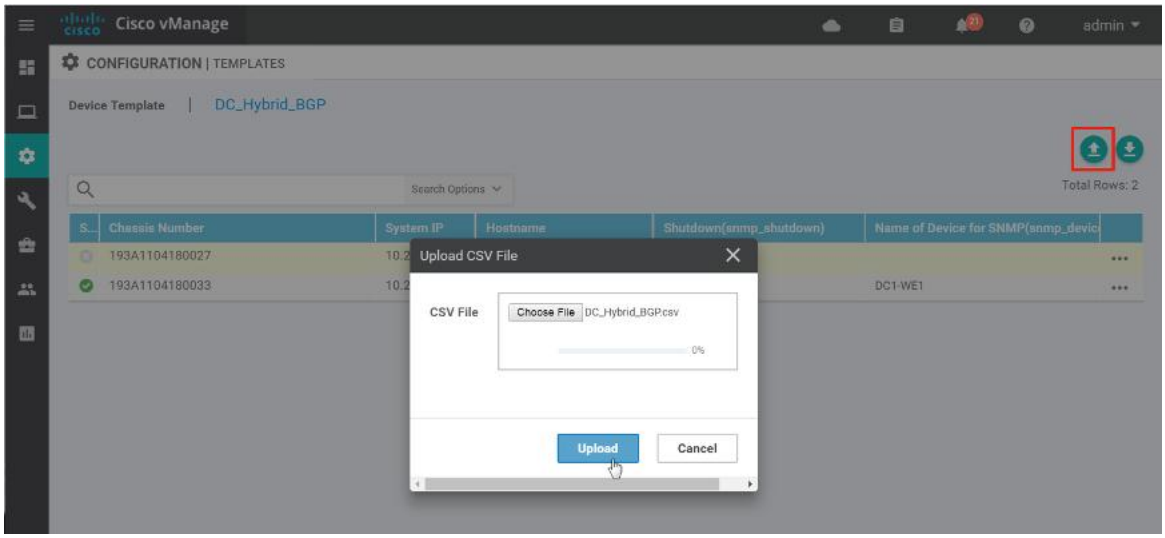
Interface Name(vpn0_mpls_int_x|x)	ge0/2
IPv4 Address(vpn0_mpls_int_ip_addr|maskbits)	10.4.2.2/30
Preference(vpn0_mpls_tunnel_ipsec_preference)	0
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_x|x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	10.4.2.6/30
Preference(vpn_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_x|x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.168/23
AS Number(lan_bgp_as_num)	65113
Shutdown(lan_bgp_shutdown)	☐
Router ID(lan_bgp_router_id)	10.255.241.102
Network Prefix(lan_bgp_network_lo_addr|maskbits)	10.255.241.102/32
Address(lan_bgp_neighbor1_addr)	10.4.2.9
Address(lan_bgp_neighbor2_addr)	10.4.2.13
Description(lan_bgp_neighbor1_description)	Agg-Switch1
Description(lan_bgp_neighbor2_description)	Agg-Switch2
Shutdown(lan_bgp_neighbor1_shutdown)	☐
Shutdown(lan_bgp_neighbor2_shutdown)	☐
Remote AS(lan_bgp_neighbor1_remote_as)	65112
Remote AS(lan_bgp_neighbor2_remote_as)	65112
Password(lan_bgp_neighbor1_password)	cisco123
Password(lan_bgp_neighbor2_password)	cisco123

Interface Name(lan_int1_gex/x)	ge0/4
Description(lan_int1_description)	To DC1-SW1 G1/0/12
Shutdown(lan_int1_shutdown)	☐
IPv4 Address(lan_int1_ip_addr/maskbits)	10.4.2.10/30
Interface Name(lan_int2_gex/x)	ge0/5
Description(lan_int2_description)	To DC1-SW2 G1/0/12
IPv4 Address(lan_int2_ip_addr/maskbits)	10.4.2.14/30
Shutdown(lan_int2_shutdown)	☐
IPv4 Address(lo0_int_ip_addr/maskbits)	10.255.241.102/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-WE2
Location of Device(snmp_device_location)	Datacenter 1

10. Select the upload arrow in the top right corner of the screen to upload the .csv file.

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

12. Select the Upload Button. File Uploaded Successfully should appear in green at the top of the screen.



13. You can scroll to the right and view or modify the values of the 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

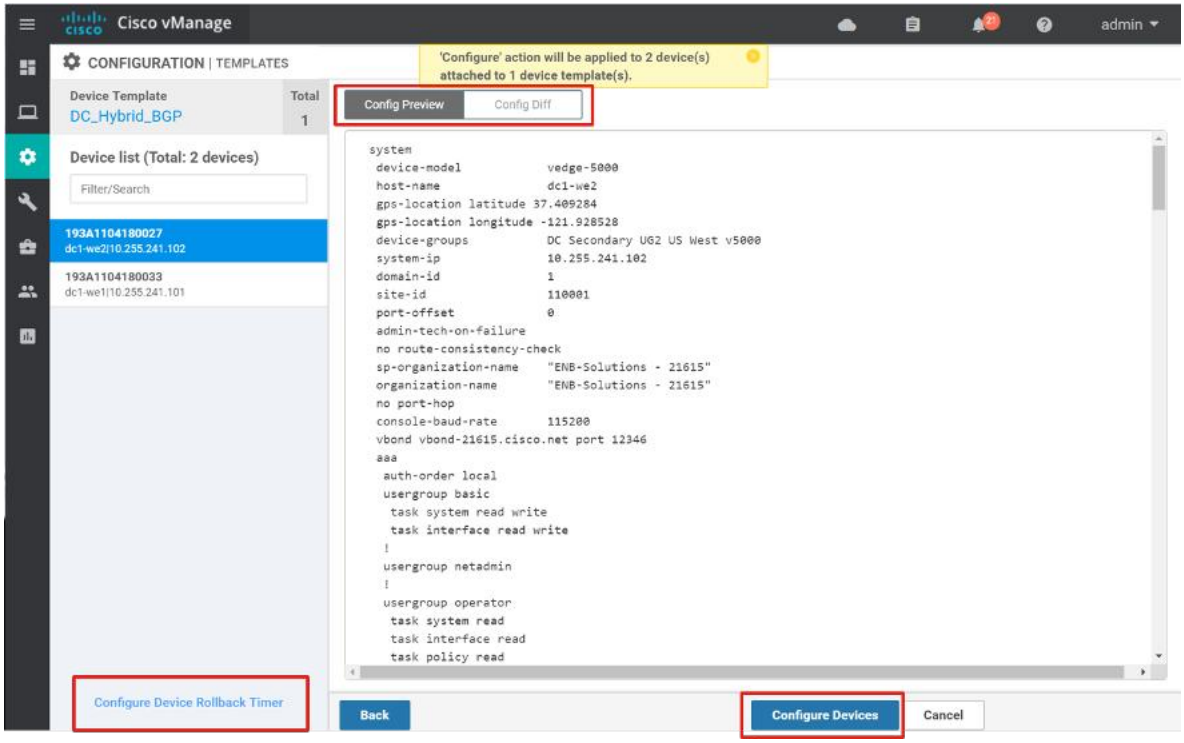
of the input variables and view or modify their values. Alternatively, you can modify the variable values by uploading a modified .csv file.

14. 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.

15. 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 WAN Edge 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.

16. 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 WAN Edge 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).

17. Back at the Config Preview page, select Configure Devices.

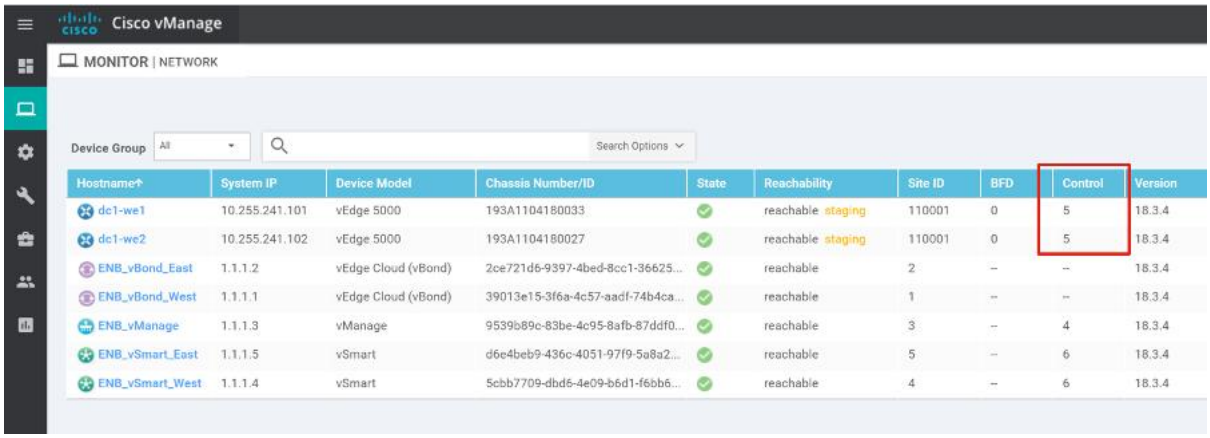


18. A pop-up window says, Committing these changes affects the configuration on 2 devices. Are you sure you want to proceed? Select the check box to Confirm configuration changes on 2 devices. Select OK.

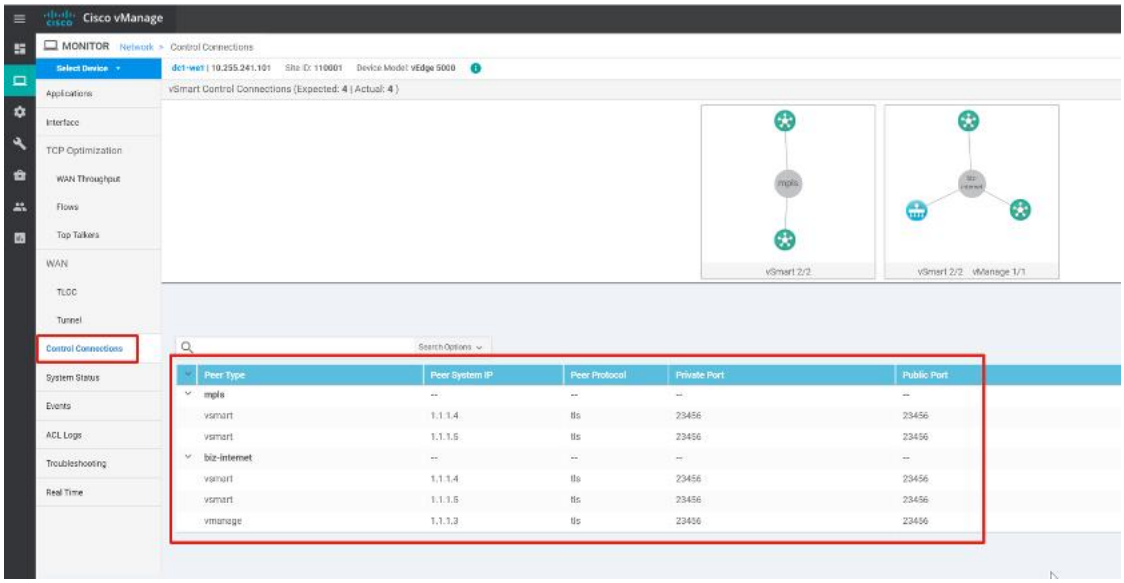
The configuration then gets pushed out to both devices. When complete, vManage should indicate success.

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

19. Go to Monitor>Network. From the table, you can see that dc1-we1 and dc1-we2 are both reachable and have a total of five control connections each.



20. Click on dc1-we1. Select on the left-hand side, 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 WAN Edge 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 WAN Edge 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 on the WAN Edge that will:

- Define a route-policy for BGP to filter any incoming prefixes on the LAN side for the MPLS transport (192.168.0.0/16 le 32, 10.101.1.0/30, 10.104.1.0/30, 10.105.1.0/30) and for the links to the CE router (10.4.1.0/30 and 10.4.2.0/30).
- Within the route-policy for BGP, match and accept route prefixes with a community of 101:101 (Non-SD-WAN-Sites).
- 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 netflow/cflowd, so the WAN Edge 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 WAN Edge router to discover, monitor, and track the applications running on the LAN. This enhances the application information that appears within the vManage GUI.

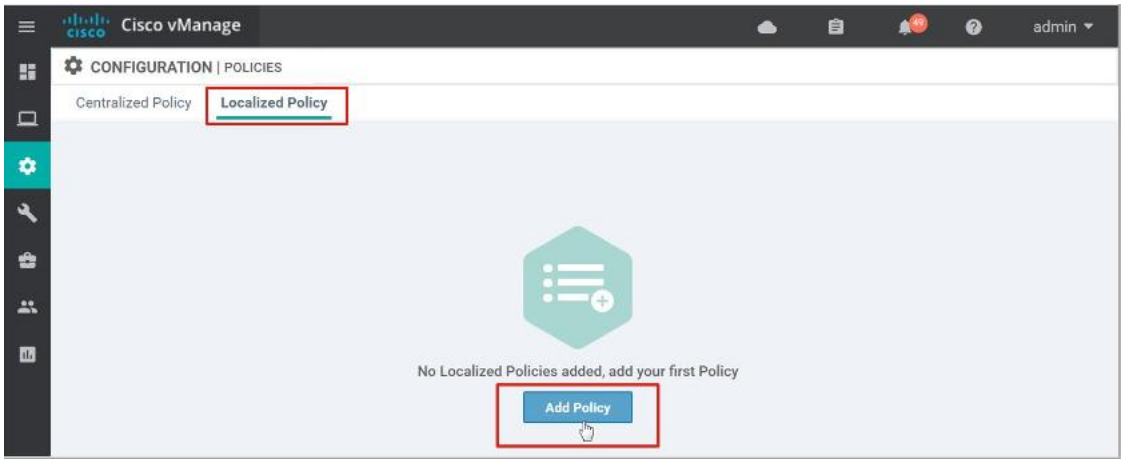
You will create a route-policy to apply to the BGP neighbors on the LAN in the datacenter for this example. Lists are defined first, followed by route policy. For each route policy, sequences are defined, each with a match/action pair. Each route policy is evaluated from top to bottom from low to high 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.

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. If a device template has been attached to a device and you try to update one of it's feature templates with a policy element but a policy has not yet been attached, the configuration update will fail.

Follow these steps to creat a localized policy.

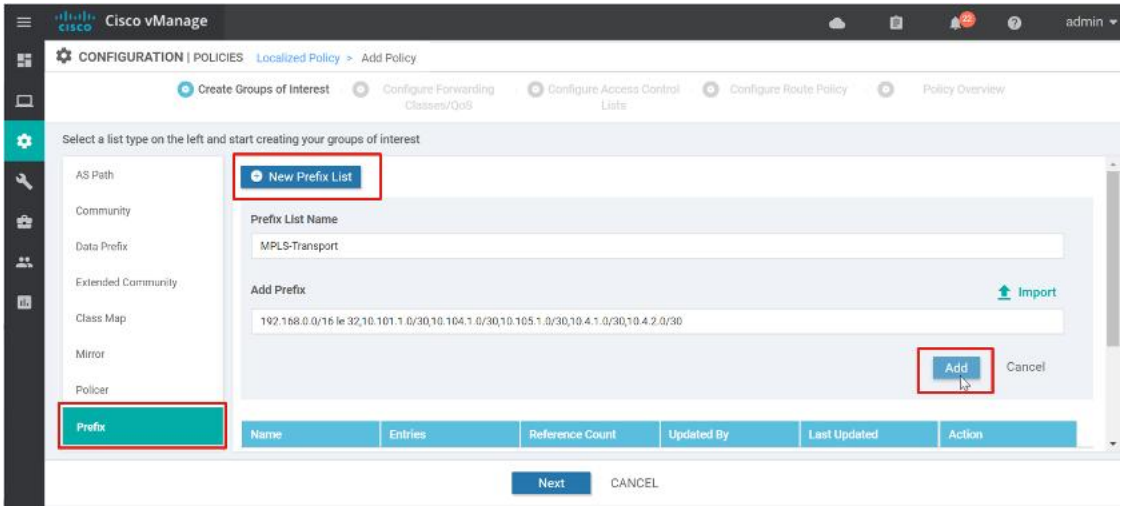
1. From the vManage GUI, go to Configuration>Policies and select the Localized Policy tab.
2. Select the Add Policy button.



Tech tip: Note that before the vManage 18.2 code version, the localized policy is CLI-based only. You can still configure the policy via CLI by clicking on the **Custom Options** drop-down box in the upper right corner and selecting **CLI Policy**.

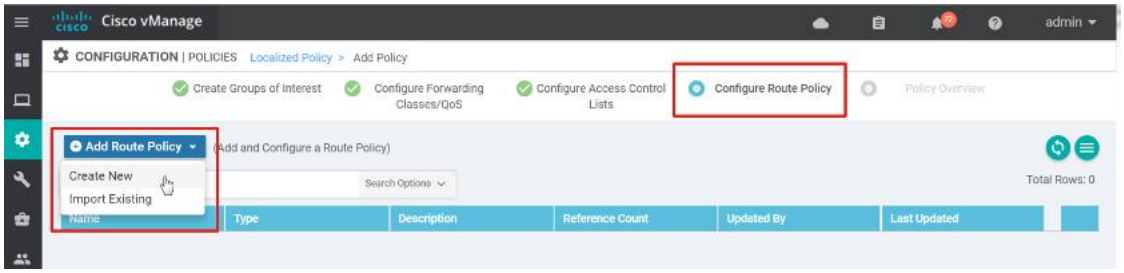
The first step in creating a localized policy is to create groups of interest. In the example requirements, define a prefix list, a community list, and an AS-PATH list.

3. Select Prefix on the left and then click on the New Prefix List button.
4. Under Prefix List Name, type MPLS-Transport in the text box.
5. Under Add Prefix, type 192.168.0.0/16 le 32,10.101.1.0/30,10.104.1.0/30,10.105.1.0/30,10.4.1.0/30,10.4.2.0/30 in the text box.
6. Click the Add button.

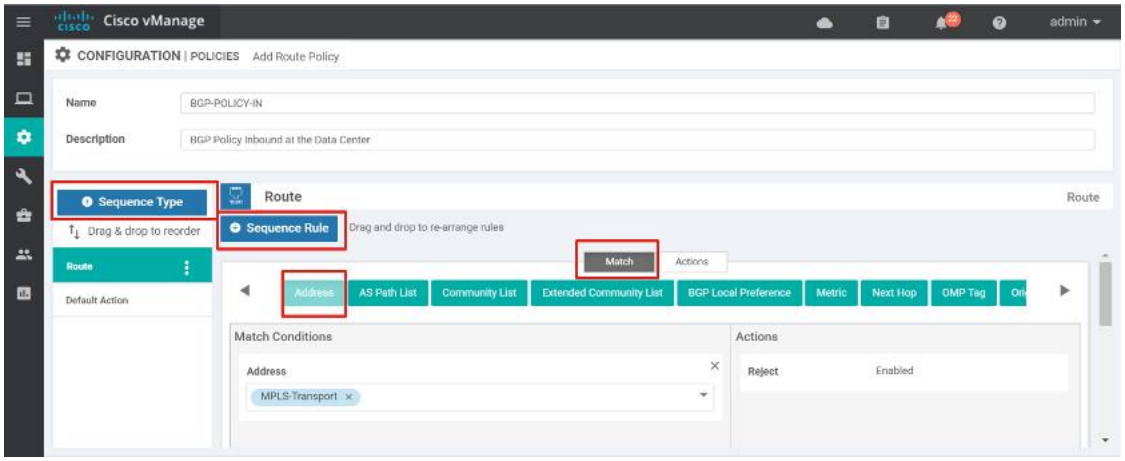


7. Select Community on the left-side and then click on the New Community List button.
8. Under Community List Name, type Non-SD-WAN-Sites in the text box.

9. Under Add Community, type 101:101 in the text box.
10. Click the Add button.
11. Select AS Path on the left-side and then click on the New AS Path List button.
12. Under AS Path List Name, type Local-Routes in the text box.
13. Under Add AS Path, type ^65112$ in the text box.
14. Click the Add button.
15. Click the Next button three times until you come to the Configure Route Policy page.
16. Click the Add Route Policy button and select Create New.



17. Next to Name, type the name of the route-policy (BGP-POLICY-IN), and next to Description, type a description (BGP Policy Inbound at the Data Center).
18. Select Sequence Type on the left side and click on Sequence Rule.
19. Ensure the Match box is selected and select Address. Under Match Conditions, select MPLS-Transport in the drop-down text box.



20. Keep the default reject action for this match condition. Click on the Save Match and Actions button.
21. Click on Sequence Rule to add the next match/action pair.

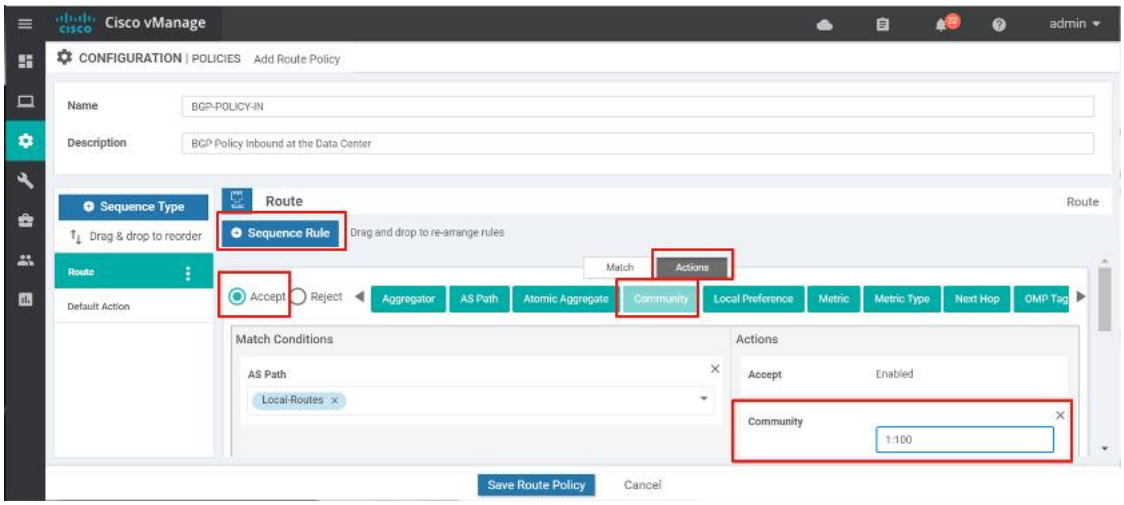
22. Ensure the Match box is selected and select Community List. Under Match Conditions, select Non-SD-WAN-Sites in the drop-down text box.

23. Select the Actions box and select the Accept radio button. Click on the Save Match and Actions button.

24. Click on Sequence Rule to add the next match/action pair.

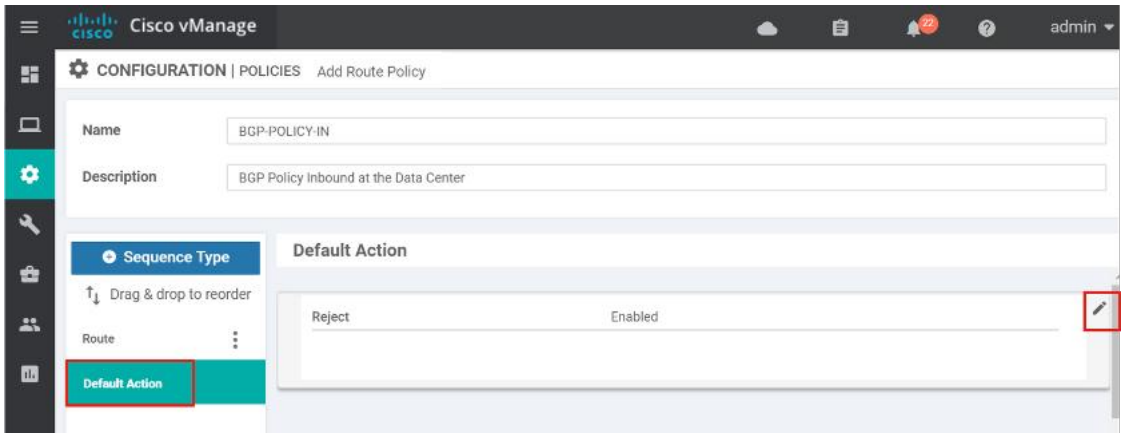
25. Ensure the Match box is selected and select AS Path List. Under Match Conditions, select Local-Routes in the drop-down text box.

26. Select the Actions box and select the Accept radio button. Select the Community box and type 1:100 in the text box. This community will be set when the action is met.



27. Click on the Save Match and Actions button.

28. Select Default Action on the left side. Keep it at the default setting which is to reject if no match occurs. To change, select the pencil icon to the far right, select Accept or Reject, and then click on Save Match and Actions.

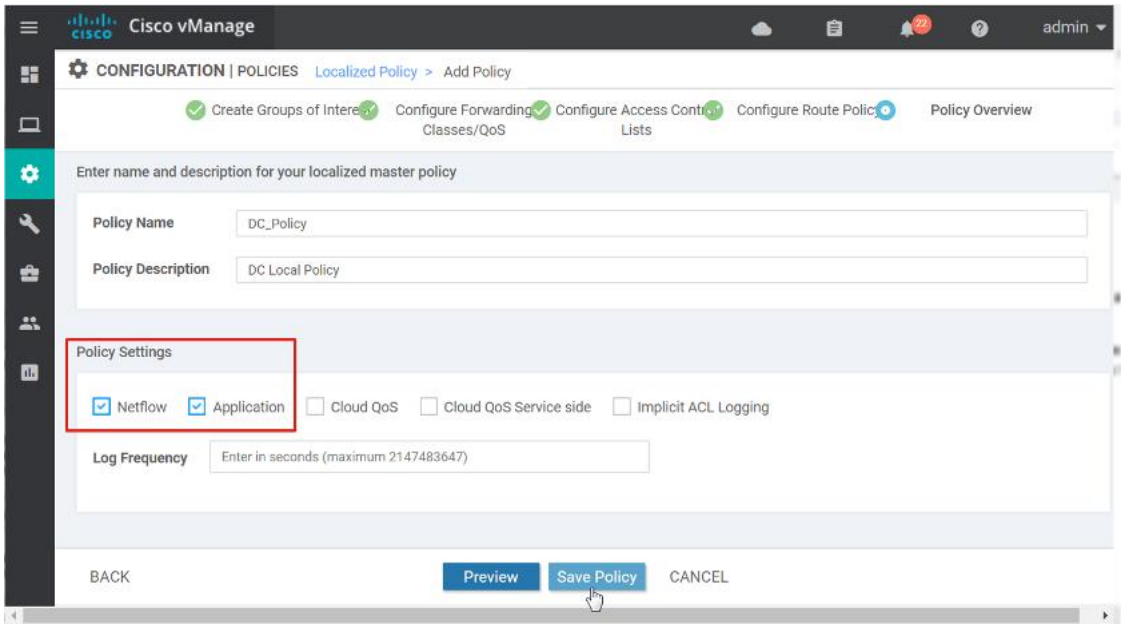


29. Click the Save Route Policy button.

30. Click Next.

31. Type in the Policy Name (DC_Policy) and Policy Description (DC Local Policy).

32. Under the Policy Settings section, select the Netflow checkbox to enable Netflow or Cflowd, and select the Application checkbox to turn on application visibility.



33. Optionally, click on the Preview button to see the policy that will be pushed to the WAN Edge router.

34. Click on Save Policy.

Tech tip: To modify the **DC_Policy** just created, you can go to Configuration>Localized Policy, select ... the right of the policy, and select Edit from the drop-down list. You will be able to add QoS configurations, access control lists, and additional route policies. If you need to create additional lists, or want to create standalone QoS configurations, access control lists, and route polices that you can later import into a localized policy, select the Custom Options button in the upper right corner of the main policy page.

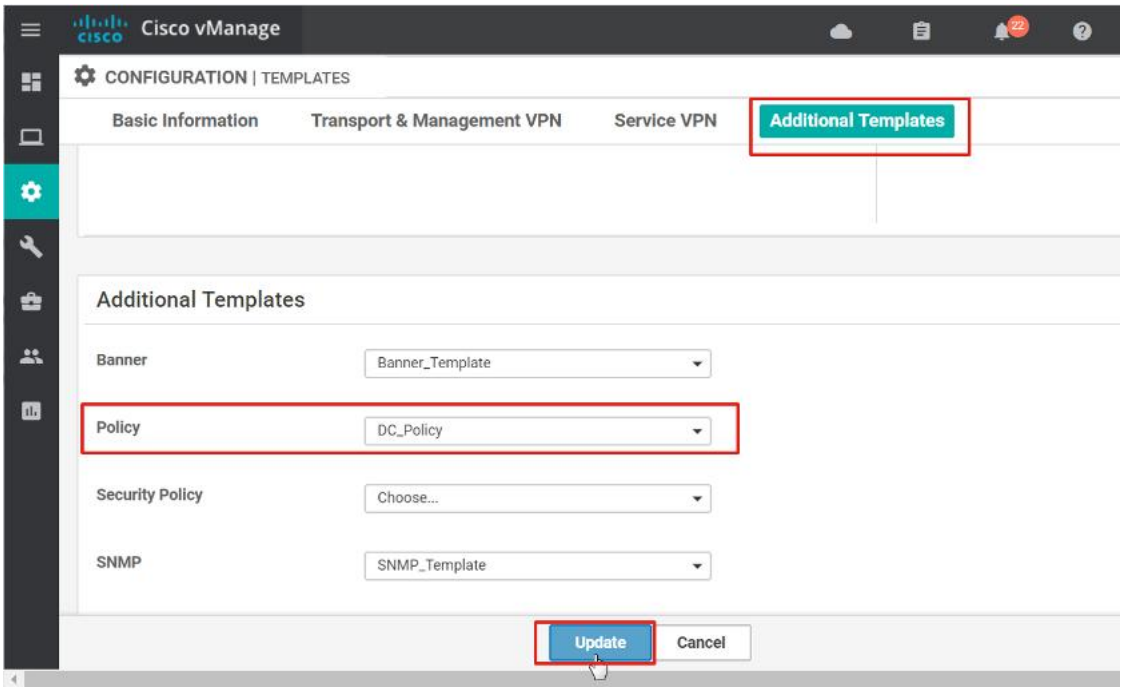
Procedure 13: Attach localized policy to a device template

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 WAN Edge router.

1. Go to Configuration>Templates and ensure the Device tab is selected. Next to the template, DC_Hybrid_ BGP, select ... to the right, and select Edit.

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

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



4. There are no variables to define, so select Next, then Configure Devices.

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

6. The policy is pushed to the WAN Edge routers and the status should indicate success.

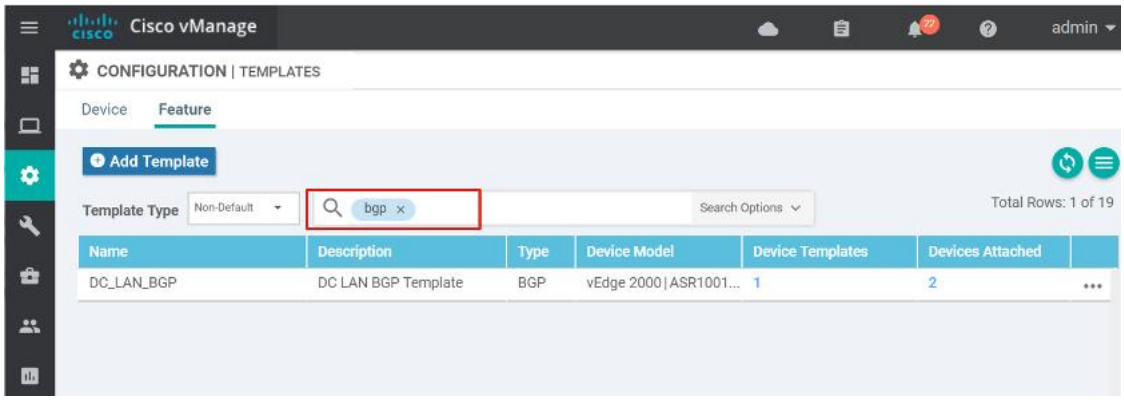
Procedure 14: Add localized policy references in the feature templates

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

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

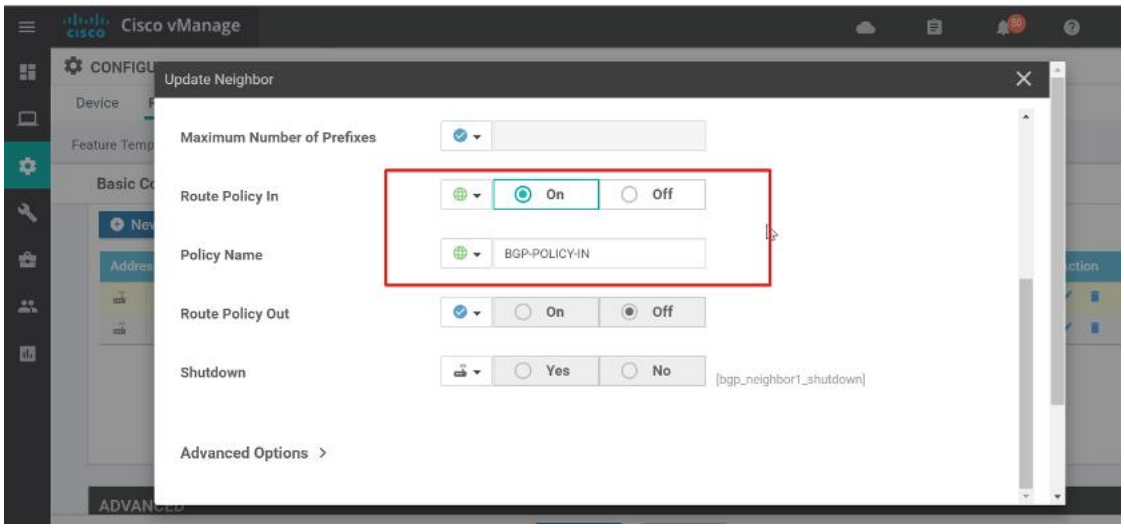
2. In the search text box, type in bgp and press the return key. The templates are filtered for the keyword in the Name, Description, Type, and Model columns.

3. Select ... to the right of the template, DC_LAN_BGP, and select Edit.



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

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



6. Select Save Changes.

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

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 WAN Edge router.

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

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

Procedure 15: Bring vEdge devices out of staging mode

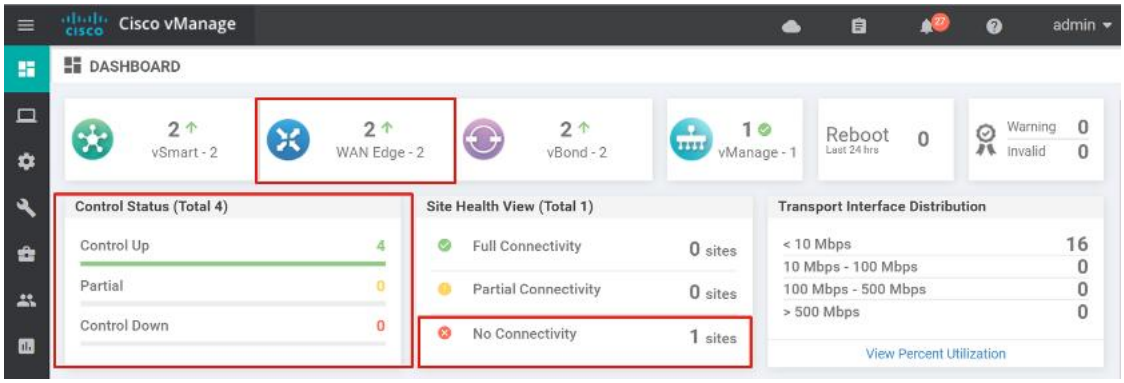
If the WAN Edge routers were initially put into staging mode, they can be brought online and made operational. This can be done at any time.

1. Go to Configuration>Certificates, find the WAN Edge routers just configured (`dc1-we1` and `dc1-we2`), and select Valid for each of them.

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

3. Once they are both valid, select the Send to Controllers button so that the controllers have the latest authorized device list. The WAN Edge 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 WAN Edge routers are in a down state. This is because no other sites are yet online and the two data center WAN Edge devices will not form BFD sessions with each other because they are both configured for the same site ID.



Deploying remote sites

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 WAN Edge routers and then the ZTP (for vEdge) or PnP (for IOS XE SD-WAN) process will be used to bring the WAN Edge routers online. The routers will be upgraded through the automated provisioning 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.

The example policy should include:

- Flow visibility
- App visibility, or Deep Packet Inspection (DPI)

- Route policies for BGP at the dual-WAN Edge router sites. One policy should advertise only the TLOC extension link subnet so that routers using the MPLS transport can connect to the WAN Edge 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 WAN Edge router gives up VRRP primary status.

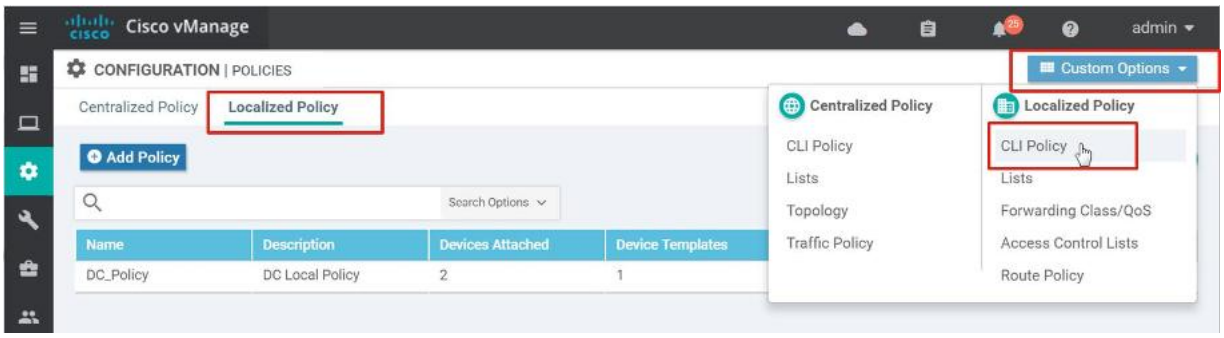
Tech tip: In vManage version 18.3, there are a few limitations to using the local policy wizard. First, you must include a reference to a QoS policy, ACL, or route policy in order to create a valid local policy; you cannot just turn on application or flow visiibility or even include just a prefix-list to be used by the routing processes. Second, you do not have the ability to use variables in a policy so that the same route policy can be applied to different WAN Edge devices, each using site-specific information. Note that within the policy wizard GUI, you can still create multiple route policies and apply different route policies to different WAN Edge devices using a device-specific variable in the template to reference the route policy if need be. An alternative to using the local policy wizard is to use a localized CLI policy instead, which you can configure by clicking the **Custom Options** button in the upper right corner of the localized policy main page. You can even use the policy wizard to build a local policy, and you can choose to preview that policy. Take the preview CLI, create a CLI policy with it, and modify it from there.

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 WAN Edge routers configured for BGP (to advertise the TLOC-extension subnet) or OSPF. Branch_Policy is used on non-OSPF and non-BGP WAN Edge routers and is used for flow and application visibility and for default route tracking for VRRP. Since the policy wizard was shown for the data center local policy, CLI local policies are used for the branches.

Note that when you apply a localized policy to a device template that gets applied to multiple WAN Edge 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.

Follow these steps to create localized policy for branches:

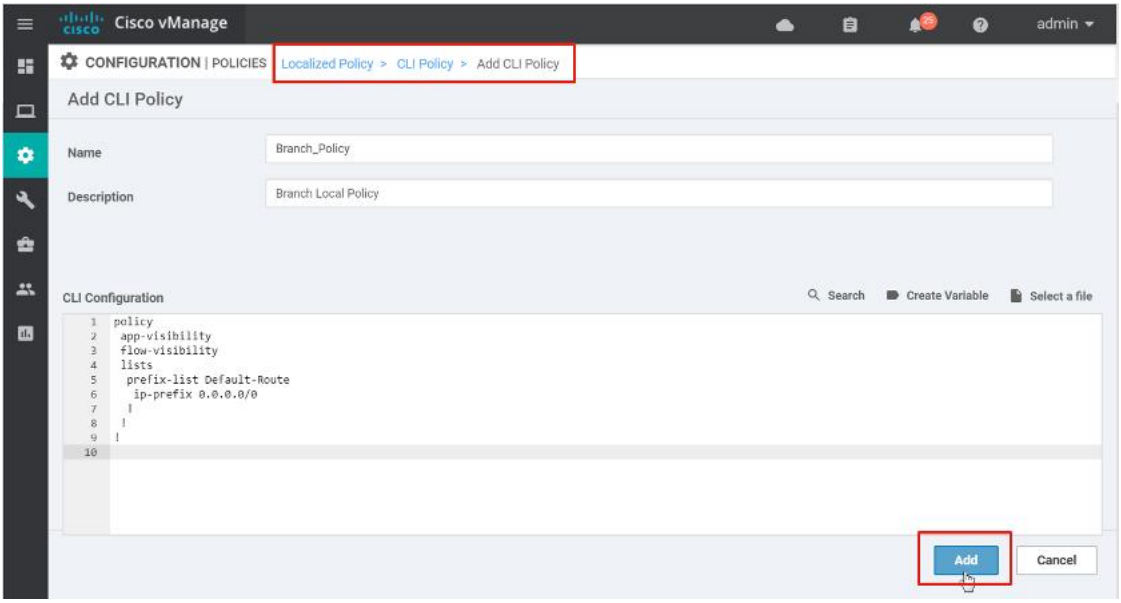
1. From the vManage GUI, go to Configuration>Policies and select the Localized Policy tab.
2. Click the Custom Options button in the top right corner of the GUI and select CLI Policy from the drop-down menu.



3. Click the Add Policy button.
4. Type in the Name (Branch_Policy) and Description (Branch Local Policy).
5. Type or paste in the following CLI:

```
policy
 app-visibility
 flow-visibility
 lists
  prefix-list Default-Route
   ip-prefix 0.0.0.0/0
  !
 !
!
```

6. Select Add to complete and save the localized policy.



7. Add the second branch local policy. Select the Add Policy button.
8. Type in the Name (Branch_BGP_OSPF_Policy) and Description (Branch BGP and OSPF Local Policy).
9. Type or paste in the following CLI:

```
policy
 app-visibility
```

```
 flow-visibility
 lists
  prefix-list Default-Route
   ip-prefix 0.0.0.0/0
!
 route-policy DENY-ALL
  sequence 10
   action reject
   !
  !
  default-action reject
```

10. 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 WAN Edge 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.

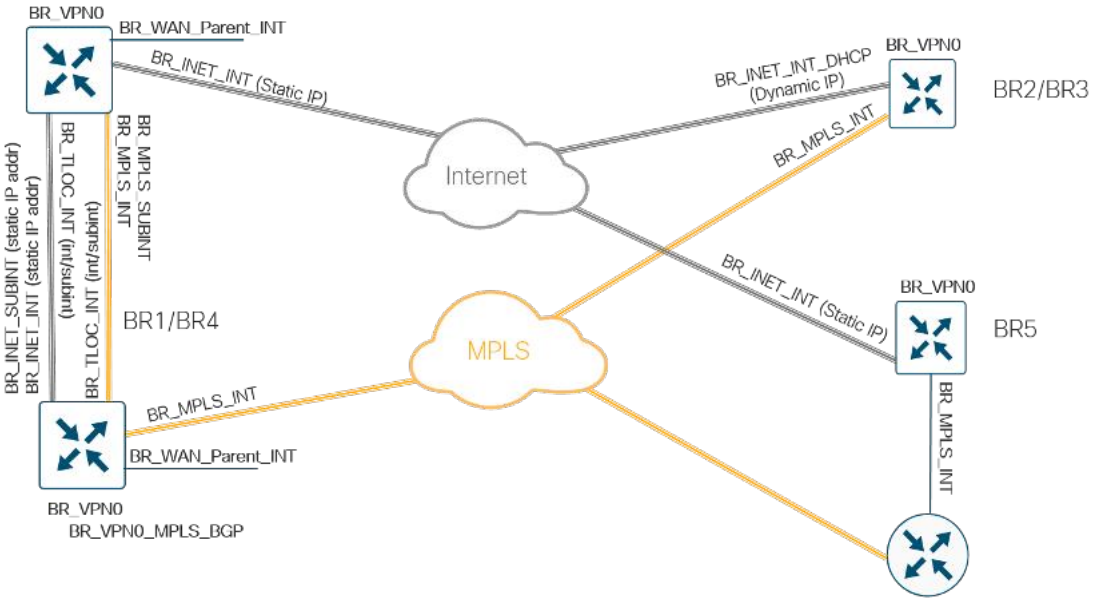
Following are the feature templates needed for the branch transport side:

- 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 extension interface or subinterface, which can be combined into one template (BR_TLOC_EXT_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 WAN Edge router to communicate the TLOC-extension link subnet to the MPLS transport (BR_VPN0_MPLS_BGP for branches 1 and 4).

Figure 15 Branch WAN Edge transport side templates



Branch VPN 0 Template

One VPN 0 template will be used for all the branch WAN Edge devices. When using DHCP for the Internet interface, technically only one static next hop will be needed for the default route prefix for the MPLS interface because the default route for the Internet interface is typically obtained dynamically. Instead of creating a separate VPN 0 template in the case of DHCP for the Internet IP address, the same template can be used for either case because the dynamic ip gateway should overwrite a statically-defined one when the interface is configured for DHCP.

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: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN

Template Name: BR_VPN0

Description: Branch Transport VPN 0

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

2. Select Save to complete the template.

Branch MPLS Interface Template

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

Select Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_MPLS_INT

Description: Branch MPLS Interface with Static IP

Branch VPN 0 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_x|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	Clear-Dont-Fragment	Global	On

4. Select Save to create the template.

Branch MPLS Subinterface Template

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_x|x.VLAN.

Select Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_MPLS_SUBINT

Description: Branch MPLS Subinterface with Static IP

Branch VPN 0 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_x|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	Clear-Dont-Fragment	Global	On

6. Select Save or Update to save the template.

Branch Internet Interface Template

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_INET_INT

Description: Branch Internet Interface with Static IP

Branch VPN 0 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_x|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	nat-enable
Advanced	Clear-Dont-Fragment	Global	On

8. Select Save to create the template.

Branch Internet DHCP Interface Template

9. Copy the last template created (BR_INET_INT). Edit by changing the parameter IPv4 radio button from static to dynamic. Also be certain to change the DHCP setting under Allow Service to On. Without this, the Internet interface may not get a dynamic IP address and connection to the controllers could be lost over the interface.

Template Name: BR_INET_INT_DHCP

Description: Branch Internet Interface with DHCP IP

Branch VPN 0 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	On
Allow Service	NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	nat-enable
Advanced	Clear-Dont-Fragment	Global	On

10. Select Update to save the template.

Branch Internet Subinterface Template

11. Copy the Internet template static template created (BR_INET_INT). Edit by changing the interface name variable to vpn0_inet_int_x|x.VLAN.

Template Name: BR_INET_SUBINT

Description: Branch Internet Subinterface with Static IP

Branch VPN 0 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_x|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	nat-enable
Advanced	Clear-Dont-Fragment	Global	On

12. Select Update to save the template.

Branch TLOC Extension Interface Template

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_TLOC_EXT_INT

Description: Branch TLOC Extension Interface/Subinterface

Branch VPN 0 TLOC interface/subinterface feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_tloc_ext_int_shutdown
	Interface Name	Device Specific	vpn0_tloc_ext_int_x|x_or_x|x.VLAN
	Description	Global	TLOC Extension Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 address	Device-specific	vpn0_tloc_ext_int_ip_addr|maskbits
Advanced	TLOC extension	Device-specific	vpn0_tloc_ext_wan_int_x|x

14. Select Save to create the template.

Branch WAN Parent Interface Template

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_WAN_Parent_INT

Description: Branch WAN Parent Interface

Branch VPN 0 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_x|x
	Description	Global	WAN Parent Interface
Advanced	IP MTU	Global	1504

16. Select Save to complete the template.

Branch VPN 0 MPLS BGP Template

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/BGP

Template Name: BR_VPN0_MPLS_BGP

Description: Branch VPN 0 MPLS BGP to Provider

Branch VPN 0 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	vpn0_bgp_router_id
IPv4 Unicast Address Family	Maximum Paths	Global	2
	Address-Family	Drop-down	ipv4-unicast
	Network/Network Prefix	Device Specific	bgp_tloc_ext_prefix_to_advertise
Neighbor	Address	Device Specific	vpn0_bgp_neighbor_addr
	Description	Device Specific	vpn0_bgp_neighbor_description
	Remote AS	Device Specific	vpn0_bgp_neighbor_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	DENY-ALL
	Shutdown	Device Specific	vpn0_bgp_neighbor_shutdown

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.

Starting with 18.2 code, some template parameters can be marked optional. This allows you to combine templates where in the past you may have had to define multiple templates.

The service VPN template for branch 5 contains static routes, but the service VPN for the other branches do not, so now all branches can share a common service VPN template by marking the static routes as optional configurations inside the template.

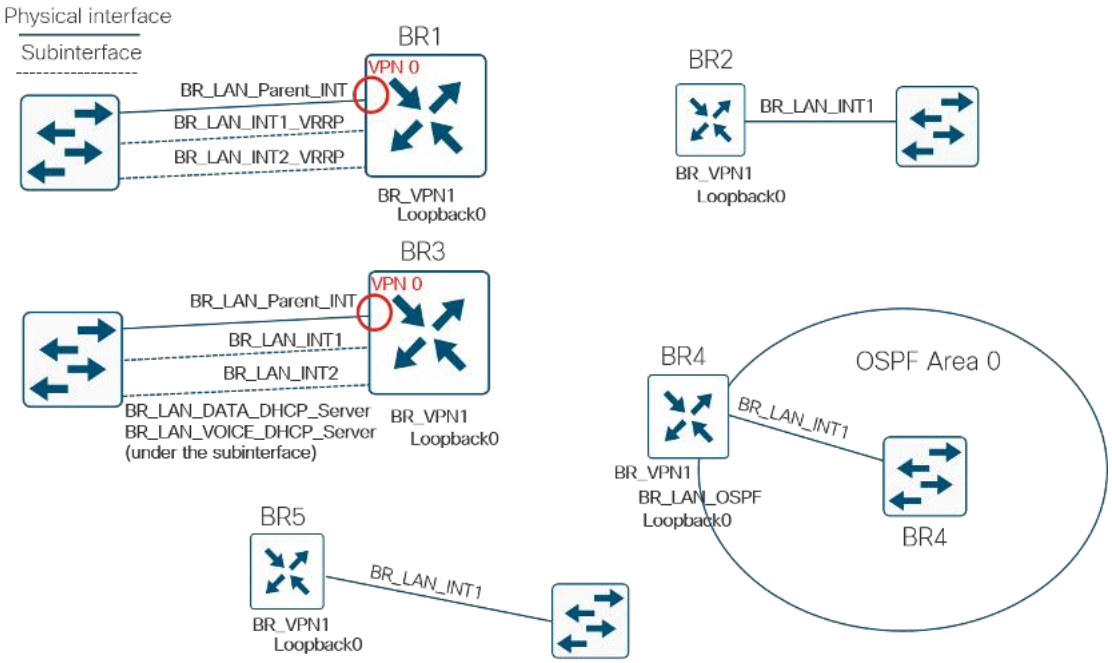
Tech tip: While you can also mark VRRP configuration as optional inside a VPN Ethernet Interface template, when you try to deploy the template in the tested release, VRRP is treated like a required configuration and you won't be able to deploy the template until the variables associated with the VRRP configuration are provided. As a work around to this, create two different VPN Ethernet Interface templates, one with VRRP configured and one without.

The LAN interfaces associated with VPN 1 can be either physical or subinterfaces. One VPN Ethernet interface 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 WAN Edge router functions as a DHCP server for the LAN segment. If you have two LAN interfaces on a single WAN Edge 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 template: - One base service VPN feature template can cover the branch requirements (BR_VPN1 for branches 1-5). Static routes will be added into the template and marked as optional 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. You need to create two templates, 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_LAN_OSPF for branch 4).
- Loopback0 - The VPN Ethernet interface feature template for loopback 0 (already configured) is needed under VPN 1 (branches 1-5)

Figure 16 Branch WAN Edge service side templates



BR_VPN1

One aggregate prefix for the remote site is advertised into OMP instead of multiple site routes. Note that even though you can mark this prefix as an optional configuration, once you turn aggregation on, you need at least one aggregate prefix defined. Redistribute connected is turned on to advertise the loopback interface for reachability to and from the data center for management.

A static route is configured and marked optional so that it can be used on branch 5 to reach the LAN segments behind a layer 3 switch. Instead of redistibuting static routes into OMP, the site is advertising the aggregate prefix instead.

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN

Template Name: BR_VPN1

Description: Branch VPN1

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
IPv4 Route [Mark as Optional Row]	Prefix	Device Specific	vpn1_lan_static_route_prefix|mask bits
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn1_lan_next_hop_ip_addr

2. Select Save to create the template.

Branch LAN Interface 1 Template

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT1

Description: Branch LAN Interface 1

Branch VPN 1 interface 1 feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10

4. Select Save to create the template.

Branch LAN Interface 2 Template

5. Add a new feature template using the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT2

Description: Branch LAN Interface 2

Branch VPN 1 interface 2 feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10

6. Select Save to complete the template.

BR_LAN_INT1_VRRP

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

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT1_VRRP

Description: Branch LAN Interface 1 VRRP

Branch VPN 1 interface 1 VRRP feature template settings

Section	Parameter	Type	Variable/value
	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP	Group ID	Global	1
	Priority	Device Specific	lan_int1_vrrp_priority
	Track OMP	Global	Off
	Track Prefix List	Global	Default-Route

	IP Address	Device Specific	lan_int1_vrrp_ip_addr

8. Select Save to create the template.

BR_LAN_INT2_VRRP

9. Add a new feature template using the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT2_VRRP

Description: Branch LAN Interface 2 VRRP

Branch VPN 1 interface 2 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP	Group ID	Global	2
	Priority	Device Specific	lan_int2_vrrp_priority
	Track OMP	Global	Off
	Track Prefix List	Global	Default-Route
	IP Address	Device Specific	lan_int2_vrrp_ip_addr

10. Select Save to create the template.

Branch LAN Parent Interface Template

11. Add a new feature template using the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_Parent_INT

Description: Branch LAN Parent Interface

Branch VPN 1 LAN parent interface template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_parent_int_shutdown
	Interface Name	Device Specific	lan_parent_int_x|x
	Description	Global	LAN Parent Interface
Advanced	IP MTU	Global	1504

12. Select Save to complete the template.

Branch LAN Data VLAN DHCP Server Template

13. Add a new feature template using the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/DHCP Server

Template Name: BR_LAN_DATA_DHCP_Server

Description: Branch LAN DHCP Server for Data VLAN

Branch VPN 1 LAN DHCP Server for Data VLAN feature template

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

14. Select Save to complete the template.

Branch LAN Voice VLAN DHCP Server Template

15. 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 and the phones need to register with the Call Manager. Use the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/DHCP Server

Template Name: BR_LAN_VOICE_DHCP_Server

Description: Branch LAN DHCP Server for Voice VLAN

Branch VPN 1 LAN DHCP Server for Voice VLAN feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Address Pool	Device Specific	voice_dhcp_addr_pool|maskbits
	Exclude Addresses	Device Specific	voice_dhcp_addr_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

16. Select Update to save the template.

Branch LAN OSPF

17. Add a new feature template using the following parameters:

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/OSPF

Template Name: BR_LAN_OSPF

Description: Branch LAN OSPF

Branch LAN OSPF feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Router ID	Device Specific	lan_ospf_router_id
Redistribute	Protocol	Global	omp
Area	Area Number	Global	0
	Interface/Interface Name	Device Specific	lan_ospf_int_x|x
	Interface/Interface Cost	Device Specific	lan_ospf_int_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	lan_ospf_message_digest_key
Area Range	Address	Device Specific	lan_ospf_area_range_addr_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Global	On

18. 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 four general types of branches in this example network.

- Type A branch: Dual WAN Edge router site, hybrid configuration (MPLS and Internet), TLOC extension interfaces, layer 2 switch stack, VRRP
- Type B branch: Single WAN Edge router site, hybrid configuration (MPLS and Internet), single layer 2 LAN switch
- Type C branch: Dual WAN Edge router site, hybrid configuration (MPLS and Internet), TLOC extension interfaces, layer 3 switch, OSPF
- Type D branch: Single WAN Edge router site, hybrid configuration (MPLS and Internet), CE router, layer 3 switch

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

Configure the following device templates:

- Branch_A_MPLS_BGP_TLOCEXT_VRRP (branch 1, WAN Edge 1)
- Branch_A_INET_TLOCEXT_VRRP (branch 1, WAN Edge 2)
- Branch_B_MPLS_INET(DHCP) (branch 2)
- Branch_B_MPLS_INET(DHCP)_LAN(DHCP) (branch 3)
- Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF (branch 4, WAN Edge 1)
- Branch_C_INET_TLOCEXT_SubInt_OSPF (branch 4, WAN Edge 2)
- Branch_D_MPLS_CE_INET_LAN-Static-Routing (branch 5)

Branch_A_MPLS_BGP_TLOCEXT_VRRP

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

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

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

Device Model: ISR4351

Template Name: Branch_A_MPLS_BGP_TLOCEXT_VRRP

Description: Branch Dual WAN Edge Hybrid TLOC Extension with MPLS BGP and LAN-side Trunk and VRRP

4. Configure with the following feature templates:

Branch_A_MPLS_BGP_TLOCEXT_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	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN _INT1_VRRP
	VPN Interface	BR_LAN _INT2_VRRP
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy

SNMP		SNMP_Template

5. Select Create to create and save the template.

Branch_A_INET_TLOCEXT_VRRP

6. Select Create Template and select From Feature Template from the drop-down box.
7. Configure the device template with the following parameters:

Device Model: ISR4351

Template Name: Branch_A_INET_TLOCEXT_VRRP

Description: Branch Dual WAN Edge Hybrid TLOC Extension with INET and LAN-side Trunk and VRRP

Branch_A_INET_TLOCEXT_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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN _INT1_VRRP
	VPN Interface	BR_LAN _INT2_VRRP
	VPN Interface	Loopback0

Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

8. Select Create to create and save the template.

Branch_B_MPLS_INET(DHCP)

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

10. Configure the device template with the following parameters:

Device Model: ISR4331

Template Name: Branch_B_MPLS_INET(DHCP)

Description: Branch Single WAN Edge Hybrid Internet DHCP address with LAN Trunk

Branch_B_MPLS_INET(DHCP) 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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT_DHCP
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_Policy

SNMP		SNMP_Template

11. Select Create to create and save the template.

Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

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

13. Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

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

Branch_B_MPLS_INET(DHCP)_LAN(DHCP) 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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	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	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

14. Select Create

Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

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

16. Configure the device template with the following parameters:

Device Model: ISR4351

Template Name: Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

Description: Branch Dual WAN Edge Hybrid TLOC Extension SubInts with MPLS BGP and LAN-side OSPF

Branch_C_MPLS_BGP_TLOCEXT_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	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_SUBINT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template

	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

17. Select Create

Branch_C_INET_TLOCEXT_SubInt_OSPF

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

19. Configure the device template with the following parameters:

Device Model: vEdge 1000

Template Name: Branch_C_INET_TLOCEXT_SubInt_OSPF

Description: Branch Dual WAN Edge Hybrid TLOC Extension SubInts with INET and LAN-side OSPF

Branch_C_INET_TLOCEXT_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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_SUBINT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT

	VPN Interface	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

20. Select Create to create and save the template.

Branch_D_MPLS_CE_INET_LAN-Static-Routing

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

22. Configure the device template with the following parameters:

Device Model: vEdge 100 B

Template Name: Branch_D_MPLS_CE_INET_LAN-Static-Routing

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

Branch_D_MPLS_CE_INET_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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT

	VPN Interface	BR_INET_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

23. Select Create to create and save the template.

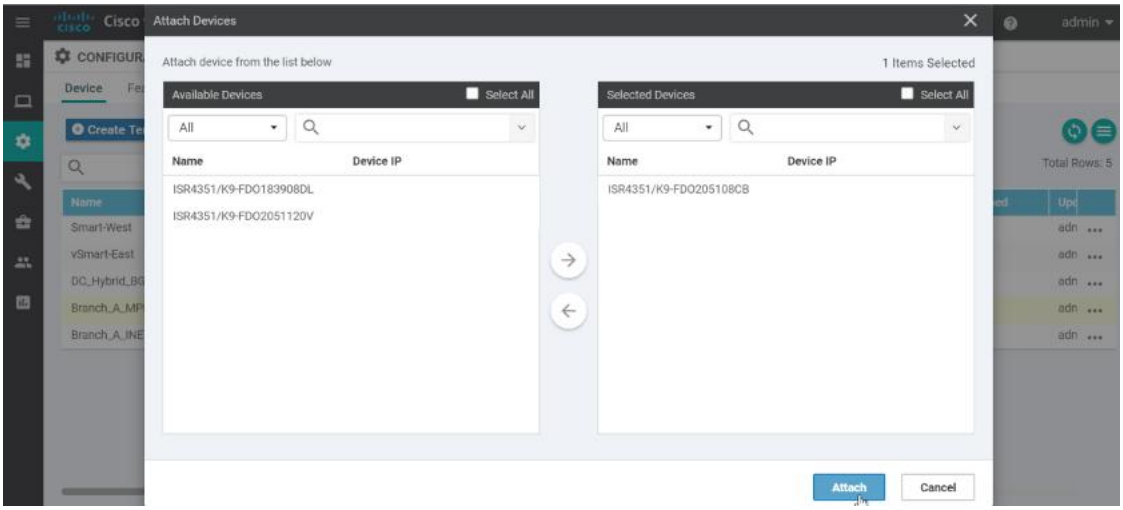
Procedure 5: Attach the device templates

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

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

2. Beside the desired template (Branch_A_MPLS_BGP_TLOCEXT_VRRP), select **...** and select Attach Devices.

3. Select branch 1 WAN Edge 1 connected to the MPLS transport, br1-we1. You will need to find the serial number associated with this device (ISR4351) because this device is not on the network yet. You can find the serial number on the outside of the chassis. Alternatively, on an IOS XE router, you can execute a show license udi on the console to see the serial number. For a vEdge router, you can execute a show hardware inventory on the console. The serial numbers of all of the ISR4351 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.



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.

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

Branch 1 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br1-we1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,ISR4K,US,West,UG5,Primary
System IP(system_system_ip)	10.255.241.11
Site ID(system_site_id)	112001
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	☑
Console Baud Rate (bps)(system_console_baud_rate)	9600
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_addr)	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
Network Prefix(bgp_tloc_ext_prefix_to_advertise)	10.101.1.0/30
Interface Name(vpn0_inet_int_x|x)	GigabitEthernet0/0
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_x|x)	GigabitEthernet0/0/2
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_ext_int_x|x_or_x|x.VLAN)	GigabitEthernet0/1/0
IPv4 Address(vpn0_tloc_ext_int_ip_addr|maskbits)	10.101.1.1/30
TLOC Extension(vpn0_tloc_ext_wan_int_x|x)	GigabitEthernet0/0/2
Shutdown(vpn0_tloc_ext_int_shutdown)	☐
Interface Name(lan_parent_int_x|x)	GigabitEthernet0/0/1
Shutdown(lan_parent_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_ x|x)	GigabitEthernet0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.143/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix)	10.101.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.10

Description(lan_int1_description)	Data Vlan
IPv4 Address(lan_int1_ip_addr|maskbits)	10.101.10.2/24
Shutdown(lan_int1_shutdown)	☐
Priority(lan_int1_vrrp_priority)	200
IP Address(lan_int1_vrrp_ip_addr)	10.101.10.1
Interface Name(lan_int2_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.20
Description(lan_int2_description)	Voice Vlan
IPv4 Address(lan_int2_ip_addr|maskbits)	10.101.20.2/24
Shutdown(lan_int2_shutdown)	☐
Priority(lan_int2_vrrp_priority)	200
IP Address(lan_int2_vrrp_ip_addr)	10.101.20.1
IPv4 Address(lo0_ip_addr|maskbits)	10.255.241.11/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-WE1
Location of Device(snmp_device_location)	Branch 1

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

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

8. Repeat steps 1-8 with the following templates. See Appendix G for the variable values.

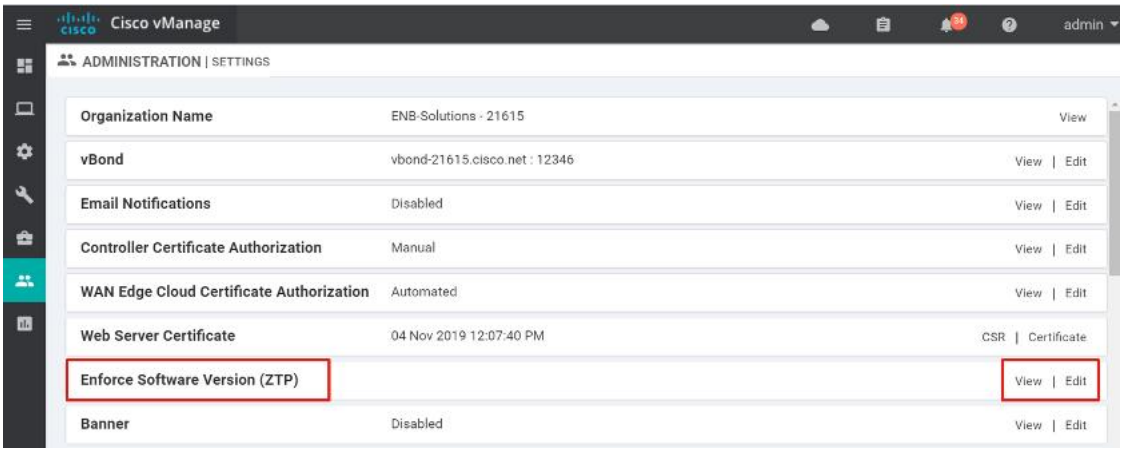
- BR1-WE2: Branch_A_INET_TLOCEXT_VRRP
- BR2-WE1: Branch_B_MPLS_INET(DHCP)
- BR3-WE1: Branch_B_MPLS_INET(DHCP)_LAN(DHCP)
- BR4-WE1: Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF
- BR4-WE2: Branch_C_INET_TLOCEXT_SubInt_OSPF
- BR5-WE1: Branch_D_MPLS_CE_INET_LAN-Static-Routing

Procedure 6: Bring remote vEdge routers online via ZTP

In this procedure, the vEdge in branch 4, br4-we2, 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.

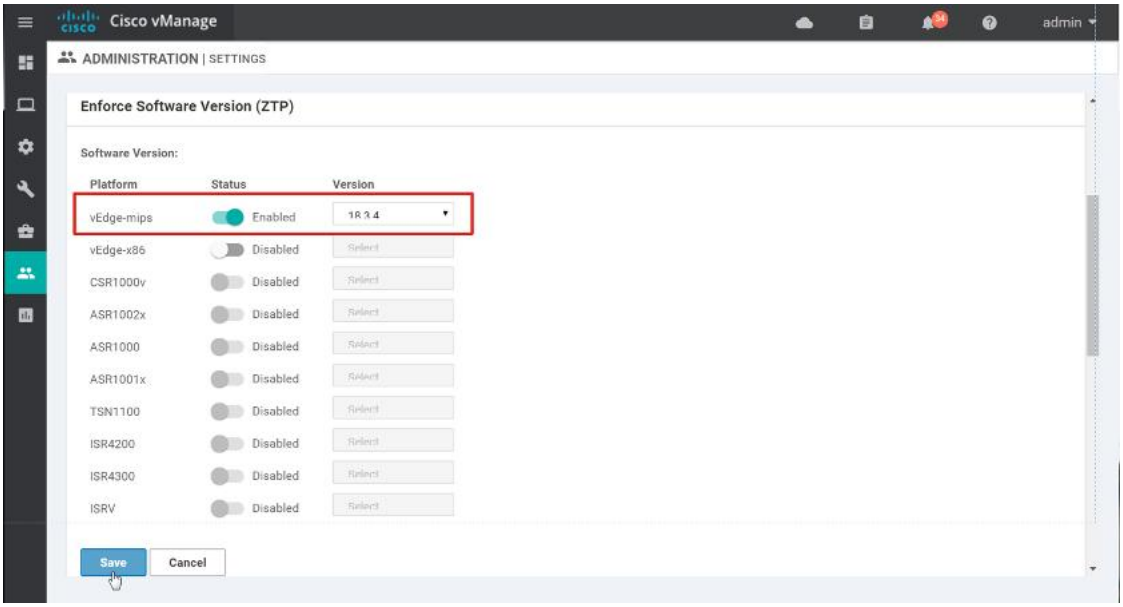
1. To check the code version for the vEdge router that comes online via ZTP, go to Administration>Settings from the vManage GUI. Find the Enforce Software Version (ZTP) configuration. Select Edit in the far right.



2. Under the expanded section, find the desired platform (vEdge-mips) and under Status, slide the bar to the right to change the status to Enabled. Under the Version column, choose the software version to upgrade (18.3.4). If the desired version is not listed as a choice to select, go to Maintenance>Software Repository to add the needed version. Note that the vEdge-mips option refers to Cisco the vEdge 100, 1000, and 2000 models, while the vEdge-x86 option refers to the Cisco vEdge Cloud and vEdge 5000 models.

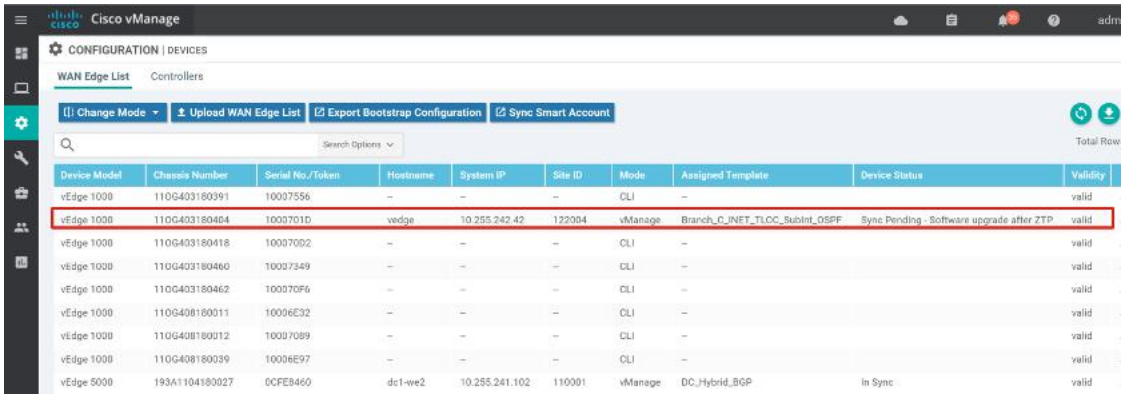
3. Select Save.

Tech tip: The vManage code version 18.3 does not support IOS XE SD-WAN code upgrades during the PnP process.

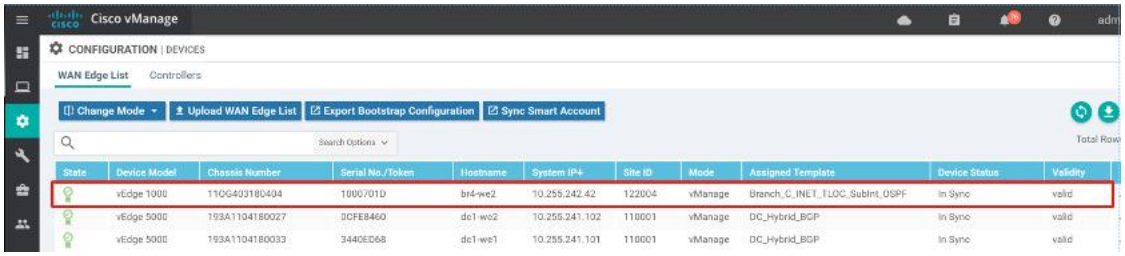


Br4-we2 is installed into the network. It is a vEdge 1000 and its ZTP port, ge0/0, is plugged into the Internet transport. It is assumed that br4-we2 is at factory defaults, and is currently running 17.2.7 software.

4. 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.



5. The full configuration is pushed and the vEdge router becomes in sync with vManage.



6. Bring the additional vEdge devices up, either through ZTP or the manual bootstrap process. See Deploying the data center WAN Edge routers section to see an example of the manual bootstrap process.

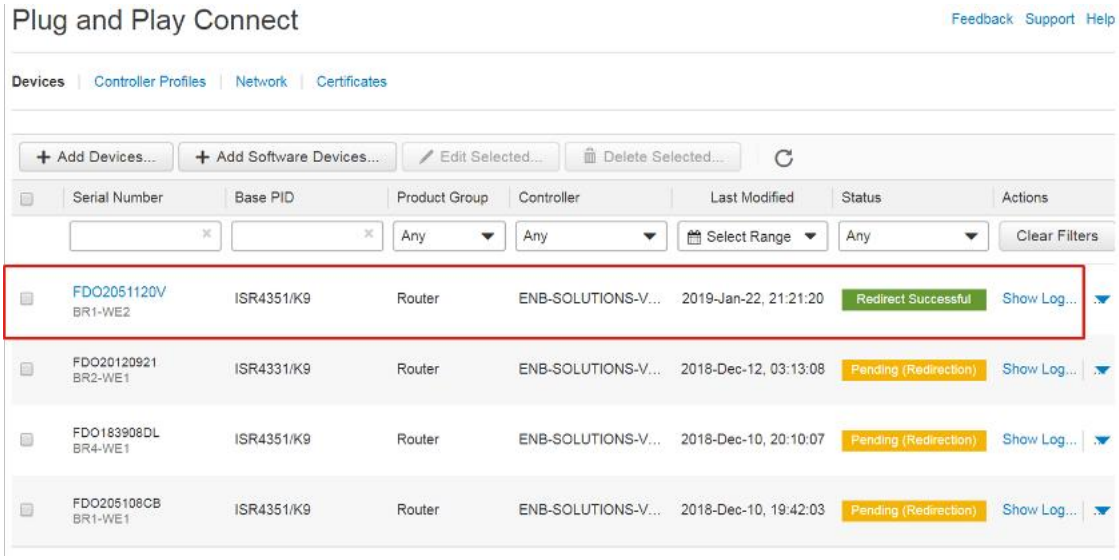
Procedure 7: Bring remote IOS XE SD-WAN routers online via PnP

In this procedure, the IOS XE SD-WAN router in branch 1, br1-we2, is brought online using PnP. Software upgrades are not supported by PnP in this tested vManage version. During the PnP process, DHCP is used on the physical interface to retrieve an IP address. Once the IOS XE SD-WAN router gets an IP address, it will attempt to resolve devicehelper.cisco.com and contact the PnP server in order to find its vBond IP address and start the authentication process with the controllers.

1. Ensure the SD-WAN device information is entered into the PnP portal. See Appendix C for additional information.

2. Br1-we2 is installed into the network. The GigabitEthernet0/0/0 interface on the Cisco ISR4351 router connects to the Internet Service Provider. It is assumed that the router is already converted to the SD-WAN image (See the process in Appendix B).

Power on the IOS XE SD-WAN router. After getting an IP address, the router reaches out to the PnP server, the PnP portal will then redirect the WAN Edge router to the vBond. The WAN Edge router then authenticates to the vBond and subsequently, to the rest of the controllers. The PnP portal will indicate a Redirect Successful status when the WAN Edge router is redirected through PnP to the vBond.



3. Bring any additional IOS XE SD-WAN devices up through the PnP process. For the manual bootstrap method, see the next section.

4. Upgrade the routers using vManage if required.

Procedure 8: Bring remote IOS XE SD-WAN routers online via manual bootstrap method

In this procedure, the IOS XE SD-WAN router in branch 2, br2-we2, is brought online using the manual bootstrap method. In this method, a minimal configuration is used to get reachability to the vBond controller and start the authentication process with the rest of the controllers.

1. Ensure the SD-WAN device information is entered into the PnP portal. See Appendix C for additional information.

2. Br2-we2 is installed into the network and powered on. The GigabitEthernet0/0/0 interface on the Cisco ISR4351 router connects to the Internet Service Provider. It is assumed that the router is already converted to the SD-WAN image (See the process in Appendix B).

3. Connect a console to the router and enter the following at the router console:

```
config-transaction
```

or

```
config-t
```

4. Wait several seconds until you see admin connected from 127.0.0.1 using console on Router text. Enter the following to establish basic connectivity to the vbond:

```
ip domain lookup
ip name-server 64.100.100.125
ip route 0.0.0.0 0.0.0.0 64.100.102.1
interface GigabitEthernet 0/0/0
ip address 64.100.102.2 255.255.255.240
no shutdown
commit
end
```

5. Test out connectivity to the vbond controller

```
Router#ping vbond-21615.cisco.net
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.100.100.51, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

6. Enter the following information so that the router can establish controller connections

```
config-t
system
host-name br2-we1
system-ip 10.255.241.21
site-id 111002
organization-name "ENB-Solutions - 21615"
vbond vbond-21615.cisco.net
```

```
interface Tunnel 0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
color biz-internet
encapsulation ipsec
commit
```

7. Verify connectivity with the controllers

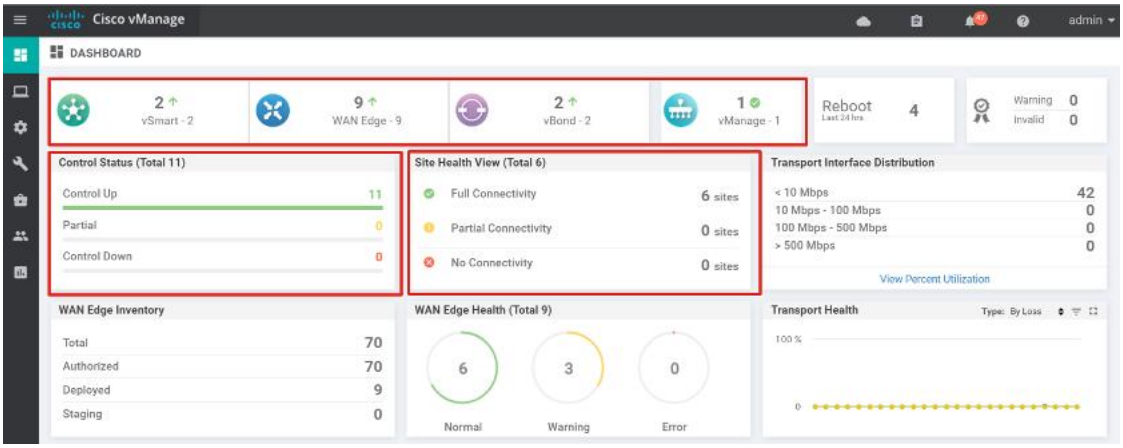
```
Router#show sdwan control summary
control summary 0
 vbond_counts   0
 vmanage_counts 1
 vsmart_counts  2
```

8. Bring any additional IOS XE SD-WAN remote devices up.

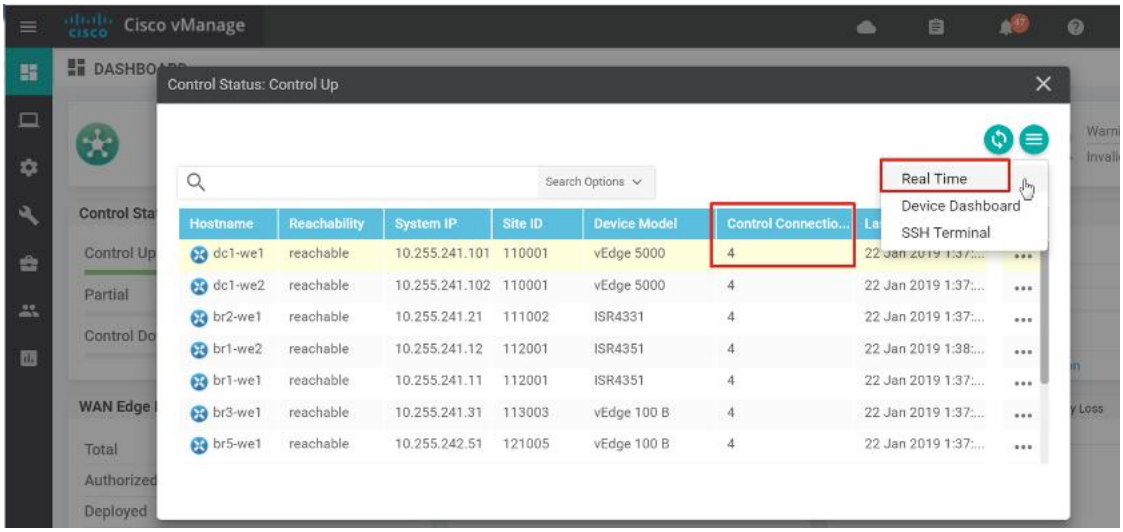
9. Upgrade the routers using vManage if required.

Procedure 9: Verify the network status

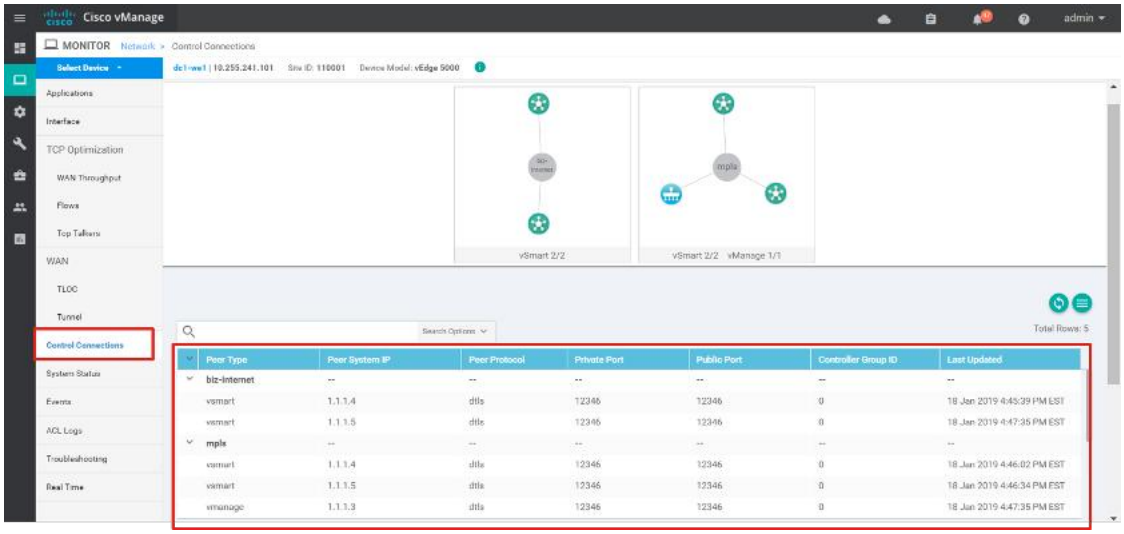
1. Verify the status of the network. vManage should show that all devices are reachable at the top of the dashboard. The Control Status should show that all of the control connections are up for the nine WAN Edge routers and two vSmart controllers, and the Site Health View should show Full Connectivity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



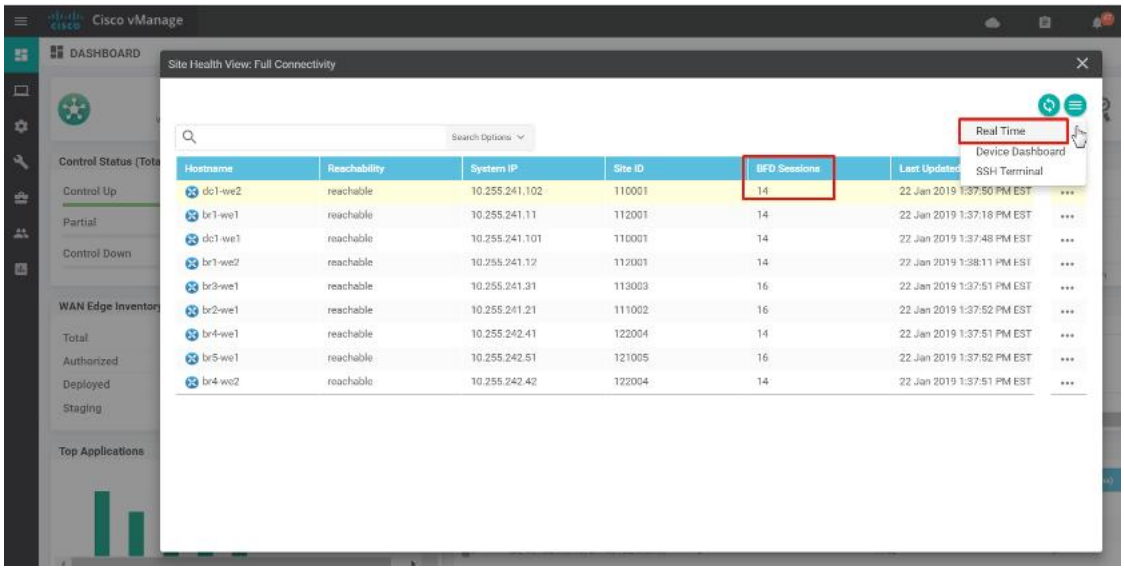
2. If you select Control Up, Partial, or Control Down in the Control Status box, you will get a pop-up window summarizing the number of control connections each WAN Edge device has. This counts only the vSmart connections. To get more information, select **...** to the right of the desired device and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



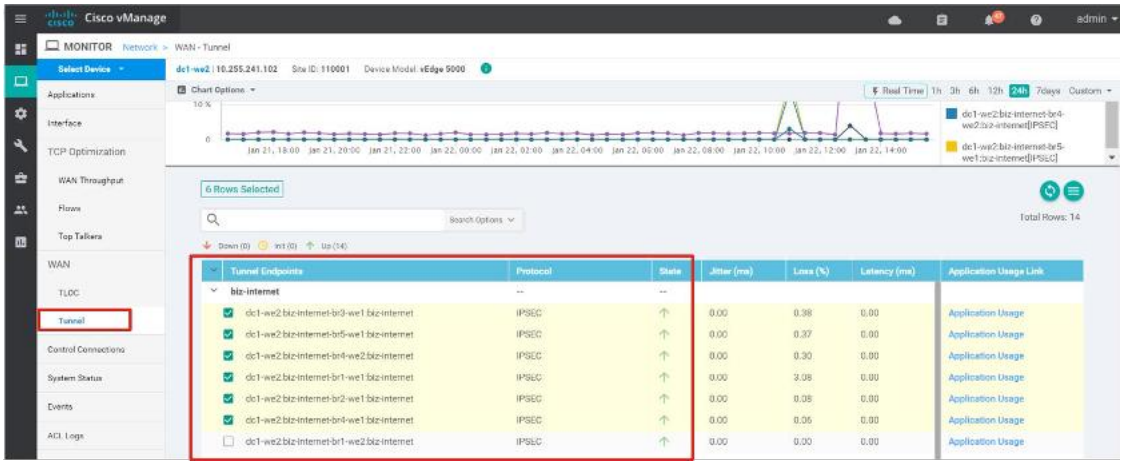
3. To view the state of all of the control connections, select Control Connections in the left column.



4. From the dashboard, 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 WAN Edge has. To get more information, to the right of the desired device, go to **...** and select Real Time or Device Dashboard.



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.



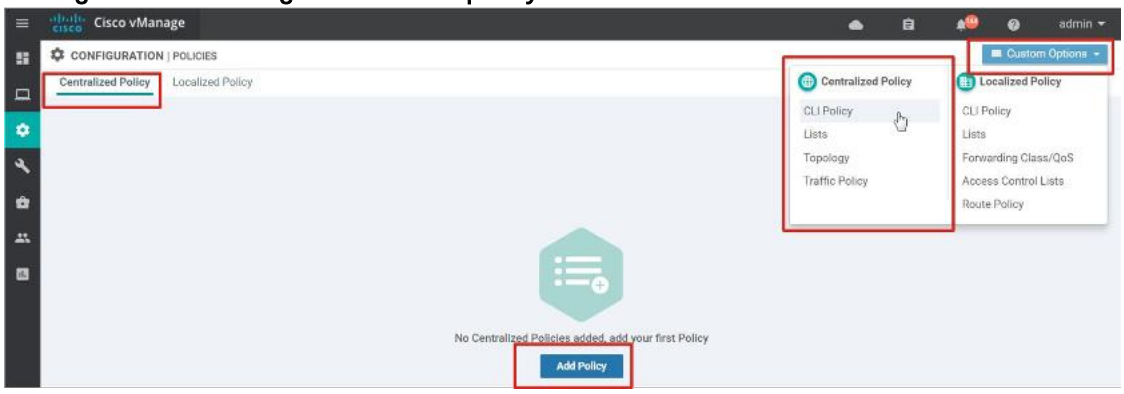
Configuring centralized policy

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:

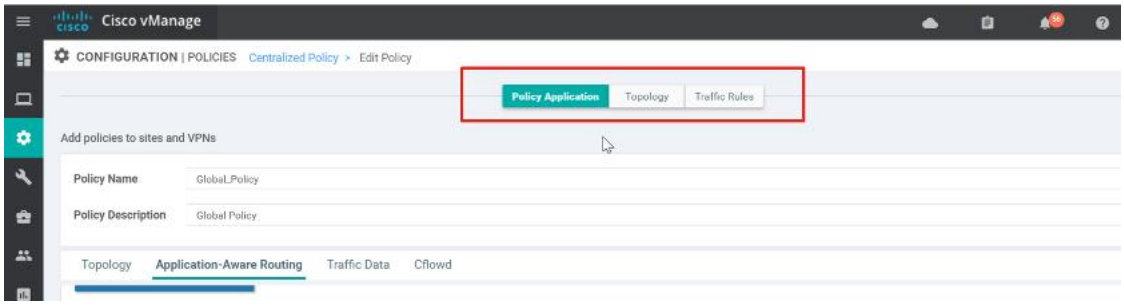
1. Create groups of interest. In this section, you will create lists that you will use in your policy, such as application, color, data prefixes, policer, prefix, site, SLA class, TLOC, and VPN lists. Minimally, you need to create a list of site IDs in order to apply the individual policy definitions. 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.

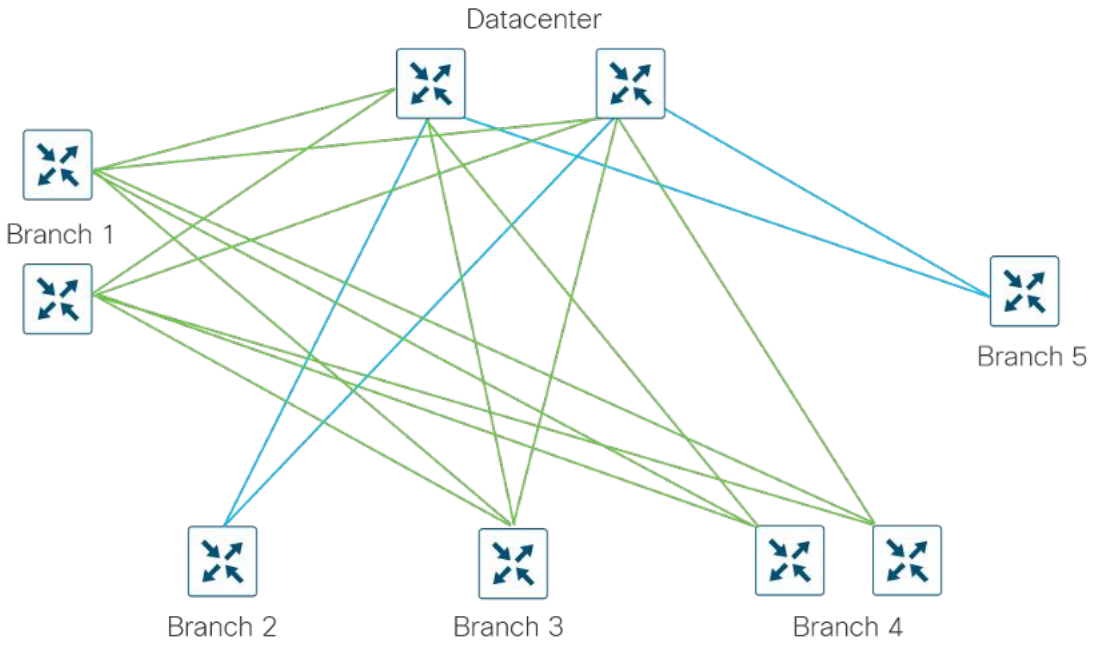
4. Apply policies to sites and VPNs. In the last step, you name and describe the new centralized policy. You then apply the various policy definitions to a site list. You may need to apply a VPN list as well.

If you want 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.



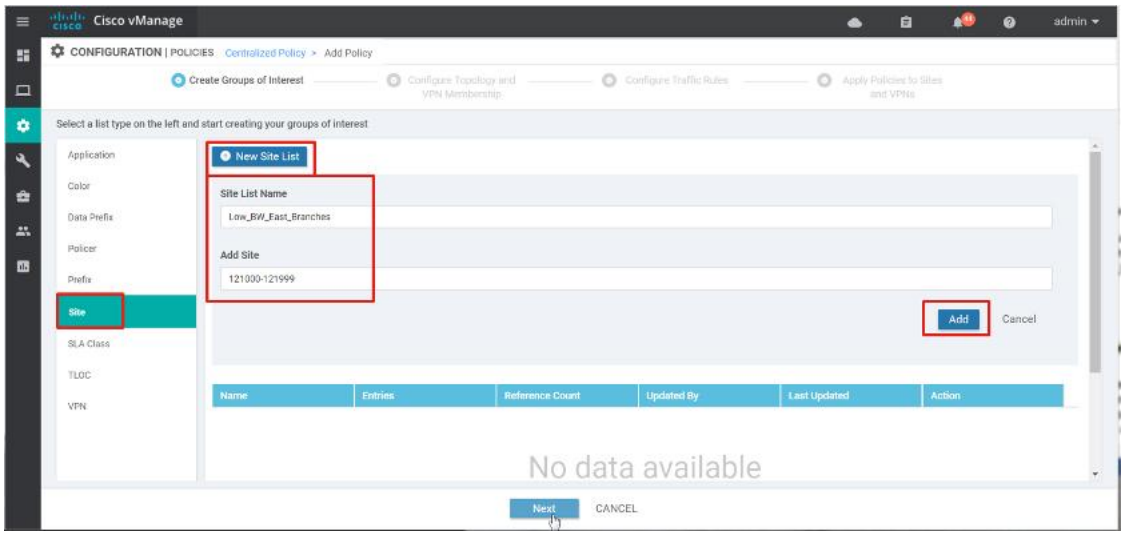
For the example network, create a centralized policy to create a hub-and-spoke topology for the low-bandwidth sites (branches 2 and 5). In the following figure, branches 2 and 5 only form IPSec tunnels with the data center vEdge routers. This is accomplished by filtering routes and TLOC routes.

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



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

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.



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

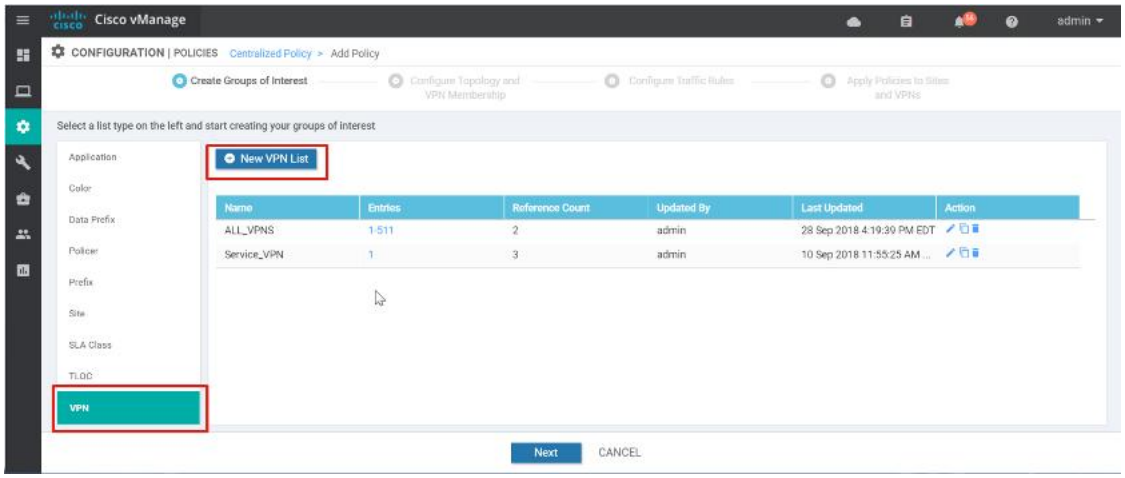
e. ALL_SITES: 0-4294967295

f. All_US_Sites: 110000-129999

g. Low_BW_US_Sites: 111000-111999,121000-121999

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.

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



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

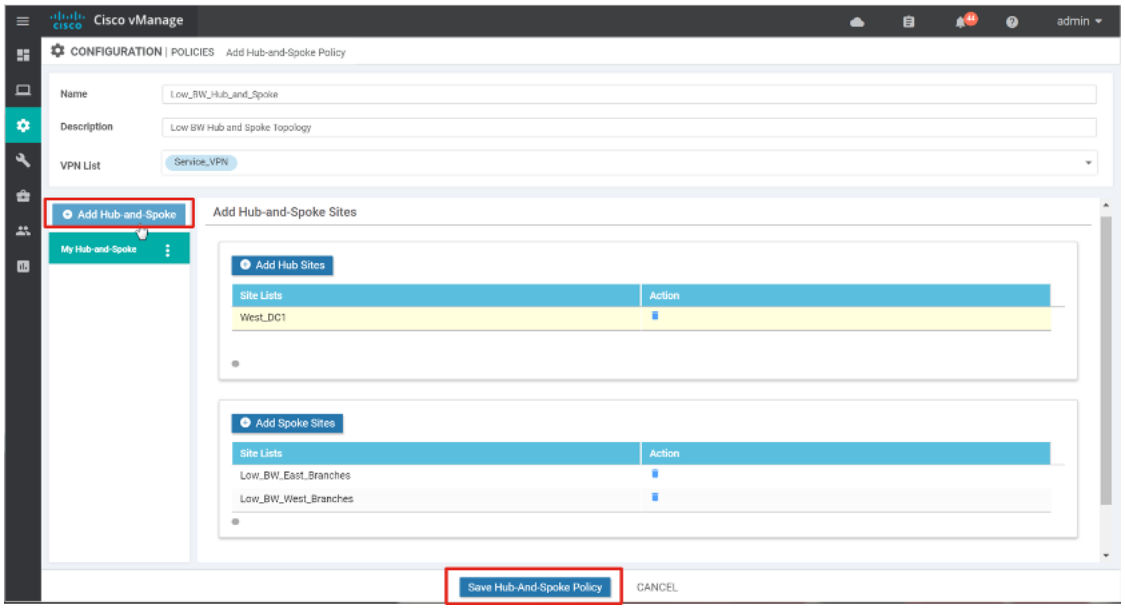
7. Ensure you are on the Topology tab and select Add Topology. Select Hub-and-Spoke from the drop-down menu.

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

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

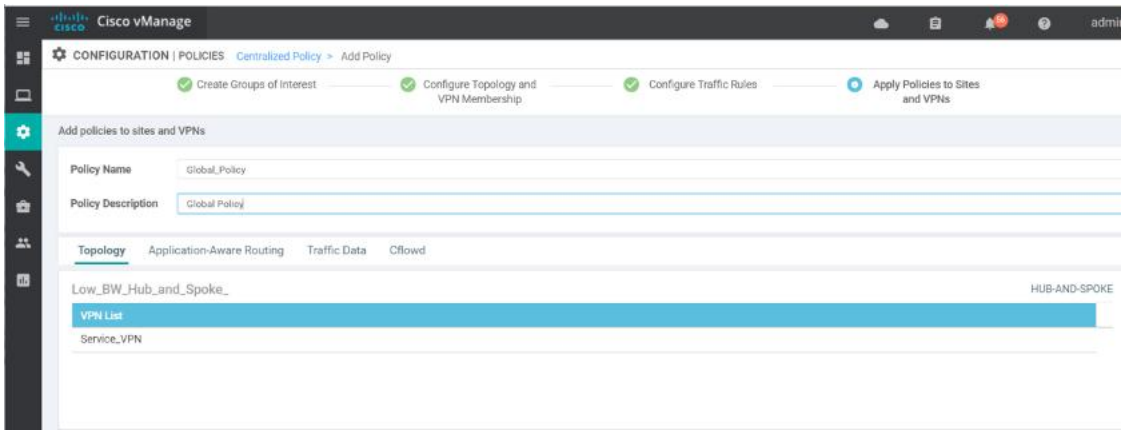
10. Select Add Spoke Sites. Select Low_BW_East_Branches and select Add. Repeat the step for Low_BW_West_Branches.

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.



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

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.



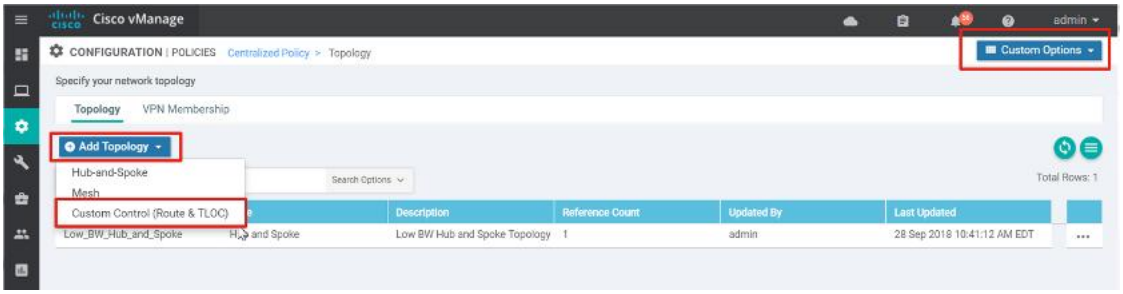
Tech tip: When you use the Predefined Hub-and-Spoke topology policy, only TLOCs and routes from the data center site are distributed to the low-bandwidth sites specified. Ensure a summary or default route is distributed from the data center if you want the low-bandwidth sites to reach other remote sites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

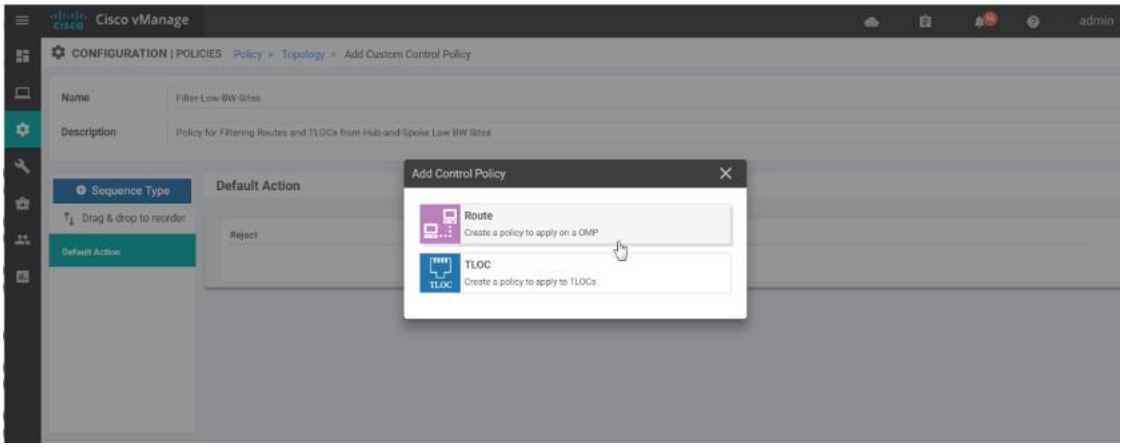
14. From the Configuration>Policies page, select Custom Options in the top right corner of the page. Select Topology from the drop-down menu, since you are adding an additional control policy definition.

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



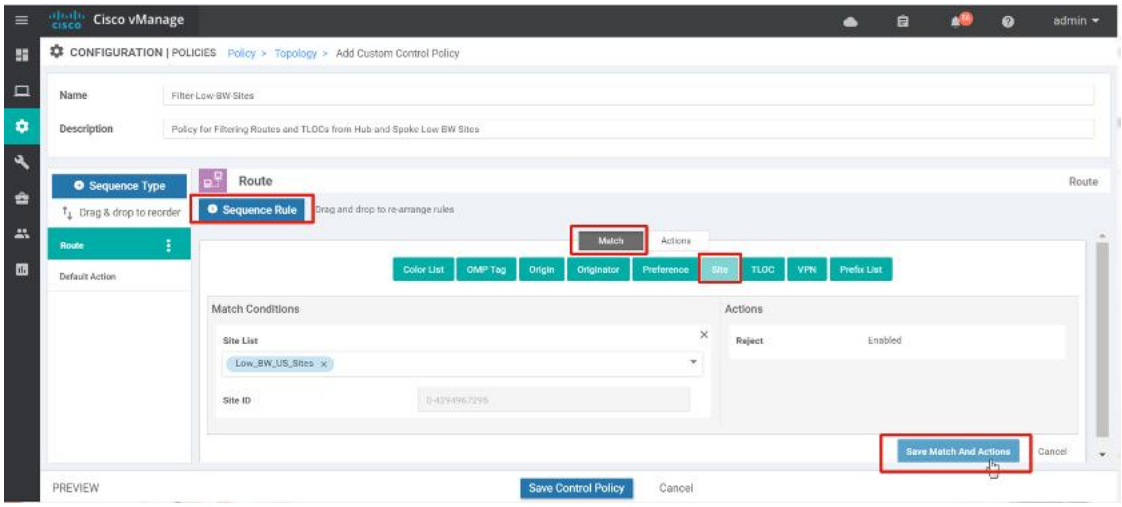
16. Type Name (Filter-Low-BW-Sites) and Description (Policy for Filtering Routes and TLOCs from Hub-and-Spoke Low BW Sites).

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



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.

19. Select Save Match and Actions.

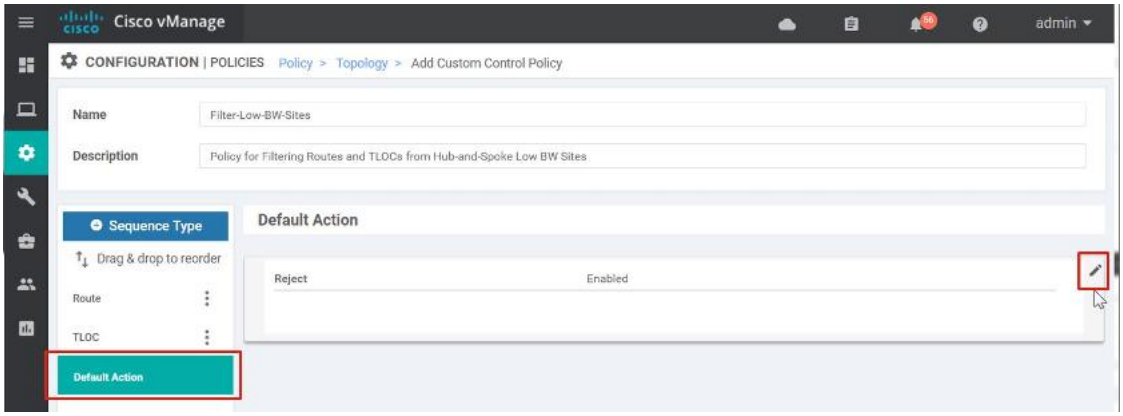


20. Select Sequence Type on the left of the page and on the Add Control Policy pop-up window, select TLOC.

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.

22. Select Save Match and Actions.

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.

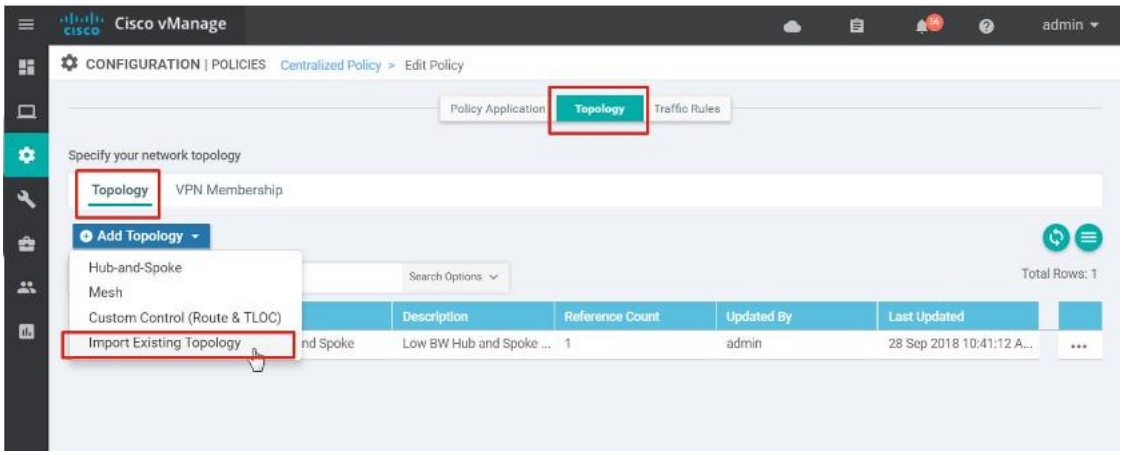


24. Select Save Control Policy to save the policy definition.

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.

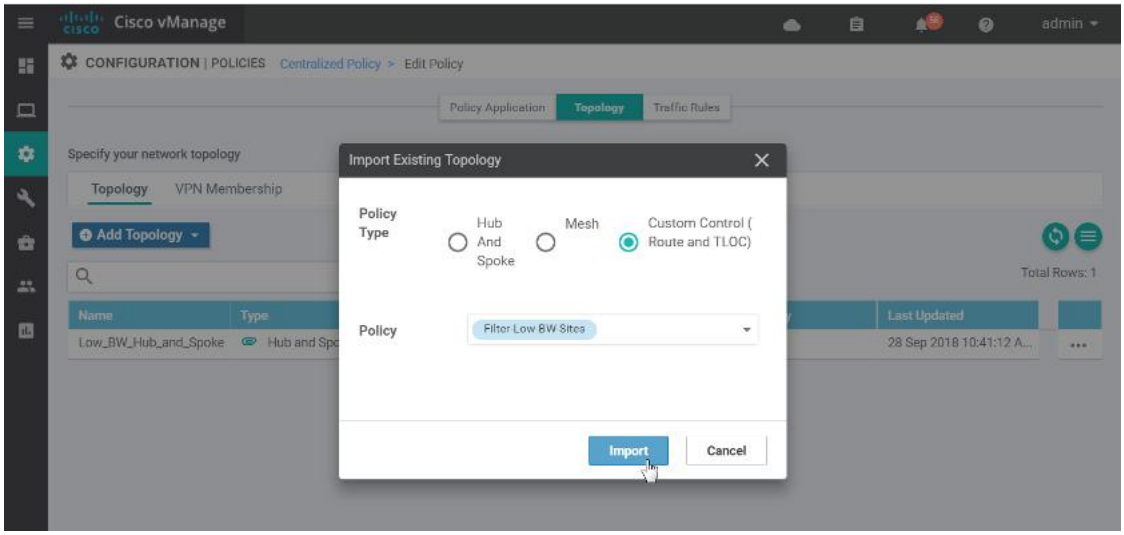
26. Select **...** to the far right of the policy named Global_Policy and select Edit from the drop-down menu.

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



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.

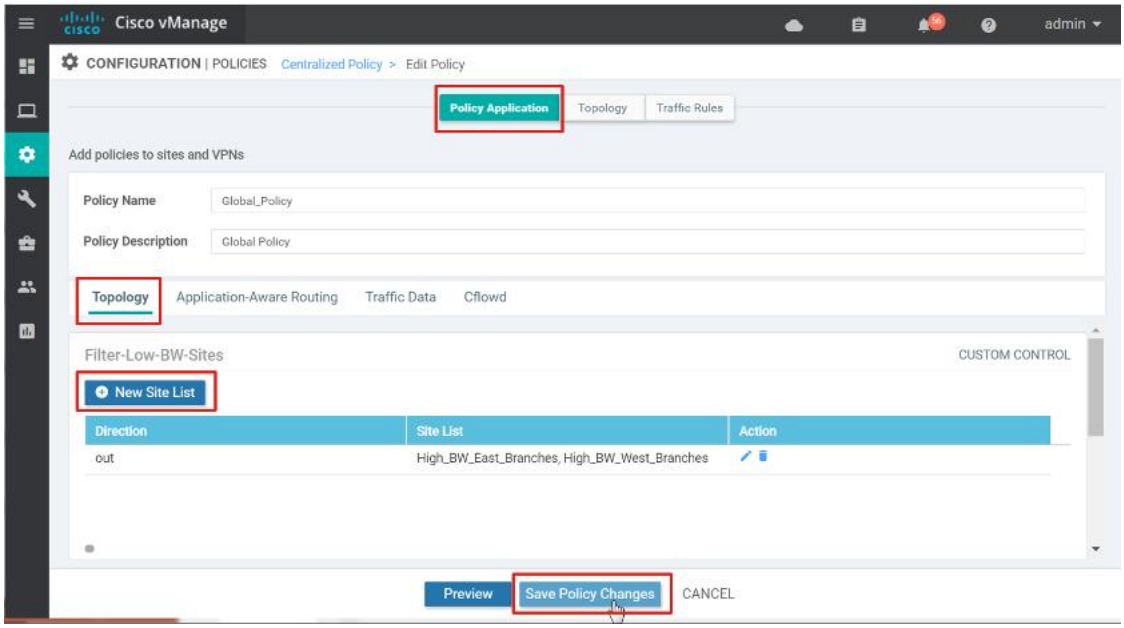
29. Select Import.



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.

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.

32. Select Save Policy Changes.



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.

34. 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.

Configuring an application-aware routing policy

Application-aware routing policies are configured as part of a centralized policy. It affects traffic on a WAN Edge 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 that 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

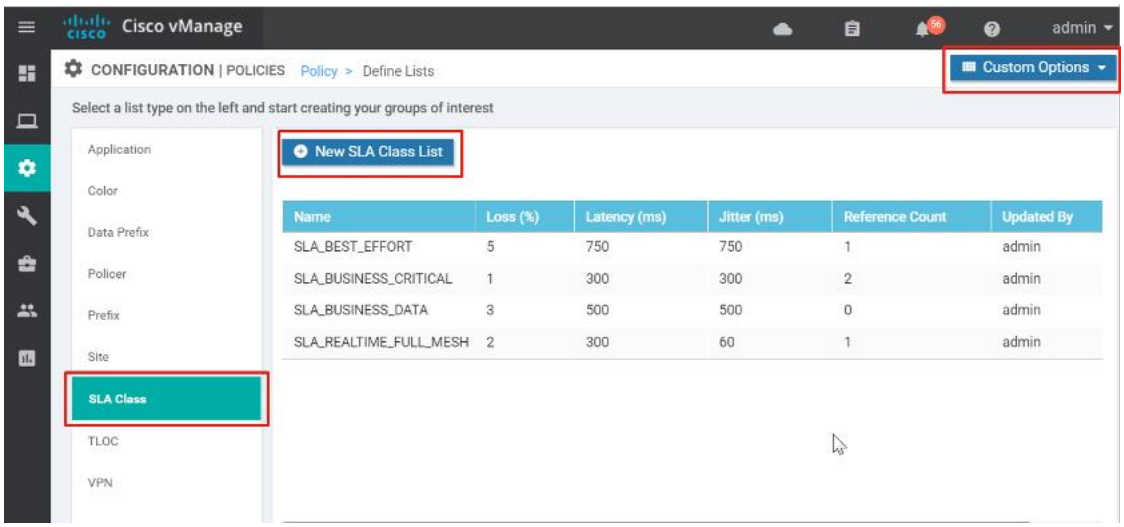
Once a centralized policy is created, it is not possible to build lists by editing the policy - you can only create policy definitions and apply them through the centralized policy configuration. You need to select Custom Options on the main policy page in order to modify or create lists.

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

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:

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



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

4. Type in the Application List Name, and select several applications as part of the list. The application drop-down search 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:

Application-aware routing policy applications list (example)

Application list name	Application
APPS_SCAVENGER	Apple Update, Twitter, Instagram, Youtube HD, Google Play Music, Facebook Mail
APPS_NETWORK_CONTROL	Network Time Protocol (NTP), Remote Authentication Dial-In User Service (Radius), Secure Shell (SSH), Terminal Access Controller Access-Control System Plus (TACACS Plus), Telnet

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

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).

7. Select Add.

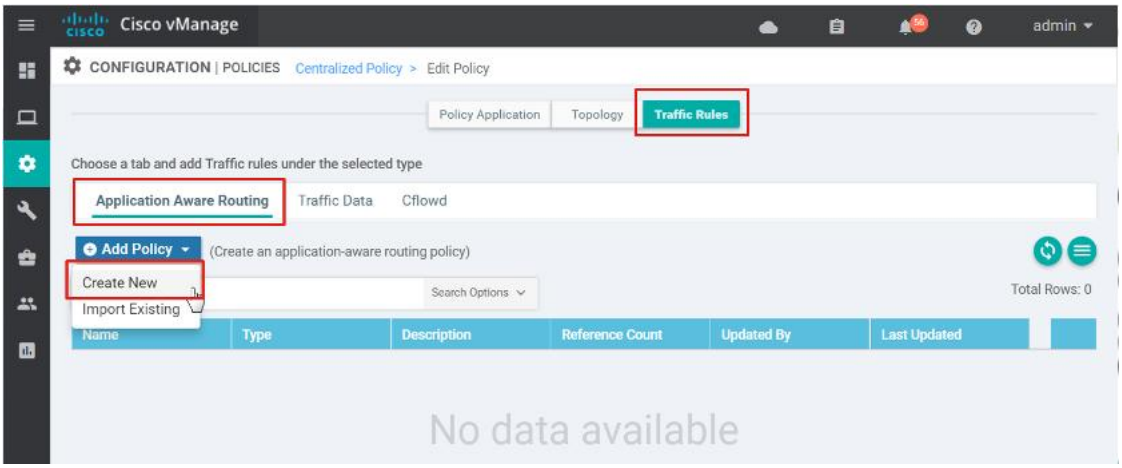
Procedure 2: Create the application-aware routing policy

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

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.

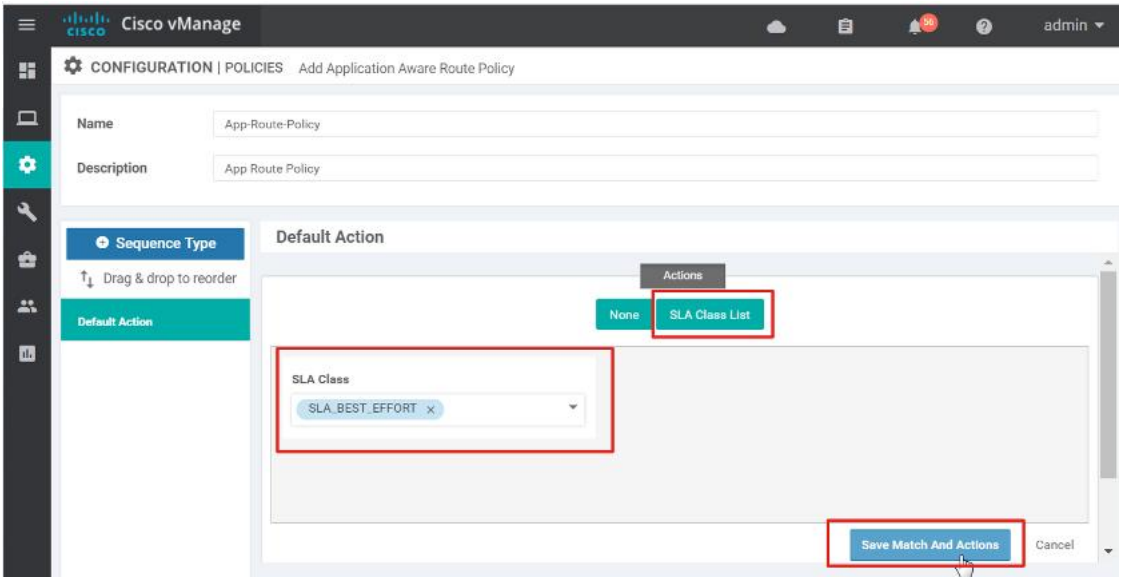
3. The application-aware policy is part of data policy, listed under Traffic Rules. Select the Traffic Rules box at the top of the page to create a new application-aware policy inside the centralized policy. Application Aware Routing is the default tab on this page.

4. Select Add Policy and select Create New.



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

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.



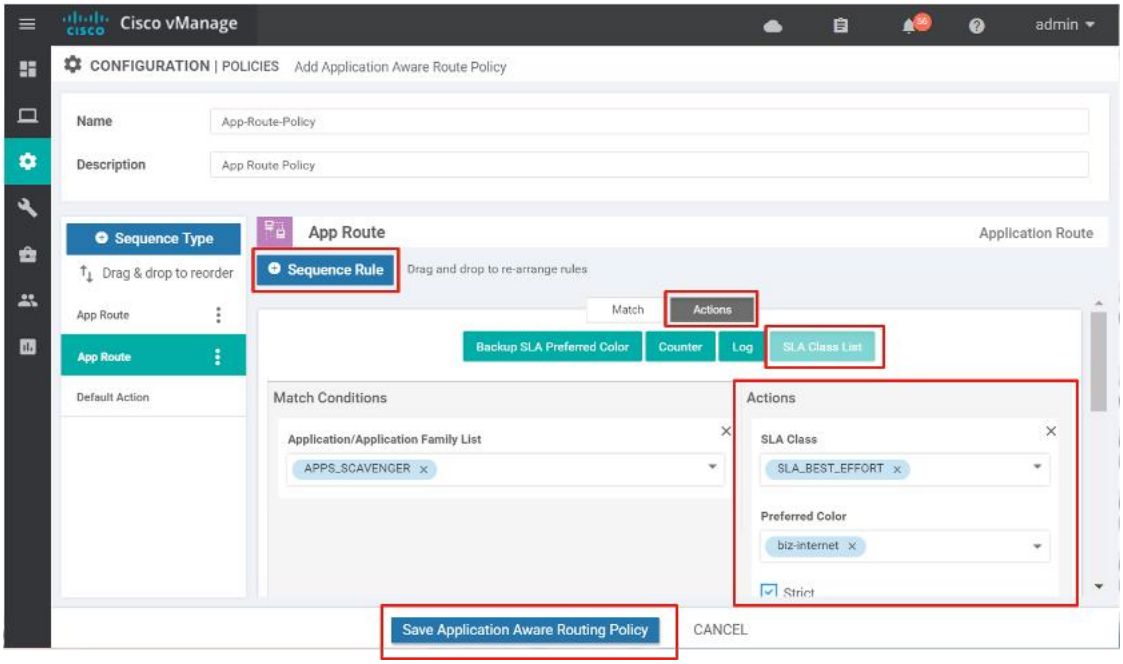
7. Select Sequence Type on the left side, then select Sequence Rule.

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:

Application-aware routing policy App Route Policy (example)

Application list name	Application
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

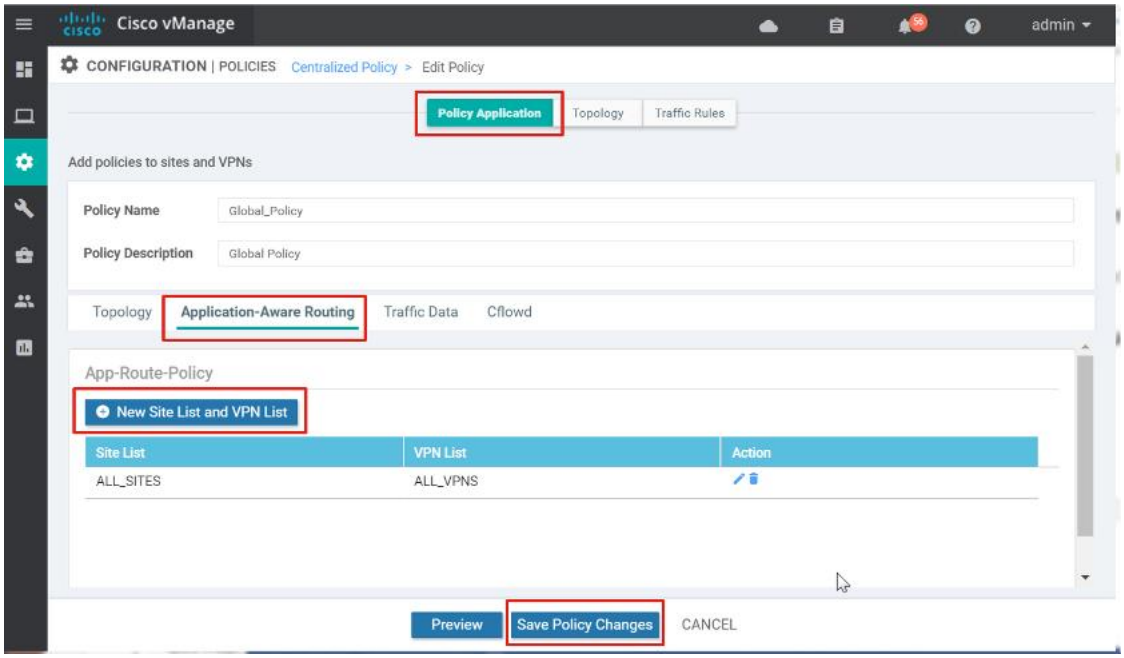


Procedure 3: Apply the policy definition

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

2. Select the Application-Aware Routing tab. Select New Site List and VPN List under the policy definition just created.

3. Select the Site List (ALL_SITES), and select the VPN List (ALL_VPNS), and select Add.



4. Select Save Policy Changes.

5. 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.

Configuring symmetric traffic for DPI

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 WAN Edge router to be able to classify most application traffic, it is important that the WAN Edge router sees network traffic in both directions. To ensure symmetry at dual WAN Edge 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:

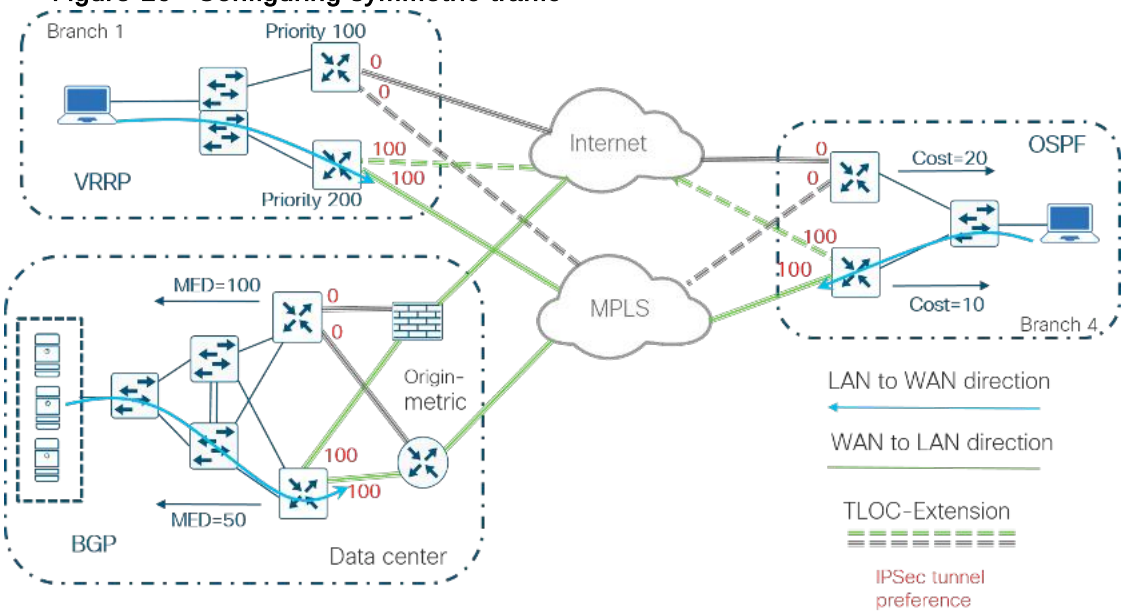
- With VRRP, by setting VRRP priority
- With OSPF, by creating a route policy that modifies the metric of routes distributed from OMP to OSPF
- With BGP, by creating a route policy that modifies the MED (metric) of routes distributed from OMP to BGP.

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

- With IPSec tunnel preference

WAN Edge 1 of each dual-WAN Edge router site will be picked as the primary WAN Edge 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 WAN Edge routers at branch 1 to prefer BR1-WE1 when the VRRP priority was set to 200 on BR1-WE1 and the VRRP priority was set to 100 on BR1-WE2.

OSPF

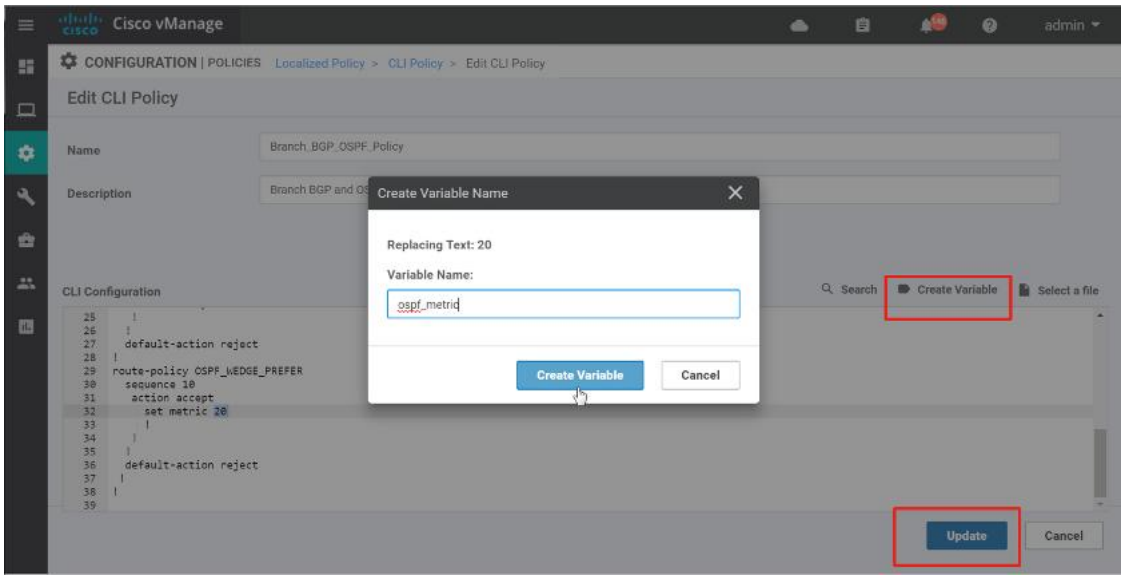
For OSPF, create a route policy that modifies the metric of routes redistributed from OMP to OSPF.

1. Go to Configuration>Policies and select the Localized Policy tab.
2. Edit the Branch_BGP_OSPF_Policy. Select ... to the far right of the desired policy and select Edit.
3. Add the following route policy to the existing one:

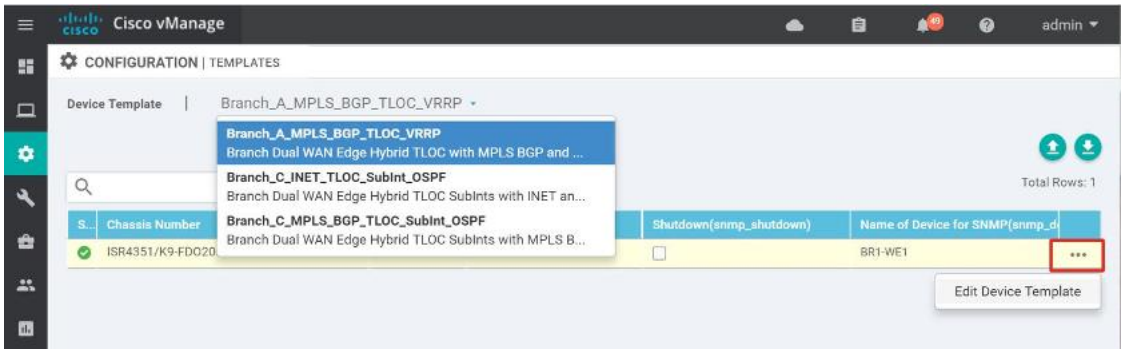
```
route-policy OSPF_WEDGE_PREFER
 sequence 10
  action accept
    set metric 20
    !
  !
```

```
  !
  default-action reject
 !
!
```

4. Highlight 20 in the set metric line of the policy and select Create Variable. In the pop-up window, type ospf_metric into the text box and select Create Variable. Select Update to save the policy configuration.



5. Before the updated policy is pushed out to the WAN Edge routers, the variable value ospf_metric first needs to be defined for all WAN Edge 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 WAN Edge routers that are attached to the device template appear on the main screen. Next to each WAN Edge router, select **...** to the right and select Edit Device Template.



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-WE1 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.

OSPF metric values

Device Template	Device	ospf_metric
Branch_C_INET_TLOCEXT_SubInt_OSPF	BR4-WE2	20
Branch_A_MPLS_BGP_TLOCEXT_VRRP	BR1-WE1	0
Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF	BR4-WE1	10

7. Select Next and then Configure Devices.

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

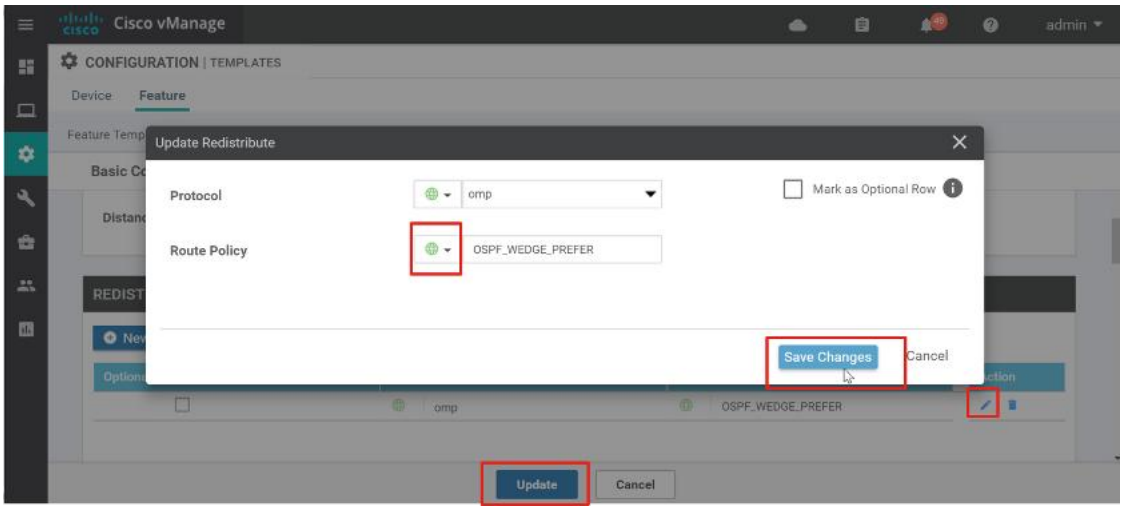
9. Once the policy has been updated, the route policy can be referenced in the feature template. Go to Configuration>Templates and select the Feature tab.

10. Edit the BR_LAN_OSPF feature template

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

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

13. Select Update to save the feature template configuration.

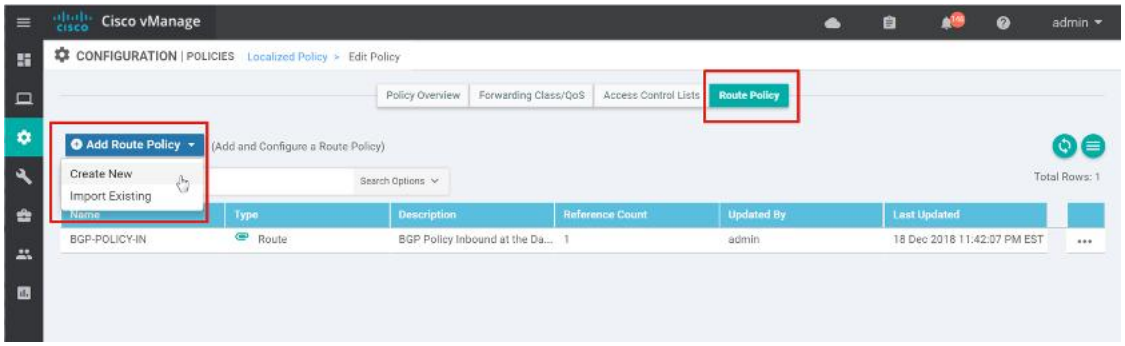


14. Select Next, then Configure Devices. Confirm configuration changes on two devices, and then select OK. The configurations are pushed out and the screen will indicate success.

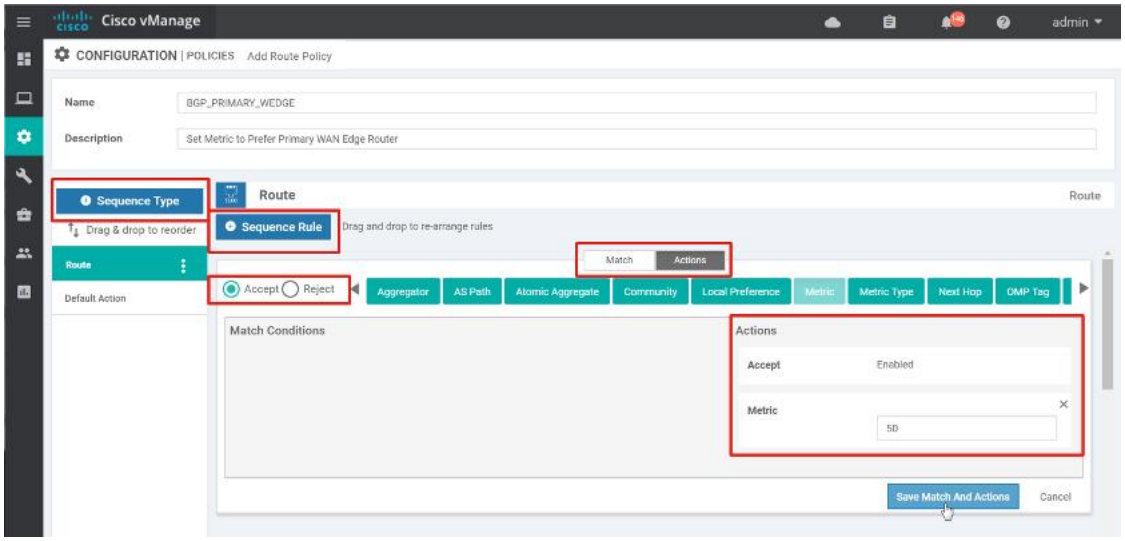
BGP

For BGP, create a route policy that sets MED (metric) on routes redistributed from OMP to BGP in the data center. The DC local policy was created using the policy wizard, which doesn't allow variables, so two different route policies can be created inside the localized policy called DC_Policy. One route policy would apply to the primary WAN Edge and the other route policy would apply to the secondary WAN Edge.

1. Go to Configuration>Policies and select the Localized Policy tab.
2. Edit the DC_Policy. Select ... to the far right of the desired policy and select Edit.
3. Select the Route Policy box at the top of the page.
4. Click the Add Route Policy button and select Create New from the list.



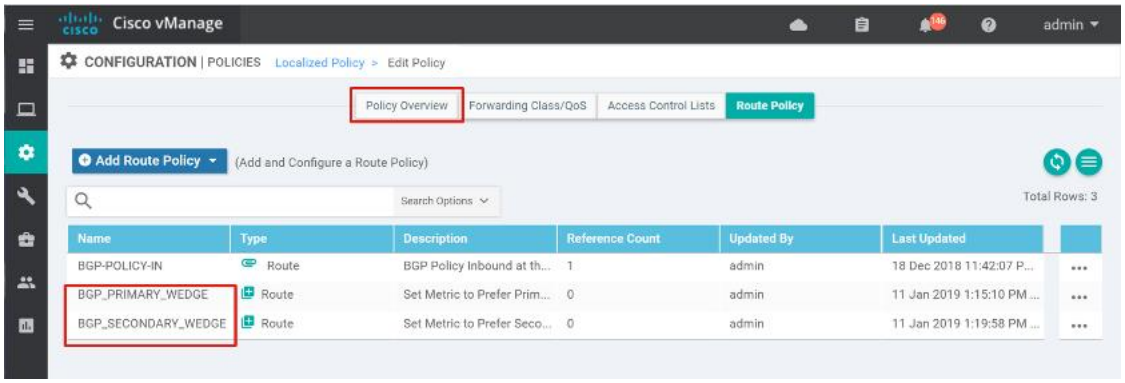
5. Fill in the Name (BGP_PRIMARY_WEDGE) and Description (Set Metric to Prefer Primary WAN Edge Router) of the new route policy.
6. Select Sequence Type on the left side, then select Sequence Rule.
7. Since all routes will be matched, do not select any Match conditions.
8. Select the Actions box and then select the Accept radio button.
9. Select the Metric box and type 50 in the text box.
10. Select Save Match and Actions.



11. Click Save Route Policy.

12. Repeat the previous steps to create a second route policy with the Name (BGP_SECONDARY_WEDGE) and Description (Set Metric for Secondary WAN Edge Router). Use 100 as the metric.

13. Once the two route policies are created, select the Policy Overview box at the top of the page.



14. Select Save Policy Changes to save the localized policy. The configuration changes will be pushed out to the data center SD-WAN routers.

15. Select Next and then Configure Devices

16. Confirm configuration on two devices and select OK. The configurations will be pushed out and the screen will indicate success.

17. 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.

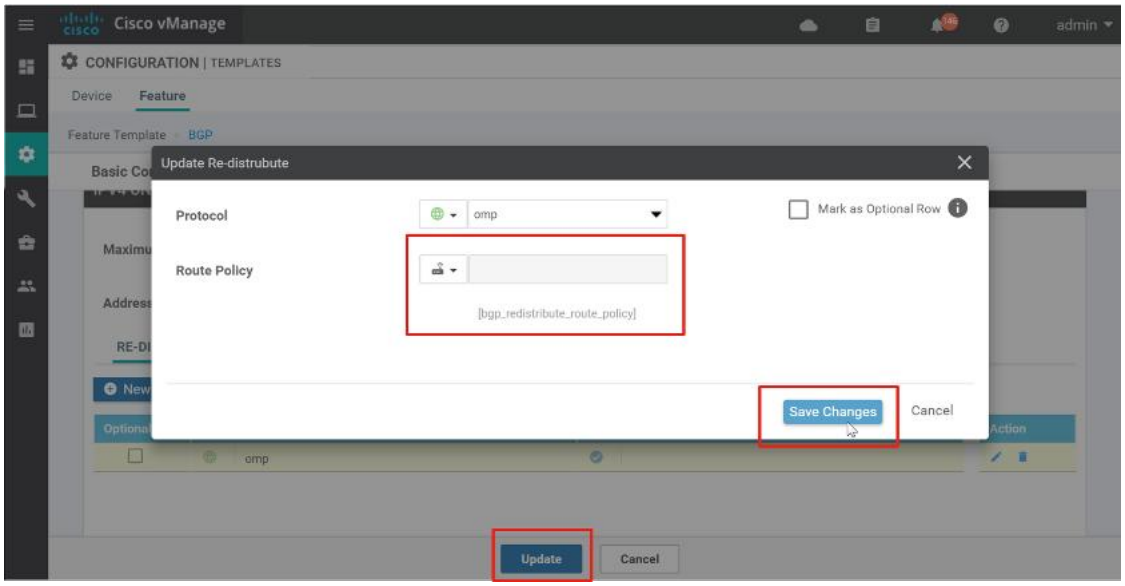
18. Edit the DC_LAN_BGP feature template.

19. Under the Redistribute under the IPv4 Unicast Address Family section, select the Edit symbol next to the OMP protocol.

20. Next to Route Policy, select Device Specific and use the default variable name, bgp_redistribute_route_policy.

21. Select Save Changes.

22. Select Update to save the feature template configuration.



Before configurations can be pushed out, the route policy variable just added needs to be defined.

23. Select **...** to the right of dc1-we1 and select Edit Device Template from the drop-down list.

24. Next to Route Policy(bgp_redistribute_route_policy) type BGP_PRIMARY_WEDGE.

25. Select Update.

26. Repeat the steps for dc1-we2, using BGP_SECONDARY_WEDGE as the route policy.

27. Click 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

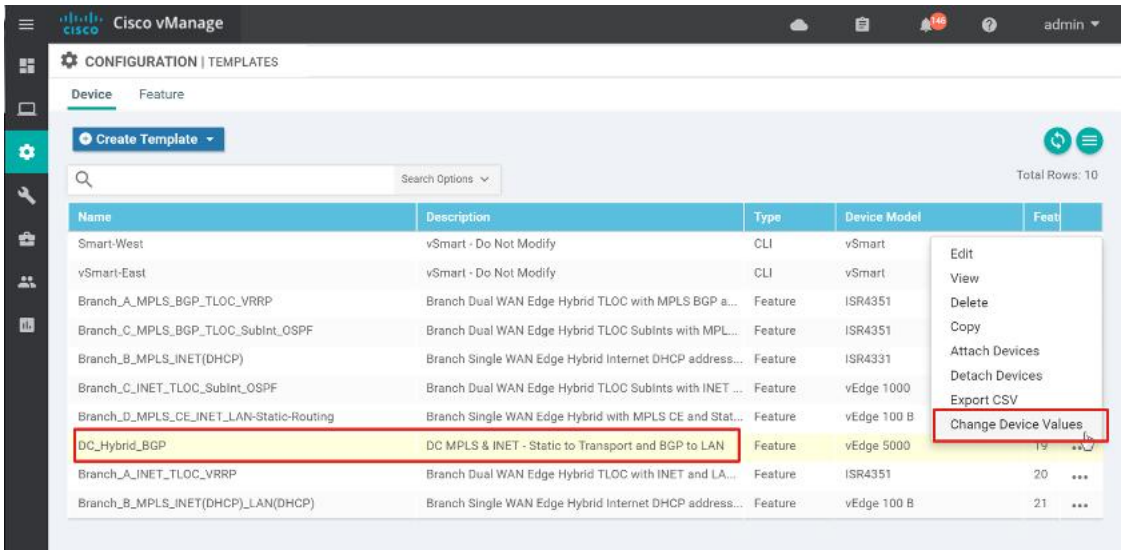
IPSec tunnel preference

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 WAN Edge 1 over WAN Edge 2 at the dual-WAN Edge sites by changing the IPSec tunnel preference of the primary WAN Edge to 100. Only three device templates need to be modified:

- DC_Hybrid_BGP
- BR1-WE1: Branch_A_MPLS_BGP_TLOCEXT_VRRP
- BR4-WE1: Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

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

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



3. To the right of dc1-we1, select **...** and select Edit Device Template. Next to vpn0_mpls_tunnel_ipsec_pref and vpn0_inet_tunnel_ipsec_pref, type 100. DC1-WE2 values are already set to 0 so they do not need to be modified. Select Update.

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.

5. Repeat steps 1-5 for the device templates, Branch_A_MPLS_BGP_TLOCEXT_VRRP and Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF. Change the tunnel IPSec preference values of vpn0_mpls_tunnel_ipsec_preference and vpn0_inet_tunnel_ipsec_preference to 100 for BR1-WE1 and BR4-WE1.

Configuring quality of service

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:

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:

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:

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 (localized or centralized policy).

6. Apply the classification access list to an interface (localized or centralized policy). In localized policy, this is accomplished by referencing the access list in the VPN Interface Ethernet template. For centralized policy, this is accomplished by applying the QoS data policy to a site and vpn list.

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

Localized policy can be configured with a CLI policy or through the local policy GUI.

CLI Policy

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

2. To the right of Branch_Policy, select ... and select Edit.

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
!
```

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
!
```

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.

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
!
```

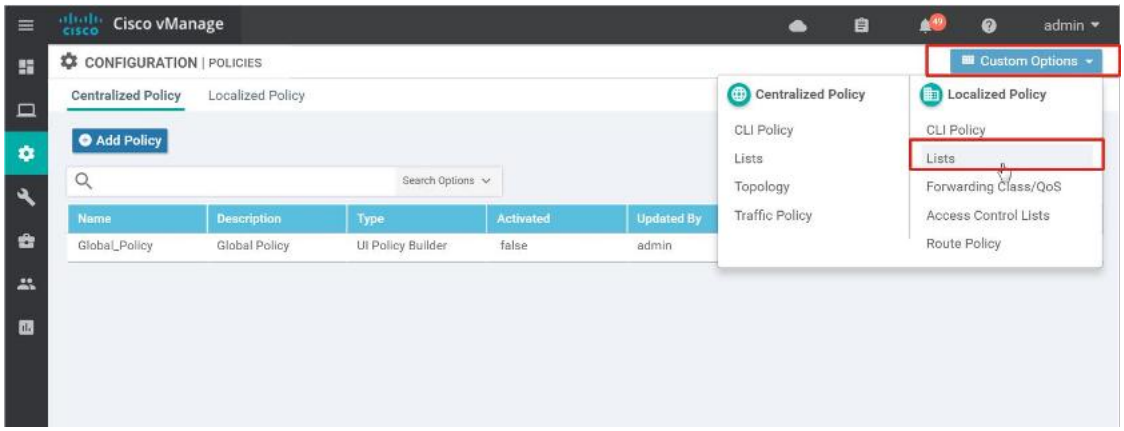
7. Select Update, then Next, and then Configure Devices. Confirm the changes to the configuration by selecting the check box and selecting OK. The modified localized policy will be downloaded to devices already configured with Branch_Policy.

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

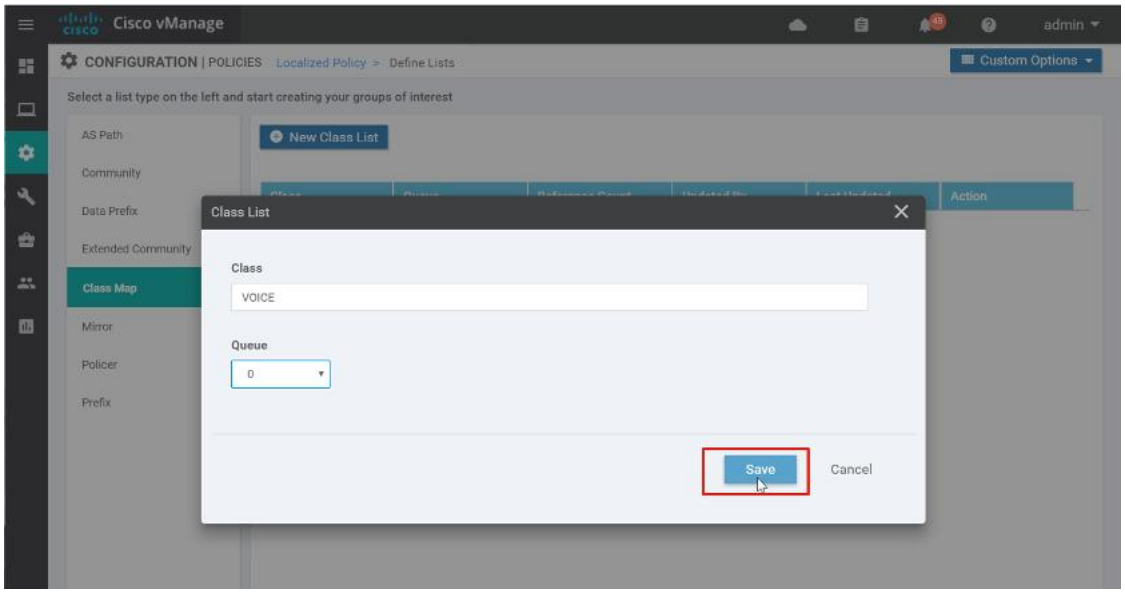
Localized policy GUI

To configure QoS with the localized policy GUI, first create forwarding classes and assign them to queues in the Lists section before adding a QoS map which defines the characteristics of each queue inside the localized policy.

1. Go to Configuration>Policies, click the Custom Options button and select Lists under Localized Policy.



2. Select Class Map on the left-hand side.
3. Click the New Class List button.
4. Under the Class textbox, type VOICE. Under Queue, select 0 from the drop-down box.
5. Click Save.



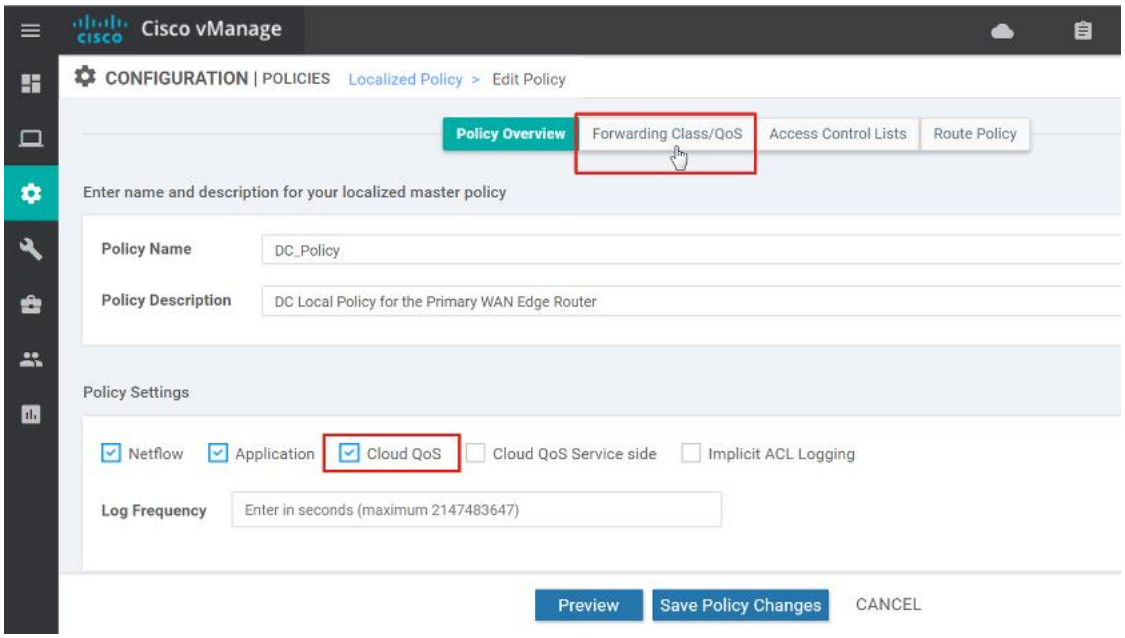
6. Repeat the previous three steps to add the remaining class lists:

Class list and queue mappings

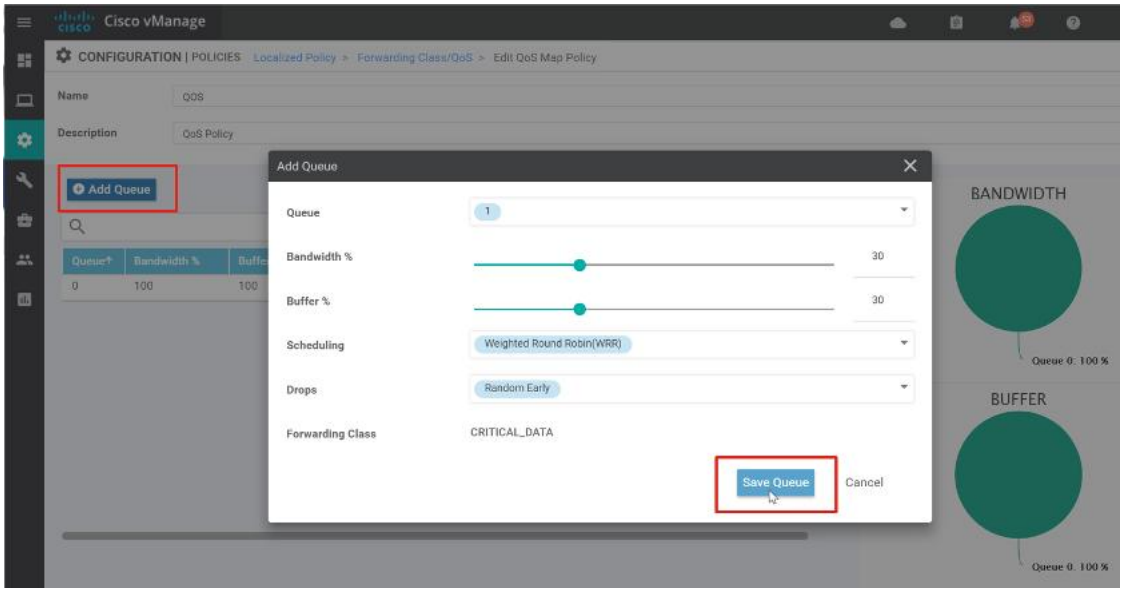
Class	Queue
VOICE	0
CRITICAL_DATA	1
BULK	2
CLASS_DEFAULT	3

INTERACTIVE_VIDEO	4
CONTROL_SIGNALING	5

7. Next, go to Configuration>Policies and select the Localized Policy tab.
8. To the right of DC_Policy, select ... and select Edit.
9. Since the DC routers are vEdge 5000s, select the Cloud QoS checkbox to enable QoS on the transport side.
10. Click the Forwarding Class/QoS box at the top of the page.



11. On the QoS Map tab, click the Add QoS Map box, and select Create New from the drop-down list.
12. Enter the Name (QOS) and and Description (QoS policy).
13. Queue 0 has already been defined by default and cannot be modified. Click the Add Queue button.
14. Next to Queue, select 1. Slide the Bandwidth % and Buffer % slider bar to 30. Next to Drops, select Random Early in the drop-down box.
15. Click the Save Queue button.



16. Repeat the previous three steps to add the remaining queue information:

Bandwidth and buffer values and drop algorithm

Queue	Bandwidth/Buffer	Drops
1	30/30	Random Early (RED)
2	10/10	Random Early (RED)
3	20/20	Random Early (RED)
4	20/20	Random Early (RED)
5	10/10	Tail Drop

QoS queue 0 should now be left at 10% Bandwidth and Buffer.

17. Click the Save Policy button.

18. Select the Policy Rewrite tab to add a rewrite policy (optional).

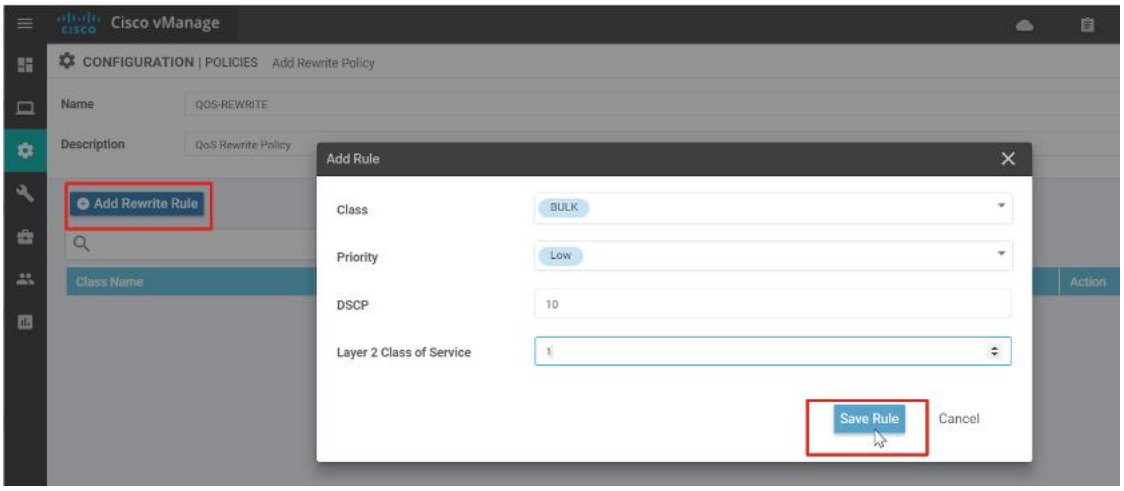
19. Click the Add Rewrite Policy button and select Create New.

20. Type in a Name (QOS-REWRITE) and a Description (QoS Rewrite Policy)

21. Click the Add Rewrite Rule button.

22. Next to Class, choose BULK. Next to Priority, choose Low. Next to DSCP, type in 10, and next to Layer 2 Class of Service, type in 1.

23. Click the Save Rule button.



24. Repeat the previous three steps to add the remaining rewrite information:

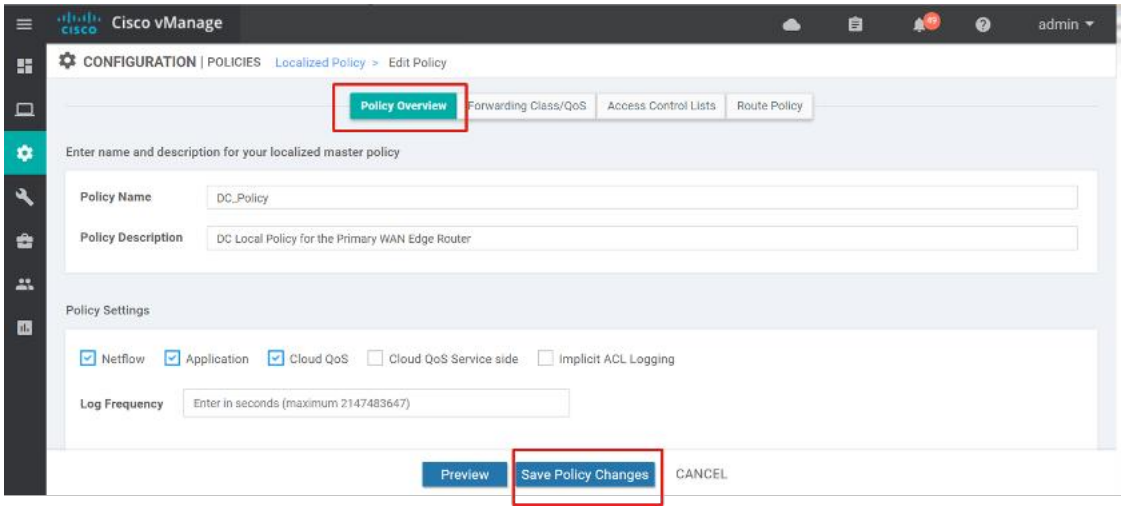
QoS rewrite information

Class	Priority	DSCP	Layer 2 Class of Service
BULK	Low	10	1
BULK	High	10	1
DEFAULT	Low	0	0
DEFAULT	High	0	0
CONTROL_SIGNALING	Low	18	2
CONTROL_SIGNALING	High	18	2
CRITICAL_DATA	Low	18	2
CRITICAL_DATA	High	18	2
INTERACTIVE_VIDEO	Low	34	4
INTERACTIVE_VIDEO	High	34	4

25. Once complete, click the Save Policy button.

26. Select the Policy Overview box at the top of the page.

27. Click Save Policy Changes to save the changes to the localized master policy.



The configuration changes are pushed to the devices associated with the modified localized policy.

28. Click Next, then Configure Devices, then select the checkbox to confirm configuration changes on two devices, then click OK. vManage should indicate success.

Procedure 2: Define QoS classification access list

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

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

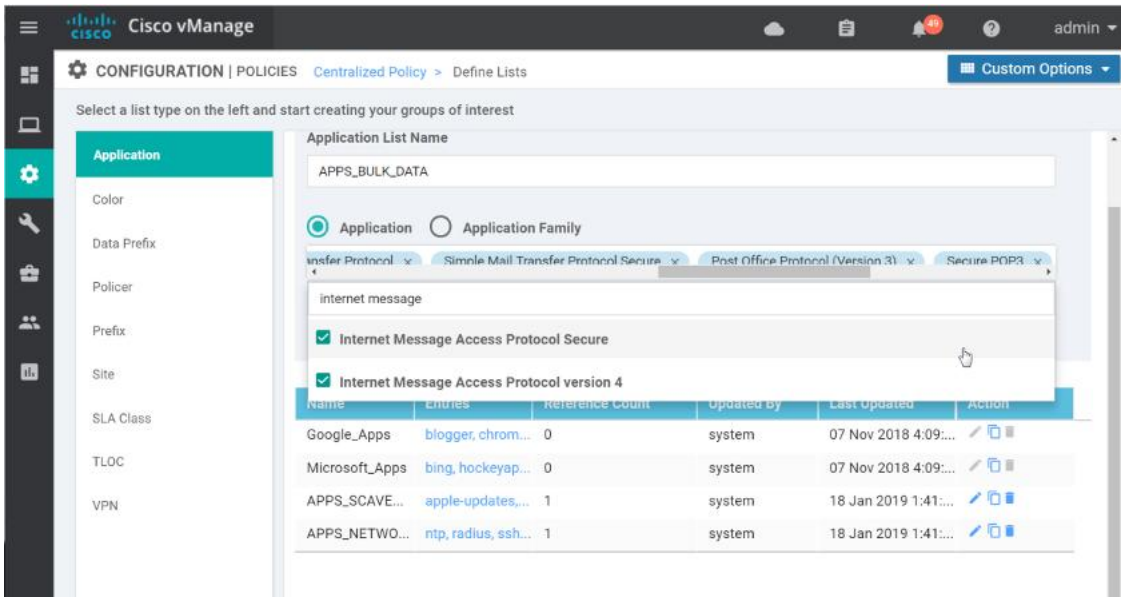
2. Select Custom Options and select Lists from the drop-down menu in the Centralized Policy section.

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

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.

Quality of service applications list (example)

Application list name	Application
APPS_SCAVENGER	Apple Update, Twitter, Instagram, Youtube HD, Google Play Music, Facebook Mail
APPS_BULK_DATA	File Transfer Protocol (FTP), File Transfer Protocol Secure, File Transfer Protocol Data, Trivial File Transfer Protocol (TFTP), Lotus Notes, Outlook Web App, Simple Mail Transfer Protocol (SMTP), Simple Mail Transfer Protocol Secure, Post Office Protocol (Version 3) (POP3), Secure POP3, Internet Message Access Protocol Version 4 (IMAP), Internet Message Access Protocol Secure



5. Click the Add button to save the application list.

6. 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.

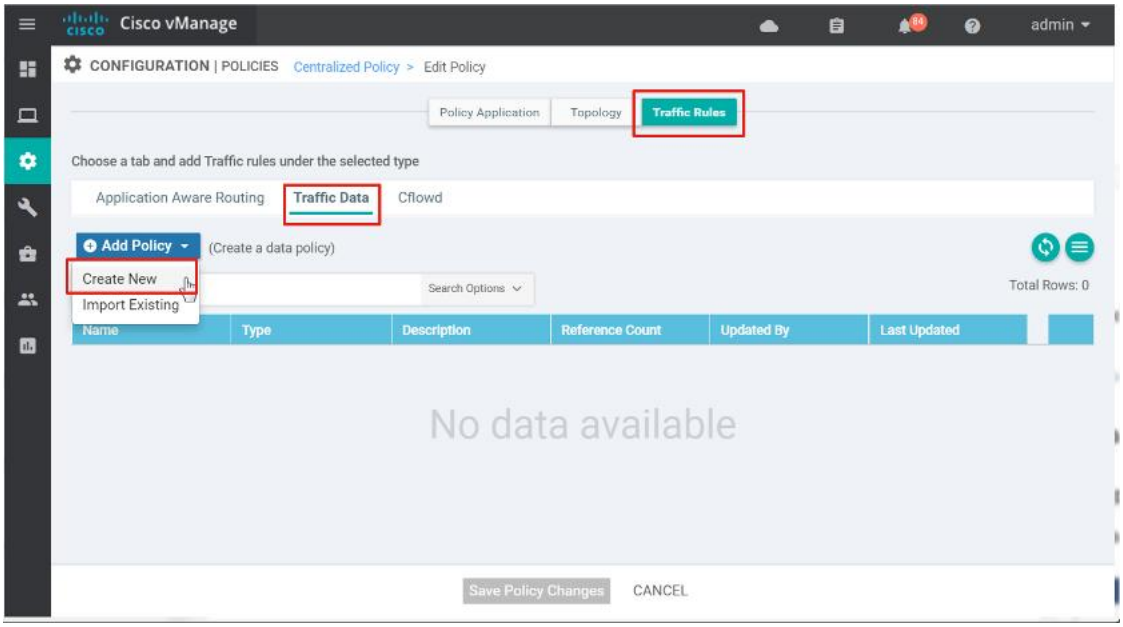
7. If the data prefix list MGT_Servers is not configured, then create a Data Prefix list to use within the QoS policy. Select New Data Prefix List. Type the Data Prefix List Name (MGT_Servers), then in the Add Data Prefix text box, type in the data prefix list (10.4.48.10/32,10.4.48.13/32,10.4.48.15/32,10.4.48.17/32)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

8. Go to Configuration>Policies and ensure the Centralized Policy tab is selected.

9. To the right of Global_policy, select **...** and select Edit.

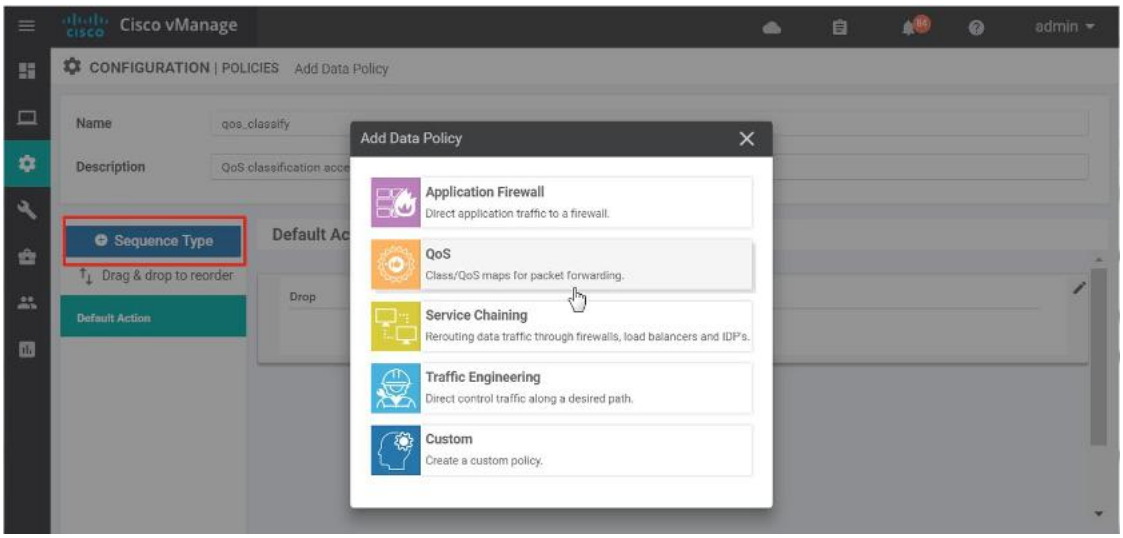
10. Select the Traffic Rules box at the top of the page to create a centralized data policy.

11. Select the Traffic Data tab. Select Add Policy and select Create New from the drop-down menu.

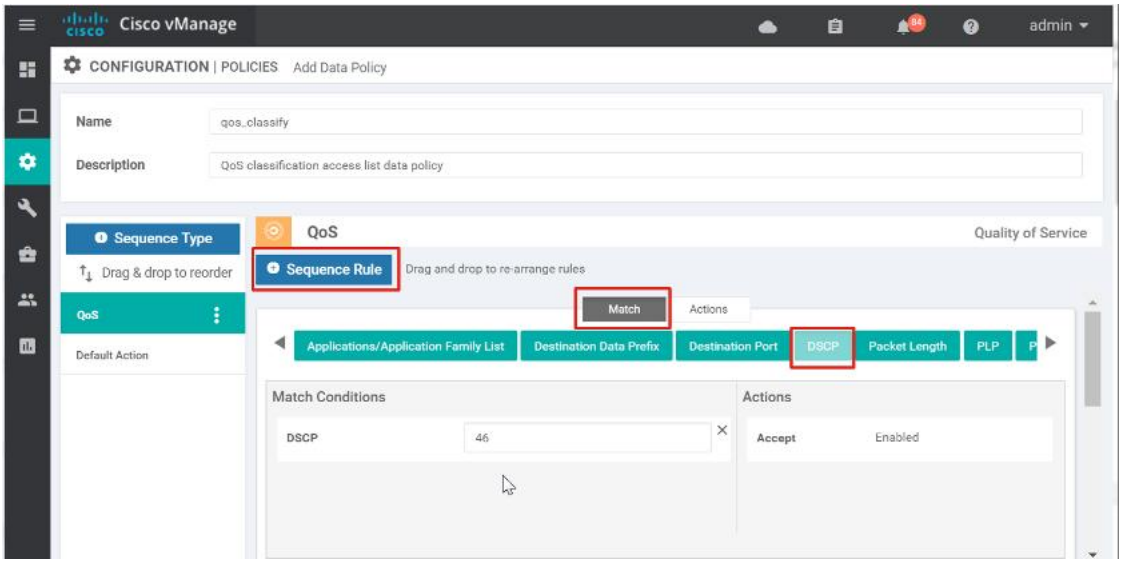


12. Type in the Name (qos_classify) and Description (QoS classification access list data policy).

13. Select Sequence Type, and select QoS from the Add Data Policy pop-up window.

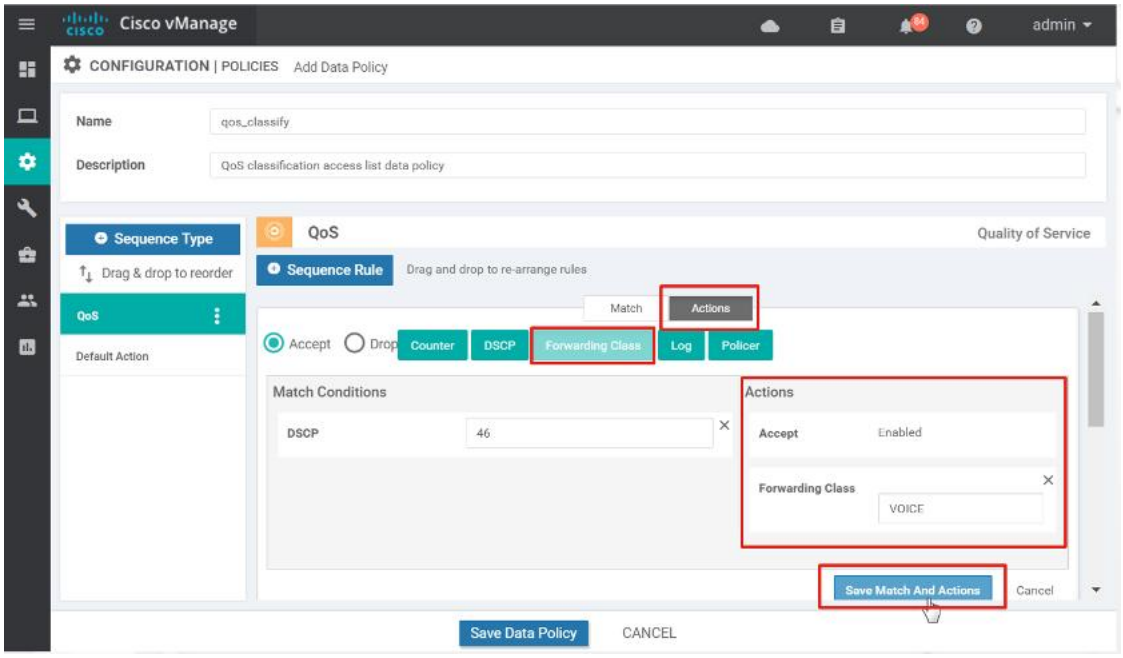


14. Select Sequence Rule and select the match conditions (DSCP 46).



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

16. Select Save Match and Actions.



17. Repeat steps 12-15 for the remaining match/action statements:

QoS classification access list

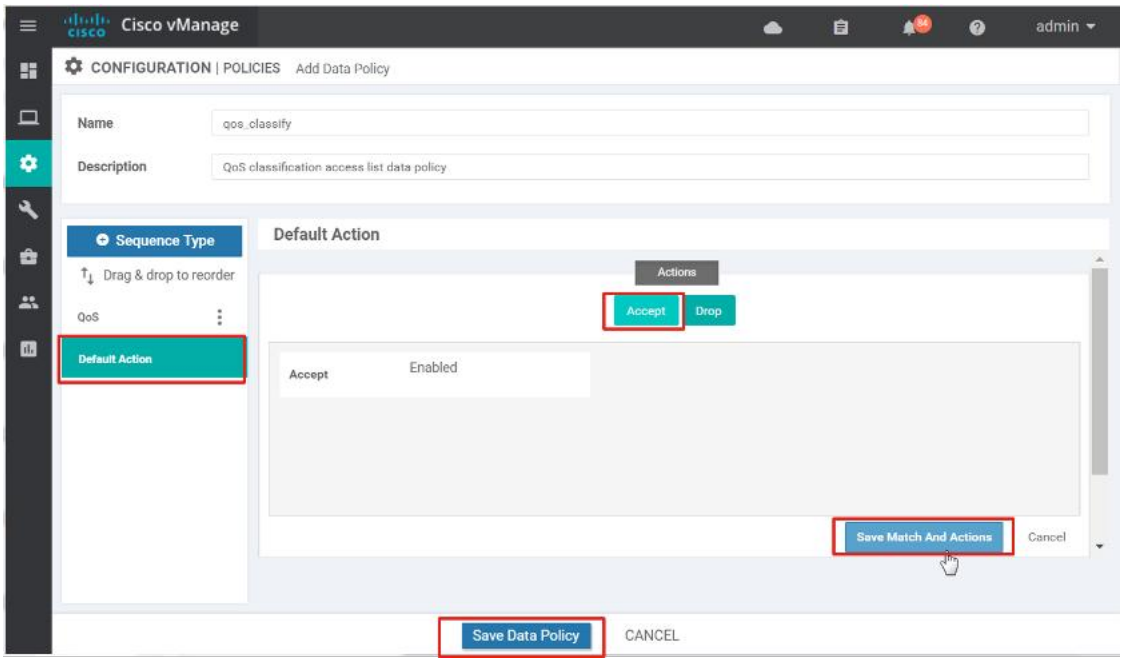
Match conditions	Accept or drop	Actions
DSCP 46	Accept	Forwarding Class VOICE
DSCP 34 36 38	Accept	Forwarding Class INTERACTIVE_VIDEO

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

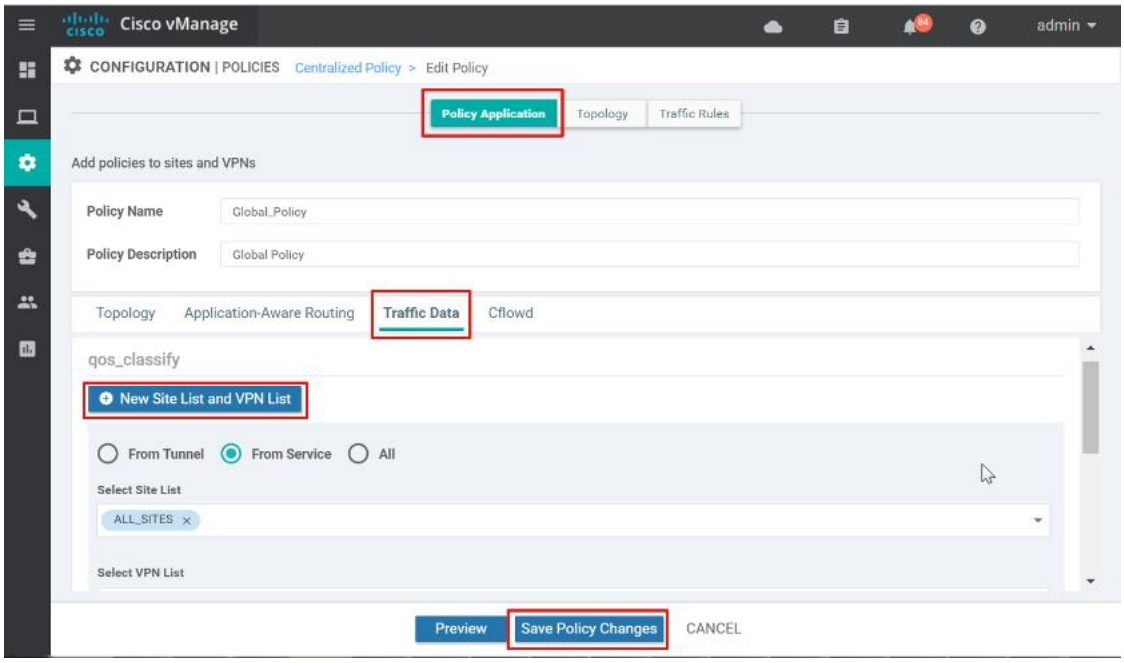
18. Select Default Action on the left side, and select the edit symbol.

19. Select the Accept box and select Save Match and Actions.

20. Select Save Data Policy.



21. You can now apply the policy. Select the Policy Application box at the top of the page.
22. Select the Traffic Data tab.
23. Under the qos_classify policy section, select New Site List and VPN list.
24. Select the From Service radio button since this is applied incoming on the LAN, or service side.
25. Under the Select Site List box, select ALL_SITES, and under the Select VPN List box, select ALL_VPNS. Select Add.
26. Select Save Policy Changes.



27. A window pops up indicating the policy will be applied to the vSmart controllers. Select Activate.

28. 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
- BR_INET_INT_DHCP

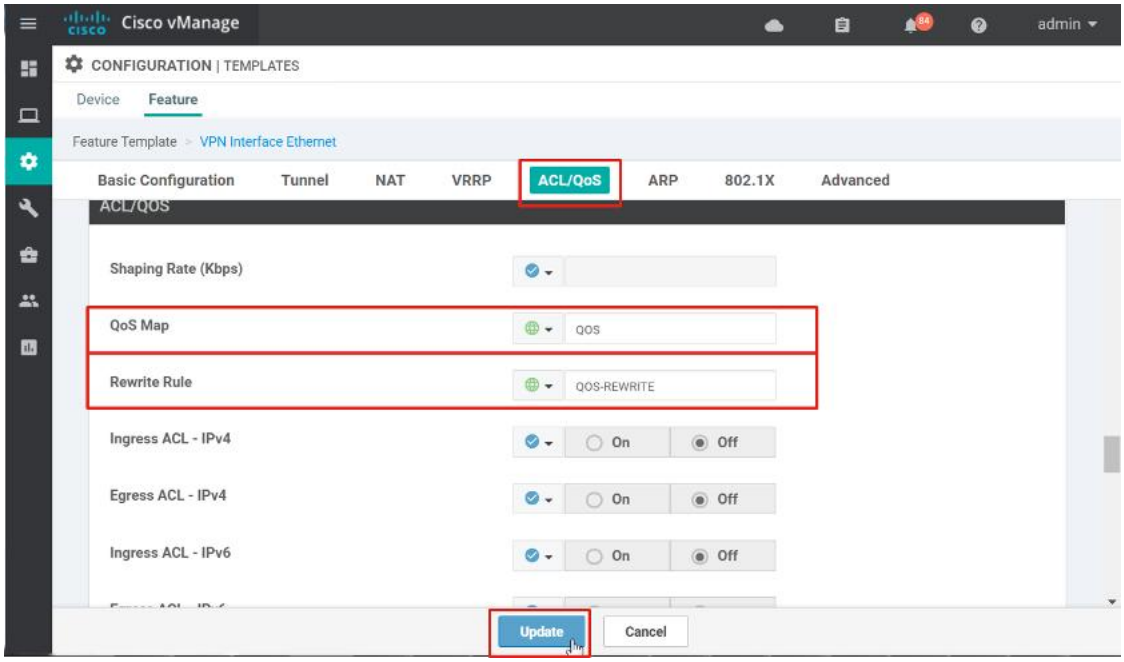
1. Go to Configuration>Templates and ensure that the Feature tab is selected.

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

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.

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

5. Select Update.



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.

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	18.3.5
Cloud	Cisco vSmart Controller	18.3.5
Cloud	Cisco vBond Orchestrator	18.3.5
Data center	Cisco vEdge 5000 Series Routers	18.3.5
Branch	Cisco vEdge 1000 Series Routers	18.3.5
Branch	Cisco vEdge 100 Series Routers	18.3.5
Branch	Cisco ISR4331 IOS XE SD-WAN Routers	16.9.4
Branch	Cisco ISR4351 IOS XE SD-WAN Routers	16.9.4

Location	Product	Software version
Data center	Cisco ASR 1002	3.16.8S
Data center	Cisco Catalyst® 3850 switch	3.6.8E
Data center	Cisco ASA 5512 firewall	9.6(4)20
Branch	Cisco Catalyst 3850 switch	3.6.8E
Branch	Cisco Catalyst 2960X switch	15.2(4)E6
Branch	Catalyst 3750E switch	15.2(4)E6
Branch	Catalyst 3650 switch	3.6.8E
Branch	4321 Integrated Services Router (ISR) / K9	16.3.7

Appendix B: Prepare IOS XE routers for SD-WAN deployment

Before deploying IOS XE SD-WAN device in the network:

- Ensure that all hardware and software requirements have been met.
- Upgrade the rommon image if need be.
- Convert the devices from IOS XE to IOS XE SD-WAN code.

- Update the Cisco Plug and Play Connect portal with IOS XE device information for authenticating the IOS XE SD-WAN devices into the SD-WAN overlay network.

Procedure 1: Check the hardware and software requirements

It is important that all hardware and software requirements are met before converting a device from IOS XE to IOS XE SD-WAN software and deploying the device into the SD-WAN overlay.

See https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_Cisco_IOS_XE_Routers to review all hardware and software requirements.

To summarize some of the major requirements:

- Ensure you have a supported router model and supported interface modules. Remove modules that are unsupported. Use show inventory on the CLI to check for unsupported hardware interface modules.
- Ensure the DRAM and bootflash memory requirements are met.
- Ensure the IOS XE routers are running at least the minimum rommon version supporting the SD-WAN image, though the latest maintenance is recommended.
- Ensure that you have a Smart licensing account.
- Ensure the SD-WAN controllers are running software release 18.3 at a minimum
- If you have a vEdge and IOS XE mixed environment, ensure the vEdge routers are at 17.2.1 or higher, and if both are deployed at the same site, ensure the vEdge router software is 18.3 or higher.

Tech tip: In IOS XE SD-WAN software version 16.9, it is required that all unsupported modules be removed before converting an IOS XE router to SD-WAN code. If you do not do this, the code may not be fully installed and properly functioning, and it may be impossible to deploy vManage templates to the device. If you convert to SD-WAN code, remove an unsupported module, and find that the interfaces still show up in the output of the **show sdwan running-config** command, you can clear the configuration by typing **request platform software sdwan config reset** followed by a **reload**.

See also: SD-WAN on Cisco IOS XE Routers: An End-to-End View for information on requirements, licensing, the upgrade process, typical deployment cases, and caveats for the initial software release: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741071.pdf

Procedure 2: Upgrade the rommon image

Use the CLI command, show rom-monitor or show platform to see the current rommon version. Under show platform, the rommon version is under the Firmware Version column next to R0. If the rommon does not need upgrading, skip to the next procedure.

```
ISR4351#show rom-monitor r0

System Bootstrap, Version 16.2(2r), RELEASE SOFTWARE
```

```
Copyright (c) 1994-2016  by cisco Systems, Inc.
```

1. Connect to the management console of the router.

```
ISR4351#copy ftp://admin:c1sco123@192.168.254.51/isr4200_4300_rommon_169_1r_SPA.pkg
bootflash:

Destination filename [isr4200_4300_rommon_169_1r_SPA.pkg]?

Accessing ftp://*:*@192.168.254.51/isr4200_4300_rommon_169_1r_SPA.pkg...

Loading isr4200_4300_rommon_169_1r_SPA.pkg !!!!!!!!!!!!!!!!!!!!

[OK - 5010380/4096 bytes]

5010380 bytes copied in 1.318 secs (3801502 bytes/sec)
```

2. Run the upgrade rom-monitor command to begin the rommon upgrade process. Note: Do not interrupt the rommon upgrade as there may be some situations that make the router unrecoverable.

```
ISR4351#upgrade rom-monitor filename bootflash:isr4200_4300_rommon_169_1r_SPA.pkg R0
```

3. Reload the router to make the new rommon version permanent.

```
ISR4351#reload
```

4. Verify the rommon version when the router finishes booting.

```
ISR4351#sh rom-mon R0


System Bootstrap, Version 16.9(1r), RELEASE SOFTWARE

Copyright (c) 1994-2018  by cisco Systems, Inc.
```

See https://www.cisco.com/c/en/us/td/docs/routers/access/4400/cpld/isr4400_hwfp.html for more information.

Procedure 3: Upgrade to the SD-WAN image

1. Connect to the management console of the router.

2. Copy the IOS XE SD-WAN image into bootflash from an external file server.

```
ISR4351#copy ftp://admin:c1sco123@192.168.254.51/isr4300-ucmk9.16.9.3.SPA.bin bootflash:

Destination filename [isr4300-ucmk9.16.9.3.SPA.bin]?

Accessing ftp://*:*@192.168.254.51/isr4300-ucmk9.16.9.3.SPA.bin...

Loading isr4300-ucmk9.16.9.3.SPA.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
[OK - 421480892/4096 bytes]

421480892 bytes copied in 106.309 secs (3964677 bytes/sec)
```

3. Backup the running configuration and save it to the router's bootflash.

```
ISR4351#copy run bootflash:original-xe-config

Destination filename [original-xe-config]?


5320 bytes copied in 1.178 secs (4516 bytes/sec)
```

4. Remove all existing boot statements.

```
ISR4351#sh run | include boot

boot-start-marker

boot system flash bootflash:isr4300-universalk9.16.03.07.SPA.bin

boot-end-marker

ISR4351#config t

Enter configuration commands, one per line.  End with CNTL/Z.

ISR4351(config)#no boot system flash bootflash:isr4300-universalk9.16.03.07.SPA.bin
```

5. Configure a boot system command that points to the new SD-WAN image.

```
ISR4351(config)#boot system flash bootflash:isr4300-ucmk9.16.9.3.SPA.bin
```

6. Ensure that the config register is set to 0x2102, so that the image will boot properly from bootflash.

```
ISR4351(config)#config-reg 0x2102

ISR4351(config)#end
```

7. Save the configuration so that the boot variables will be saved.

```
ISR4351#write mem
```

8. Verify that the BOOT variable points to the XE SD-WAN image and the configuration register is set to 0x2102 or that it will be set to 0x2102 at the next reload.

```
ISR4351#show bootvar

BOOT variable = bootflash:isr4300-ucmk9.16.9.3.SPA.bin,1;

CONFIG_FILE variable does not exist

BOOTLDR variable does not exist

Configuration register is 0x2102 (will be 0x2012 at next reload)
```

9. Remove all existing configuration from the router.

```
ISR4351#write erase
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

ISR4351#show startup-config

startup-config is not present
```

10. Reload the router. If prompted to save the configuration, enter No.

```
ISR4351#reload

Proceed with reload? [confirm]
```

11. The router reboots with the XE SD-WAN image. The initial configuration dialog should be presented when the router boots. When prompted to enter the initial configuration dialog, enter No. When prompted to terminate autoinstall, enter yes.

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes
```

12. The router will finish booting. You may either get a router prompt or Username/Password prompt. If you get the Router> prompt, type in enable. If you get the Username/Password prompt, log in with the default username, which is admin, and the default password, which is admin. You should then get a Router prompt. If not already in enable mode, enter enable.

```
Router>enable

Router#
```

or

```
User Access Verification


Username: admin

Password:

Router#
```

13. Stop PnP and allow the XE SD-WAN packages to install. The install can take a little over a minute to complete.

```
Router#pnpa service discovery stop

PNP-EXEC-DISCOVERY (1): Stopping PnP Discovery...

      …
```

```
%INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: packtool: Completed expand package running
```

14. Once the router has completed expanding the SD-WAN package, activate the SD-WAN image on the router using the request platform software sdwan software reset command. The router automatically reboots after the SD-WAN package has been activated. The activation can take a little over 2 minutes to complete while the reboot can take roughly between 4 and 4.5 minutes.

```
Router#request platform software sdwan software reset

%INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install commit

 …

%INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install activate
PACKAGE
```

15. After the router reboots, you should see the system configuration dialog. When prompted to enter the initial configuration dialog, enter no. When prompted to terminate autoinstall, enter yes.

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes
```

16. You may either get a Router prompt or Username/Password prompt. If you get the Router> prompt, type in enable. If you get the Username/Password prompt, log in with the default username, which is admin, and the default password, which is admin. You should then get a Router prompt. If not already in enable mode, enter enable.

```
Router>enable

Router#
```

or

```
User Access Verification

Username: admin

Password: admin

Router#
```

17. If you need to enter configuration mode, first stop PnP. You won't be able to enter configuration mode until PnP has been disabled.

```
Router#pnpa service discovery stop

PNP-EXEC-DISCOVERY (1): Stopping PnP Discovery...
```

18. Verify the system status.

```
Router#show sdwan system

Viptela (tm) vedge Operating System Software

Copyright (c) 2013-2017 by Viptela, Inc.
```

```
Controller Compatibility: Pkginfo File Error
Version: 16.9.3
Build: Not applicable

System logging to host  is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Disabled
Testbed mode:            Enabled

Last reboot:             LocalSoft.
CPU-reported reboot:     LocalSoft
Boot loader version:     Not applicable
System uptime:           0 days 00 hrs 06 min 45 sec
Current time:            Thu Dec 06 16:27:30 UTC 2018

Load average:            1 minute: 1.03, 5 minutes: 1.76, 15 minutes: 1.32
Processes:               525 total
CPU allocation:          8 total,   8 control,   0 data
CPU states:              7.60% user,   6.80% system,   85.00% idle
Memory usage:            16352320K total,    3127396K used,   13225244K free
                         274620K buffers,  1931356K cache

Disk usage:              Filesystem      Size   Used  Avail   Use %  Mounted on
                         /dev/bootflash1       14091M  3036M  10338M   23%   /bootflash

Personality:             vedge
Model name:              vedge-ISR-4351
Services:                None
vManaged:                false
Commit pending:          false
```

```
Configuration template:  None
```

Tech tip: Note if you try to issue a sdwan command, such as **show sdwan system**, and you receive **Failed to connect to server** error, make certain that PnP is first disabled with the **pnp service discovery stop** command.

19. To ensure PnP will run on the next power on or reboot, you can clear the configuration by running the CLI command, request platform software sdwan config reset.

20. If needed, configure the Plug and Play (PnP) Connect portal with the necessary information so that the routers can be authorized by the controllers in the overlay network. The portal also allows the IOS XE SD-WAN devices to be automatically provisioned in the network. See Appendix C for more information about the PnP Connect Portal.

To revert back to IOS XE:

1. Ensure the IOS XE image is in bootflash. If not, copy it into bootflash after ensuring there is reachability to the external file server.

```
ISR4351#copy ftp://admin:c1sco123@192.168.254.51/isr4300-universalk9.16.03.07.SPA.bin
bootflash:

Destination filename [isr4300-universalk9.16.03.07.SPA.bin]?

Accessing ftp://*:*@192.168.254.51/isr4300-
universalk9.16.03.07.SPA.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!~

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 459907472/4096 bytes]

459907472 bytes copied in 164.042 secs (2803596 bytes/sec)
```

2. Issue the CLI command, request platform software sdwan config reset to delete the SD-WAN startup configuration (if desired).

```
ISR4351#request platform software sdwan config reset

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

3. Set the config-register to 0x0 to boot into rommon.

```
ISR4351#config-t

admin connected from 127.0.0.1 using console on ISR4351

ISR4351(config)# config-reg 0x0

ISR4351(config)# commit

Commit complete.

ISR4351(config)# end

ISR4351#show bootvar

BOOT variable = bootflash:packages.conf,1;bootflash:isr4300-ucmk9.16.9.3.SPA.bin,1;
```

```
CONFIG_FILE variable does not exist

BOOTLDR variable does not exist

Configuration register is 0x2102 (will be 0x0 at next reload)
```

4. Reload the router.

```
ISR4351#reload

Proceed with reload? [confirm]
```

5. Once in rommon, boot the desired IOS XE image sitting on bootflash.

```
System Bootstrap, Version 16.9(1r), RELEASE SOFTWARE

Copyright (c) 1994-2018  by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft

ISR4351/K9 platform with 16777216 Kbytes of main memory


Rommon 1 > boot bootflash:isr4300-universalk9.16.03.07.SPA.bin

Located isr4300-universalk9.16.03.07.SPA.bin

################################################################################################
################################################################################################
#################################################
```

6. Configure a boot statement pointing to the current image.

```
Router#config t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#boot system flash bootflash:isr4300-universalk9.16.03.07.SPA.bin
```

7. Set the configuration register to 0x2102 and save the configuration.

```
Router(config)#config-reg 0x2102

Router(config)#end

Router#write mem

Building configuration...

[OK]
```

Appendix C: Plug and Play (PnP) Connect Portal

The PnP portal is located at http://software.cisco.com. At this website, you can download software, manage devices through the PnP Connect portal, and manage licenses. Licenses can be managed with the traditional method or through Smart accounts. Smart accounts are required in order to use smart licensing and they provide a central location where you can manage Cisco licenses across the entire organization. After you set up a Smart Account, you have the flexibility to create sub accounts (virtual accounts) to help manage your licenses for departments, areas, or locations within your organization. A virtual account is like a file folder, you can add multiple virtual accounts based on your business functions. A Smart Account and Virtual Account is required in order to create a controller profile on the PnP Connect portal.

For additional information on Smart Accounts and Smart Licensing:

https://cisco.com/go/smartaccounts

https://cisco.com/go/smartlicensing

The Plug and Play Connect portal (https://software.cisco.com/#pnp-devices) contains a list of WAN Edge devices and allows you to do two things:

- Create a serial authorization file for the WAN Edge hardware that you can load into vManage manually. Alternatively, you can allow vManage to sync to the PnP account to download the serial authorization information without manual intervention. Without the serial authorization file, the WAN Edge routers cannot join the overlay network.
- Enable automatic network provisioning of the IOS XE SD-WAN routers. A controller profile is created within the portal which defines your vBond and organization name information. On bootup, the IOS XE SD-WAN router looks for devicehelper.cisco.com, which directs the router to the PnP portal. The PnP portal checks the serial number of the router and pushes key parameters to it, such as vBond IP address and organization name. From there, the router contacts the vBond orchestrator and controller connectivity is initiated from there. The PnP portal information is used to populate the Zero-Touch Provisioning (ZTP) servers so the vEdge routers can be enabled for automatic network provisioning.

If you have a Cisco cloud-hosted controller deployment, the controller profile should already be created in the PnP portal. Also, WAN Edge devices that are ordered through Cisco Commerce Workspace (CCW) with a Smart account and Virtual account associated with them should be automatically pushed to the PnP portal. vEdge device information is automatically pushed from the PnP server to the ZTP server for automatic provisioning.

For on-prem controller deployments, a controller profile can be created manually and WAN Edge devices that are not already in the PnP portal can also be added manually.

Within the PnP Connect portal page, you can:

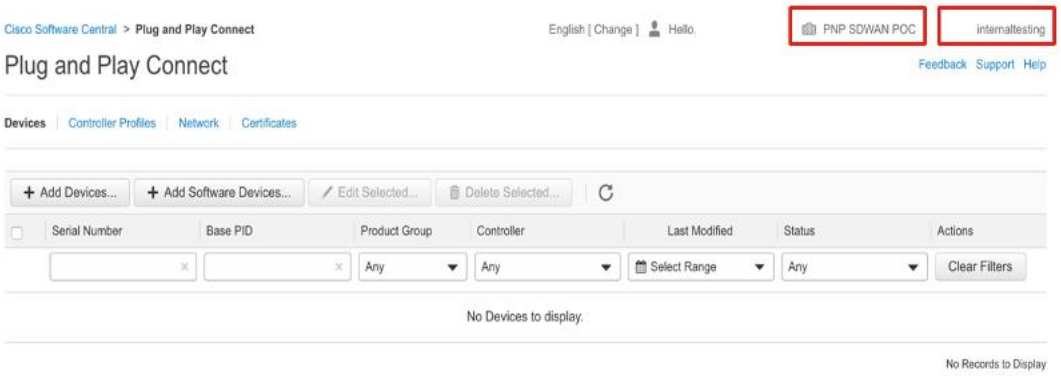
- Create a controller profile if one hasn't already been created
- Add WAN Edge devices to the portal and associate them with a controller profile
- Download the authorized device serial number file

Procedure 1: Log into the PnP Connect portal

1. Navigate to https://software.cisco.com

2. In the Network Plug and Play section, click Plug and Play Connect. If you are not logged in already, you will be prompted for a Cisco Account username and password. The Plug and Play Connect dialog box opens.

3. Within the Plug and Play Connect portal, find your Virtual Account linked to the Smart Account on the top right. Note: If you are unable to navigate to this page, ensure that the entered login user id and credentials have a valid Smart Account and Virtual Account associated with it.

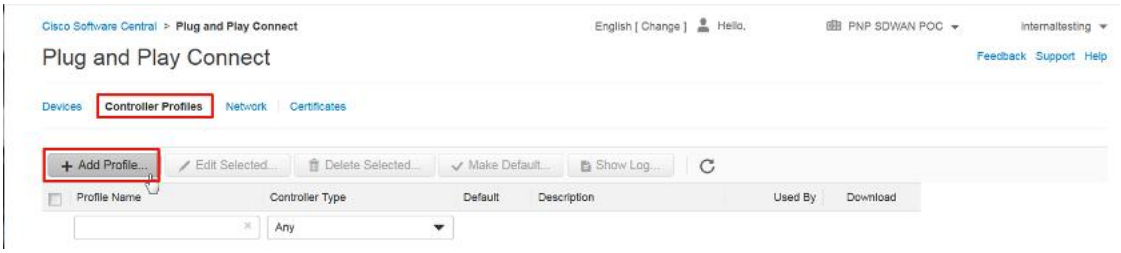


If you have not already created the controller profile, do so now. If you have a Cisco-hosted controller model, the information pertaining to your vBond controller should be pre-populated within the controller profiles and you can skip procedure 2.

Procedure 2: Configure the controller file

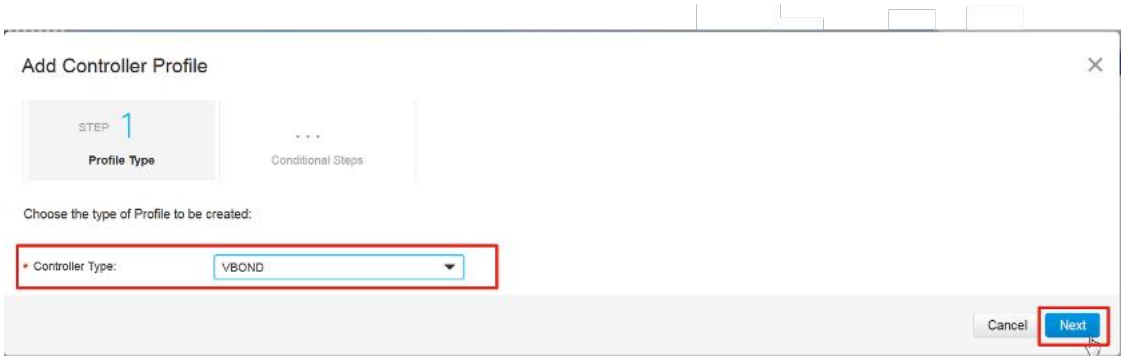
1. Click the Controller Profiles tab located directly beneath the Plug and Play Connect title and to the right of the Devices tab.

2. Click Add Profile. The Add Controller Profile dialog box opens with Step 1 Profile Type highlighted.



3. In the Controller Type drop-down, select vBond.

4. Click Next. Step 2 Profile Settings is highlighted and the profile setting fields displayed.



5. In the Profile Name field, enter a name for the controller profile you are creating (ENB-SOLUTIONS-VBOND in the example).

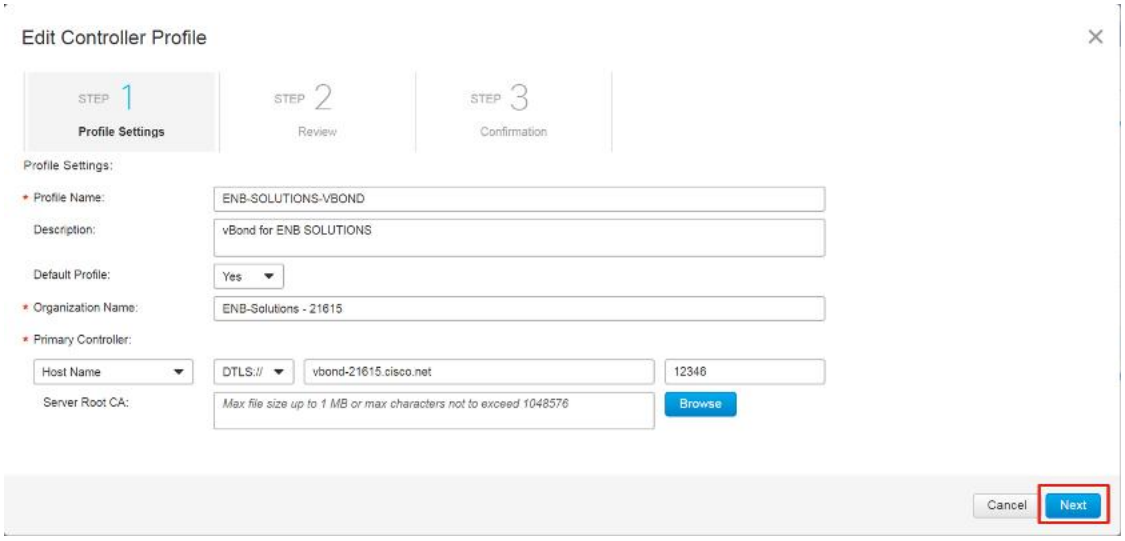
6. In the Description field, enter a description of the profile you are creating (vBond for ENB SOLUTIONS). This field is optional.

7. In the Default Profile drop-down box, select Yes if no other controller profile exists. Regardless of the setting, each WAN Edge that gets added to the PnP Connect portal needs to have a profile associated with it.

8. In the Organization Name field, enter the organization name (ENB-Solutions - 21615). You can find the organization name in the vManage GUI under the Administration> Settings screen.

9. In the Primary Controller drop down box, select Domain Name or IPv4 and fill out the vBond hostname or IP address. In the example, select Host Name from the drop-down box, and type in vbond-21615.cisco.net in the text box.

10. Click Next.



11. Review the options you just configured. Select Submit if they are correct, else go back to correct any settings.

12. The window indicates that the profile was successfully created. Select Done

Procedure 3: Add WAN Edge devices to the portal

You can manually add WAN Edge devices that have not already been added to the portal through the Cisco Commerce Workspace process.

To add IOS XE devices to the PnP portal, you need to know the Serial Number, the Base PID (Product Identifier), and the Certificate Serial number. This information is available within the show crypto pki certificates CISCO_IDEVID_SUDI command issued on CLI mode in IOS XE code. For the purposes of PnP, the Chassis Serial Number and SUDI certificate (Secure Unique Device Identification) is bound to the Smart account to enable authentication and easy provisioning of the IOS XE device. Note that you need to be on at least 3.14.0s software or higher in order to be able to run this command for the ISR4k.

```
ISR4351#show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
  Status: Available
  Certificate Serial Number (hex): 01373974
  Certificate Usage: General Purpose
  Issuer:
    cn=ACT2 SUDI CA
    o=Cisco
  Subject:
    Name: ISR4351/K9
    Serial Number: PID:ISR4351/K9 SN:FDO205108CB
```

If you have already converted to the SD-WAN image then use the command, show sdwan certificate installed instead.

```
Router#show sdwan certificate installed
Board-id certificate
--------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 20396404 (0x1373974)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=Cisco, CN=ACT2 SUDI CA
        Validity
```

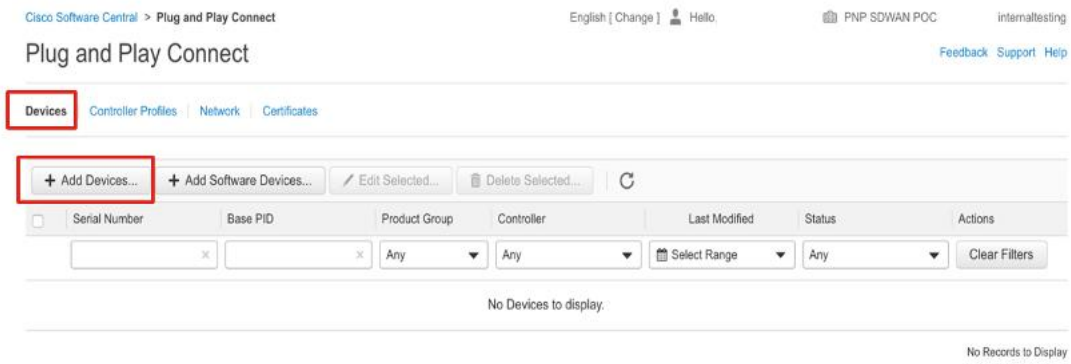
```
            Not Before: Dec 16 01:53:51 2016 GMT
            Not After : Dec 16 01:53:51 2026 GMT
        Subject: serialNumber=PID:ISR4351/K9 SN:FDO205108CB, O=Cisco,
```

Alternatively, you can use show sdwan certificate serial:

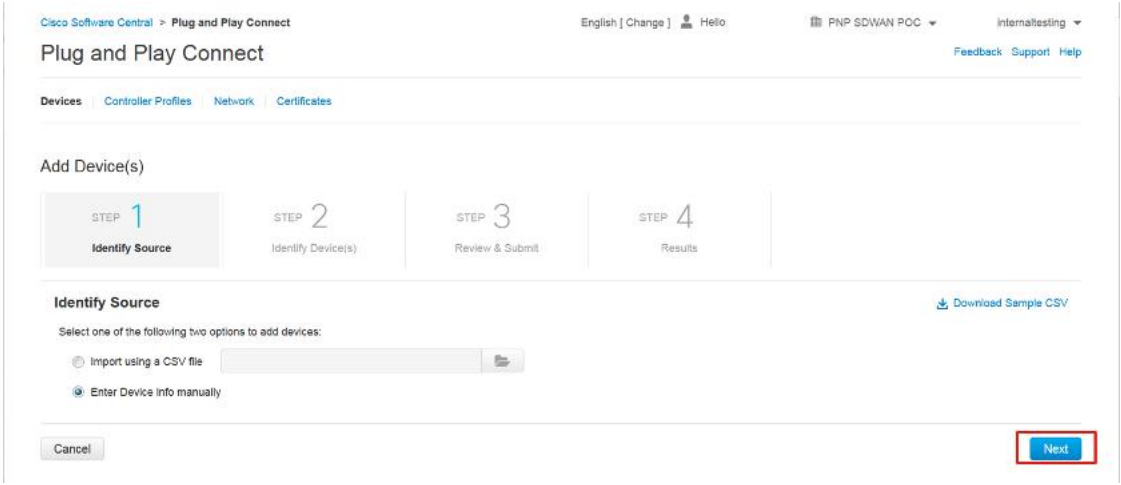
```
Router#show sdwan certificate serial
Chassis number: ISR4351/K9-FDO205108CB   Board ID serial number: 01373974
```

For vEdge routers, you need the serial number and PID of the device in order to add the device to the portal. If this isn't already known, the information can be retrieved using the show hardware inventory CLI command.

1. Navigate to https://software.cisco.com.
2. Under the Network Plug and Play section, click Plug and Play Connect.
3. Ensure the correct virtual account is chosen in the top right corner.
4. The Devices tab should be selected by default. Select Add Devices.



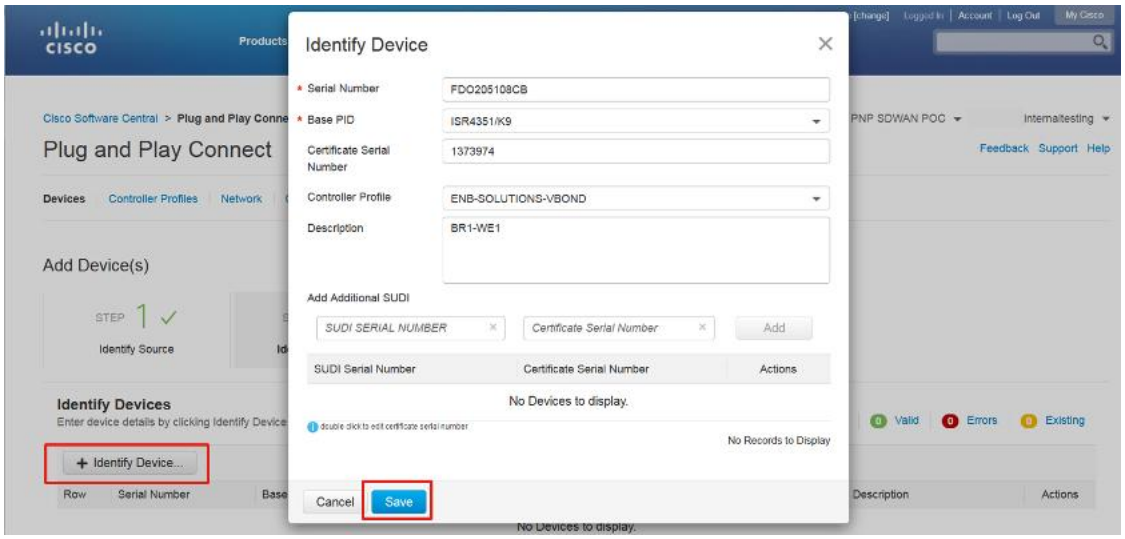
5. The first step is to identify how the device information will be entered, either manually or through a .csv file. Select the radio button next to Enter Device info manually and click Next.



6. Click on the Identify Device button. A popup-window will prompt for the Serial Number and Base PID, a Controller Profile to associate the device with, and a Description.

7. Enter the Serial Number (FDO205108CB), and the Base PID (ISR4351/K9) of the device. Once you select the Base PID textbox, enter values to search on, press enter and then select the PID that matches your device. Once a PID is selected, additional fields will appear. Enter the Certificate Serial Number (1373974) and choose the Controller Profile (ENB-SOLUTIONS-VBOND) to associate with the device when using PnP. Enter an optional Description (BR1-WE1) and click Save.

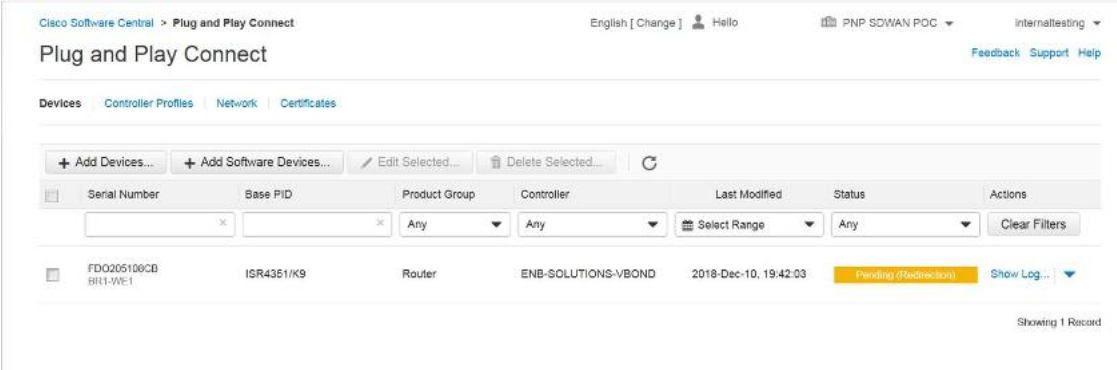
Note that the certificate serial number is in hex format with no preceding 0x.



8. Select Next. Review the device information, and then click Submit. Click the Back button if information for the device needs to be modified.

9. Click Submit. The page will indicate that it successfully added 1 device.

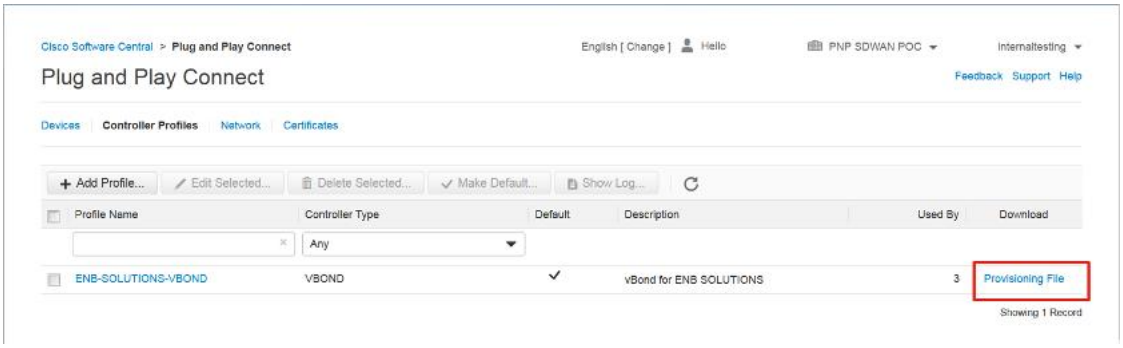
10. Select Done to refresh the page and go back to the Devices tab.



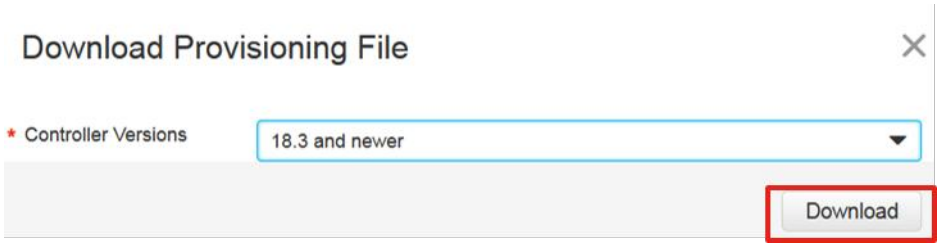
11. Repeat steps to add any additional devices.

Download the authorized serial number file

1. Navigate to https://software.cisco.com.
2. Under the Network Plug and Play section, click Plug and Play Connect.
3. Ensure the correct virtual account is chosen in the top right corner.
4. Click on Controller Profiles.
5. Next to the correct controller profile (ENB-SOLUTIONS-VBOND), click on the Provisioning File text.



6. On the pop-up window, select the controller versions from the drop-down box. Choose 18.3 and newer. Click Download and save the file to your computer. It is saved as serialFile.viptela by default.


Download Provisioning File
* Controller Versions
18.3 and newer
Download

Appendix D: vEdge 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
```

2. 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
```

3. 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
```

4. 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 E: Manual upgrade of a WAN Edge router

The following text provides an example of an upgrade using an external FTP server from the VPN 512 (vEdge) or Mgmt-intf VRF interface (cEdge). This process assumes that this 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.

vEdge Router

In this case, we are loading viptela-17.2.5-x86_64.tar.gz (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
```

IOS XE SD-WAN Router

In this case, we are loading isr4300-ucmk9.16.9.4.SPA.bin (ISR4300 IOS XE SD-WAN softare) from the FTP server at 192.168.254.51.

First, verify that the server is reachable.

```
wedge#ping vrf Mgmt-intf 192.168.254.51
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.51, timeout is 2 seconds:
```

```
.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

wedge#
```

Next, copy the image into the bootflash, ensuring that the source-interface for ftp has been defined.

```
wedge(config)# ip ftp source-interface GigabitEthernet0

wedge(config)# commit

wedge#copy ftp://admin:c1sco123@192.168.254.51/isr4300-ucmk9.16.9.4.SPA.bin bootflash:

Destination filename [isr4300-ucmk9.16.9.4.SPA.bin]?

Accessing ftp://*:*@192.168.254.51/isr4300-
ucmk9.16.9.4.SPA.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 421492305/4096 bytes]
```

Next, install the software. This will expand out the .bin file into several .pkg files. It will be activated with a separate command. Activation will cause the IOS XE SD-WAN router to reboot with the selected code version.

```
wedge#request platform software sdwan software install bootflash:isr4300-ucmk9.16.9.4.SPA.bin

wedge#

…

%INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install add bootflash:isr4300-
ucmk9.16.9.4.SPA.bin
%INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install add PACKAGE
bootflash:isr4300-ucmk9.16.9.4.SPA.bin
…
%IOSXE-5-PLATFORM: R0/0: VCONFD_NOTIFIER: Install status: 99f12590-7428-425b-9603-0d46ff919644
install-complete. Message Installation of 16.9.4 complete

%Cisco-SDWAN-cedge-action_notifier-6-INFO-1400002: R0/0: VCONFD_NOTIFIER: Notification: system-
software-install-status severity-level:minor host-name:br1-we2 system-ip:10.255.241.12
status:install-complete install-id:99f12590-7428-425b-9603-0d46ff919644 message:Installation of
16.9.4 complete
```

The following command needs to be executed in order to complete the install. If you don't complete this before activating, the router will roll back to the previous code version after 15 minutes.

```
wedge#request platform software sdwan software upgrade-confirm

INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install commit

%INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install commit SMU
```

Now, activate the new software version with the following command. The IOS XE SD-WAN router will then reboot and will boot into the desired software version.

```
wedge#request platform software sdwan software activate 16.9.4

wedge#
%INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install activate bootflash:isr4300-
ucmk9.16.9.4.SPA.bin

%INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install activate PACKAGEMar  6
17:52:34.491:


Initializing Hardware ...


Checking for PCIe device presence...done

System integrity status: 0x610

Rom image verified correctly


System Bootstrap, Version 16.9(1r), RELEASE SOFTWARE

Copyright (c) 1994-2018  by cisco Systems, Inc.
```

When the reboot is complete, you can log in and issue a "show version" to view the current software version.

```
wedge#show version

Cisco IOS XE Software, Version 16.9.4

Cisco IOS Software [], ISR Software (X86_64_LINUX_IOSD-UCMK9-M), Version 16.9.4, RELEASE SOFTWARE
(fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Fri 01-Feb-19 23:22 by cedge-sw-dev
```

Appendix F: 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-WE1
 ip address 10.4.1.1 255.255.255.252
 negotiation auto
interface GigabitEthernet0/1/2
 description TO DC1-WE2
 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
  network 10.255.241.106 mask 255.255.255.255
  ! 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-WE1
 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-WE2
 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-WE1
 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-WE2
 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-WE1
 no switchport
 ip address 10.4.1.13 255.255.255.252
!
interface GigabitEthernet1/0/12
 description To DC1-WE2
 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-WE1
 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-WE2
 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-WE1
 switchport trunk allowed vlan 10,20
```

```
 switchport mode trunk
 load-interval 30
 spanning-tree portfast trunk
!
interface TenGigabitEthernet2/0/1
 description To BR1-WE2
 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-WE1
 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-WE1
 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-WE2
 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-WE1
 no switchport
 ip address 10.105.0.1 255.255.255.252
 load-interval 30
!
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
 description To BR5-WE1
 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 G: vEdge configuration template summary

For convenience, this section summarizes the WAN Edge feature templates, device templates, and variable values for the SD-WAN devices in the example network.

Shared feature templates

System feature template

Devices: All except vManage and vSmart

Template: System

Template Name: System_Template

Description: System Template

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
	Console Baud Rate (bps)	Device Specific	system_console_baud_rate
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: All except vManage and vSmart

Template: Logging

Template Name: Logging_Template

Description: Logging Template

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: All except vManage and vSmart

Template: Basic Information/NTP

Template Name: NTP_Template

Description: NTP Template

NTP feature template settings

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

AAA feature template

Devices: All except vManage and vSmart

Template: Basic Information/AAA

Template Name: AAA_Template

Description: AAA Template

AAA feature template settings

Section	Parameter	Type	Variable/value
Authentication	Authentication Order	Drop-down	local
Local/New User	Name/Password/User Groups	Global	oper1/oper1/operator
	Name/Password/User Groups	Global	netadmin1/netadmin1/netadmin

OMP feature template

Devices: All except vManage and vSmart

Template: Basic Information/OMP

Template Name: OMP_Template

Description: OMP Template

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

Bidirectional Forwarding Detection (BFD) feature template

Devices: All except vManage and vSmart

Template: Basic Information/BFD

Template Name: BFD_Template

Description: BFD Template

BFD feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Poll Interval	Global	120000

Security feature template

Devices: All except vManage and vSmart

Template: Basic Information/Security

Template Name: Security_Template

Description: Security Template

Security feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Replay Window	Global/drop-down	4096

VPN512 feature template

Devices: All except vManage and vSmart

Template: VPN/VPN

Template Name: VPN512_Template

Description: VPN 512 Out-of-Band Management

VPN512 feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	512
	Name	Global	Management VPN
IPv4 Route/New 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 interface (VPN512)

Devices: All except vManage and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: VPN512_Interface

Description: VPN 512 Management Interface

VPN512 interface feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgt_int_x|x
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_mgt_int_ip_addr|maskbits

VPN interface Ethernet Loopback0

Devices: All except vManage and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: Loopback0

Description: Interface Loopback 0

VPN512 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	lo0_int_ip_addr|maskbits

Banner feature template

Devices: All except vManage and vSmart

Template: Other Templates/Banner

Template Name: Banner_Template

Description: Banner Template

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 feature template

Devices: All except vManage and vSmart

Template: Other Templates/SNMP

Template Name: SNMP_Template

Description: SNMP Template

SNMP feature template basic configurations 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	SNMP Version	Radio button	V2
SNMP Version/View & 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

SNMP Version/Trap	Trap Group/Group Name	Global	SNMP-GRP
	Trap Group/Trap Type Modules/Module Name	Global	all
	Trap Group/Trap Type Modules/Severity Levels	Global	critical, major, minor
	Trap Target Server/VPN	Global	1
	Trap Target Server/IP Address	Global	10.4.48.13
	Trap Target Server/UDP Port	Global	162
	Trap Target Server/Trap Group Name	Global	SNMP-GRP
	Trap Target Server/Community Name	Global	c1sco123
	Trap Target Server/Source Interface	Global	loopback0

Data center feature templates

Data center transport VPN (VPN 0) feature template

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN Interface Ethernet

Template Name: DC_ VPN0

Description: DC Transport VPN 0

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
	Next Hop	Device Specific	vpn0_inet_next_hop_ip_addr

Data center VPN interface (MPLS)

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN Interface Ethernet

Template Name: DC_ MPLS_Interface

Description: DC MPLS Interface

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_x|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	Clear-Dont-Fragment	Global	On

Data center VPN interface (Internet)

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN Interface Ethernet

Template Name: DC_INET_Interface

Description: DC Internet Interface

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_x|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	Clear-Dont-Fragment	Global	On

Data center service VPN 1

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN

Template Name: DC_VPN1

Description: DC Service VPN 1

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

Data center VPN interface Ethernet 1

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN Interface Ethernet

Template Name: DC_LAN _INT1

Description: DC LAN Interface 1

Data center VPN interface feature template settings (Interface 1)

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x
	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits

Data center VPN interface Ethernet 2

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: VPN/VPN Interface Ethernet

Template Name: DC _LAN_INT2

Description: DC LAN Interface 2

Data center VPN interface feature template settings (Interface 2)

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr|maskbits

Data center LAN Border Gateway Protocol (BGP)

Devices: ASR1001-HX, ASR1001-X, ASR1002-HX, ASR1002-X, vEdge 2000, vEdge 5000

Template: Other Templates/BGP

Template Name: DC_LAN_BGP

Description: DC LAN BGP Template

BGP feature template configuration settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_bgp _shutdown

	AS Number	Device Specific	lan_bgp_as_num
	Router ID	Device Specific	lan_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	lan_bgp_neighbor1_addr
	Description	Device Specific	lan_bgp_neighbor1_description
	Remote AS	Device Specific	lan_bgp_neighbor1_remote_as
	Address Family	Global	On
	Address Family	Global	ipv4-unicast
	Shutdown	Device Specific	lan_bgp_neighbor1_shutdown
	Advanced Options/Password	Device Specific	lan_bgp_neighbor1_password
	Advanced Options/Keepalive Time (seconds)	Global	3
	Advanced Options/Hold Time (seconds)	Global	9
Neighbor (2)	Address	Device Specific	lan_bgp_neighbor2_addr
	Description	Device Specific	lan_bgp_neighbor2_description
	Remote AS	Device Specific	lan_bgp_neighbor2_remote_as
	Address Family	Global	On
	Address Family	Drop-down	ipv4-unicast
	Shutdown	Device Specific	lan_bgp_neighbor2_shutdown
	Advanced Options/Password	Device Specific	lan_bgp_neighbor2_password
	Advanced Options/Keepalive Time (seconds)	Global	3

	Advanced Options/Hold Time (seconds)	Global	9

Branch feature templates

Branch VPN 0 feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN

Template Name: BR_VPN0

Description: Branch Transport VPN 0

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

Branch MPLS interface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_MPLS_INT

Description: Branch MPLS Interface with Static IP

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_x|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	Clear-Dont-Fragment	Global	On

Branch MPLS subinterface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_MPLS_SUBINT

Description: Branch MPLS Subinterface with Static IP

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_x|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	Clear-Dont-Fragment	Global	On

Branch Internet interface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_INET_INT

Description: Branch Internet Interface with Static IP

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_x|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	nat-enable

Advanced	Clear-Dont-Fragment	Global	On

Branch Internet DHCP interface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_INET_INT_DHCP

Description: Branch Internet Interface with DHCP IP

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	On
Allow Service	NTP	Global	On
Tunnel>Advanced Options>Encapsulation	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	nat-enable
Advanced	Clear-Dont-Fragment	Global	On

Branch Internet subinterface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_INET_SUBINT

Description: Branch Internet Subinterface with Static IP

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_x|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	nat-enable
Advanced	Clear-Dont-Fragment	Global	On

Branch TLOC Extension interface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_TLOC_EXT_INT

Description: Branch TLOC Extension Interface/Subinterface

Branch VPN0 TLOC Ext interface/subinterface feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_tloc_ext_int_shutdown
	Interface Name	Device Specific	vpn0_tloc_ext_int_x|x_or_x|x.VLAN
	Description	Global	TLOC Extension Interface
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 address	Device-specific	vpn0_tloc_ext_int_ip_addr|maskbits
Advanced	TLOC extension	Device-specific	vpn0_tloc_ext_wan_int_x|x

Branch WAN parent interface feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_WAN_Parent_INT

Description: Branch WAN Parent Interface

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_x|x
	Description	Global	WAN Parent Interface
Advanced	IP MTU	Global	1504

Branch VPN 0 MPLS BGP feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/BGP

Template Name: BR_VPN0_MPLS_BGP

Description: Branch VPN 0 MPLS BGP to Provider

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	vpn0_bgp_router_id
IPv4 Unicast Address Family	Maximum Paths	Global	2
	Address-Family	Drop-down	ipv4-unicast
	Network/Network Prefix	Device Specific	bgp_tloc_ext_prefix_to_advertise
Neighbor	Address	Device Specific	vpn0_bgp_neighbor_addr
	Description	Device Specific	vpn0_bgp_neighbor_description
	Remote AS	Device Specific	vpn0_bgp_neighbor_remote_as
	Address Family	Global	On

	Address Family	Drop-down	ipv4-unicast
	Route Policy In	Global	On
	Policy Name	Global	DENY-ALL
	Shutdown	Device Specific	vpn0_bgp_neighbor_shutdown

Branch VPN1 feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN

Template Name: BR_VPN1

Description: Branch VPN1

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
IPv4 Route [Mark as Optional Row]	Prefix	Device Specific	vpn1_lan_static_route_prefix|maskbits
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn1_lan_next_hop_ip_addr

Branch LAN interface 1 feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT1

Description: Branch LAN Interface 1

Branch VPN 1 interface 1 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10

Branch LAN interface 2 feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT2

Description: Branch LAN Interface 2

Branch VPN 1 interface 2 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10

Branch LAN interface 1 VRRP feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart z

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT1_VRRP

Description: Branch LAN Interface 1 VRRP

Branch VPN 1 interface 1 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int1_shutdown
	Interface Name	Device Specific	lan_int1_x|x_or_x|x.VLAN

	Description	Device Specific	lan_int1_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int1_ip_addr|maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP	Group ID	Global	1
	Priority	Device Specific	lan_int1_vrrp_priority
	Track OMP	Global	Off
	Track Prefix List	Global	Default-Route
	IP Address	Device Specific	lan_int1_vrrp_ip_addr

Branch LAN interface 2 VRRP feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_INT2_VRRP

Description: Branch LAN Interface 2 VRRP

Branch VPN 1 interface 2 VRRP feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_int2_shutdown
	Interface Name	Device Specific	lan_int2_x|x_or_x|x.VLAN
	Description	Device Specific	lan_int2_description
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	lan_int2_ip_addr/maskbits
Advanced	DHCP Helper	Global	10.4.48.10
VRRP	Group ID	Global	2
	Priority	Device Specific	lan_int2_vrrp_priority
	Track OMP	Global	Off
	Track Prefix List	Global	Default-Route
	IP Address	Device Specific	lan_int2_vrrp_ip_addr

Branch LAN parent interface template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: VPN/VPN Interface Ethernet

Template Name: BR_LAN_Parent_INT

Description: Branch LAN Parent Interface

Branch VPN 1 LAN parent interface feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	lan_parent_int_shutdown
	Interface Name	Device Specific	lan_parent_int_x|x
	Description	Global	LAN Parent Interface
Advanced	IP MTU	Global	1504

Branch LAN data VLAN DHCP server feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/DHCP Server

Template Name: BR_LAN_DATA_DHCP_Server

Description: Branch LAN DHCP Server for Data VLAN

Branch VPN 1 LAN DHCP server for data VLAN feature template

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

Branch LAN voice VLAN DHCP server feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/DHCP Server

Template Name: BR_LAN_VOICE_DHCP_Server

Description: Branch LAN DHCP Server for Voice VLAN

Branch VPN 1 LAN DHCP server for voice VLAN feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Address Pool	Device Specific	voice_dhcp_addr_pool|maskbits

	Exclude Addresses	Device Specific	voice_dhcp_addr_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

Branch LAN OSPF feature template

Devices: All except ASR1K, vEdge 2000, vEdge 5000, vManage, and vSmart

Template: Other Templates/OSPF

Template Name: BR_LAN_OSPF

Description: Branch LAN OSPF

LAN OSPF feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Router ID	Device Specific	lan_ospf_router_id
Redistribute	Protocol	Global	omp
Area	Area Number	Global	0
	Interface/Interface Name	Device Specific	lan_ospf_int_x|x
	Interface/Interface Cost	Device Specific	lan_ospf_int_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	lan_ospf_message_digest_key
Area Range	Address	Device Specific	lan_ospf_area_range_addr_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Global	On

Data center device template

Device Model: vEdge 5000

Template Name: DC_Hybrid_BGP

Description: DC MPLS & INET - Static to Transport and BGP to LAN

Data center device template: DC_Hybrid_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_Interface
	VPN Interface	DC_INET_Interface
VPN 512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		DC _VPN1
	BGP	DC_LAN_BGP
	VPN Interface	DC_LAN_INT1
	VPN Interface	DC_LAN_INT2
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		DC_Policy
Security Policy		
SNMP		SNMP_Template

Branch device templates

Branch_A_MPLS_BGP_TLOCEXT_VRRP

Device Model: ISR4351

Template Name: Branch_A_MPLS_BGP_TLOCEXT_VRRP

Description: Branch Dual WAN Edge Hybrid TLOC Extension with MPLS BGP and LAN-side Trunk and VRRP

Branch_A_MPLS_BGP_TLOCEXT_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	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN _INT1_VRRP
	VPN Interface	BR_LAN _INT2_VRRP
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_A_INET_TLOCEXT_VRRP

Device Model: ISR4351

Template Name: Branch_A_INET_TLOCEXT_VRRP

Description: Branch Dual WAN Edge Hybrid TLOC Extension with INET and LAN-side Trunk and VRRP

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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN _INT1_VRRP
	VPN Interface	BR_LAN _INT2_VRRP
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_B_MPLS_INET(DHCP)

Device Model: ISR4331

Template Name: Branch_B_MPLS_INET(DHCP)

Description: Branch Single WAN Edge Hybrid Internet DHCP address with LAN Trunk

Branch_B_MPLS_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
VPN0	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT_DHCP
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

Device Model: vEdge 100 B

Template Name: Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

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

Branch_B_MPLS_INET(DHCP)_LAN(DHCP) 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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT_DHCP
	VPN Interface	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	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	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

Device Model: ISR4351

Template Name: Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

Description: Branch Dual WAN Edge Hybrid TLOC Extension SubInts with MPLS BGP and LAN-side OSPF

Branch_C_MPLS_BGP_TLOCEXT_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	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_SUBINT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_C_INET_TLOCEXT_SubInt_OSPF

Device Model: vEdge 1000

Template Name: Branch_C_INET_TLOCEXT_SubInt_OSPF

Description: Branch Dual WAN Edge Hybrid TLOC Extension SubInts with INET and LAN-side OSPF

Branch_C_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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_SUBINT
	VPN Interface	BR_INET_INT
	VPN Interface	BR_TLOC_EXT_INT
	VPN Interface	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_D_MPLS_CE_INET_LAN-Static-Routing

Device Model: vEdge 100 B

Template Name: Branch_D_MPLS_CE_INET_LAN-Static-Routing

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

Branch_D_MPLS_CE_INET_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	VPN	BR_VPN0
	VPN Interface	BR_MPLS_INT
	VPN Interface	BR_INET_INT
VPN 512	VPN	VPN512_Template
	VPN Interface	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN Interface	BR_LAN_INT1
	VPN Interface	Loopback0
Banner		Banner_Template
Policy		Branch_Policy
SNMP		SNMP_Template

Data center variable values

DC1-WE1: DC_Hybrid_BGP

Data center 1 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	dc1-we1
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)	☐
Console Baud Rate (bps) (system_console_baud_rate)	115200
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_x|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_x|x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	10.4.1.6/30
Preference(vpn_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_x|x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.167/23
AS Number(lan_bgp_as_num)	65113
Shutdown(bgp_shutdown)	☐
Router ID(lan_bgp_router_id)	10.255.241.101
Network Prefix(lan_bgp_network_lo_addr|maskbits)	10.255.241.101/32
Address(lan_bgp_neighbor1_addr)	10.4.1.9
Address(lan_bgp_neighbor2_addr)	10.4.1.13
Description(lan_bgp_neighbor1_description)	Agg-Switch1
Description(lan_bgp_neighbor2_description)	Agg-Switch2
Shutdown(lan_bgp_neighbor1_shutdown)	☐
Shutdown(lan_bgp_neighbor2_shutdown)	☐
Remote AS(lan_bgp_neighbor1_remote_as)	65112
Remote AS(lan_bgp_neighbor2_remote_as)	65112
Password(lan_bgp_neighbor1_password)	cisco123
Password(lan_bgp_neighbor2_password)	cisco123
Interface Name(lan_int1_x|x)	ge0/4
Description(lan_int1_description)	To DC1-SW1 G1/0/11

Shutdown(lan_int1_shutdown)	☐
IPv4 Address(lan_int1_ip_addr|maskbits)	10.4.1.10/30
Interface Name(lan_int2_x|x)	ge0/5
Description(lan_int2_description)	To DC1-SW2 G1/0/11
IPv4 Address(lan_int2_ip_addr|maskbits)	10.4.1.14/30
Shutdown(vpn1_lan_int2_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.101/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-WE1
Location of Device(snmp_device_location)	Datacenter 1

* For IPSEC Tunnel preference, configure a number above 0 (100 in the example) to prefer this device to route traffic to ensure symmetry for DPI.

DC1-WE2: DC_Hybrid_BGP

Data center 1 WAN Edge 2 device template variable values

Variable	Value
Hostname(system_host_name)	dc1-we2
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)	☐
Console Baud Rate (bps)(system_console_baud_rate)	115200
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_x|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_x|x)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	10.4.2.6/30
Preference(vpn_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_x|x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.168/23
AS Number(lan_bgp_as_num)	65113
Shutdown(lan_bgp_shutdown)	☐
Router ID(lan_bgp_router_id)	10.255.241.102
Network Prefix(lan_bgp_network_lo_addr|maskbits)	10.255.241.102/32
Address(lan_bgp_neighbor1_addr)	10.4.2.9
Address(lan_bgp_neighbor2_addr)	10.4.2.13
Description(lan_bgp_neighbor1_description)	Agg-Switch1
Description(lan_bgp_neighbor2_description)	Agg-Switch2
Shutdown(lan_bgp_neighbor1_shutdown)	☐
Shutdown(lan_bgp_neighbor2_shutdown)	☐
Remote AS(lan_bgp_neighbor1_remote_as)	65112
Remote AS(lan_bgp_neighbor2_remote_as)	65112
Password(lan_bgp_neighbor1_password)	cisco123
Password(lan_bgp_neighbor2_password)	cisco123
Interface Name(lan_int1_x|x)	ge0/4
Description(lan_int1_description)	To DC1-SW1 G1/0/12

Shutdown(lan_int1_shutdown)	☐
IPv4 Address(lan_int1_ip_addr|maskbits)	10.4.2.10/30
Interface Name(lan_int2_x|x)	ge0/5
Description(lan_int2_description)	To DC1-SW2 G1/0/12
IPv4 Address(lan_int2_ip_addr|maskbits)	10.4.2.14/30
Shutdown(lan_int2_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.102/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	DC1-WE2
Location of Device(snmp_device_location)	Datacenter 1

Branch variable values

BR1-WE1: Branch_A_MPLS_BGP_TLOCEXT_VRRP

Branch 1 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br1-we1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,ISR4K,US,West,UG5,Primary
System IP(system_system_ip)	10.255.241.11
Site ID(system_site_id)	112001
Port Offset(system_port_offset)	1
Port Hopping(system_port_hop)	☑
Console Baud Rate (bps)(system_console_baud_rate)	9600
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_addr)	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
Network Prefix(bgp_tloc_ext_prefix_to_advertise)	10.101.1.0/30
Interface Name(vpn0_inet_int_x|x)	GigabitEthernet0/0/0
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_x|x)	GigabitEthernet0/0/2
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_ext_int_x|x_or_x|x.VLAN)	GigabitEthernet0/1/0
IPv4 Address(vpn0_tloc_ext_int_ip_addr|maskbits)	10.101.1.1/30
TLOC Extension(vpn0_tloc_ext_wan_int_x|x)	GigabitEthernet0/0/2
Shutdown(vpn0_tloc_ext_int_shutdown)	☐
Interface Name(lan_parent_int_x|x)	GigabitEthernet0/0/1
Shutdown(lan_parent_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_ x|x)	GigabitEthernet0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.143/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	

Prefix(vpn1_omp_aggregate_prefix)	10.101.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.10
Description(lan_int1_description)	Data Vlan
IPv4 Address(lan_int1_ip_addr|maskbits)	10.101.10.2/24
Shutdown(lan_int1_shutdown)	☐
Group ID(vpn_if_vrrp_grpid)	1
Priority(lan_int1_vrrp_priority)	200
IP Address(lan_int1_vrrp_ip_addr)	10.101.10.1
Interface Name(lan_int2_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.20
Description(lan_int2_description)	Voice Vlan
IPv4 Address(lan_int2_ip_addr|maskbits)	10.101.20.2/24
Shutdown(lan_int2_shutdown)	☐
Group ID(vpn_if_vrrp_grpid)	2
Priority(lan_int2_vrrp_priority)	200
IP Address(lan_int2_vrrp_ip_addr)	10.101.20.1
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.11/32
Shutdown(snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-WE1
Location of Device(snmp_device_location)	Branch 1

* For IPSEC Tunnel preference, configure a number above 0 (100 in the example) to prefer this device to route traffic to ensure symmetry for DPI.

BR1-WE2: Branch_A_INET_TLOCEXT_VRRP

Branch 1 WAN Edge 2 device template variable values

Variable	Value
Hostname(system_host_name)	br1-we2
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-112.0740
Device Groups(system_device_groups)	BRANCH,ISR4K,US,West,UG4,Secondary
System IP(system_system_ip)	10.255.241.12
Site ID(system_site_id)	112001

Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Console Baud Rate (bps)(system_console_baud_rate)	9600
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_x|x)	GigabitEthernet0/0/0
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_x|x)	GigabitEthernet0/0/2
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
Interface Name(vpn0_tloc_ext_int_x|x_or_x|x.VLAN)	GigabitEthernet0/1/0
IPv4 Address(vpn0_tloc_ext_int_ip_addr|maskbits)	10.101.2.2/30
TLOC Extension(vpn0_tloc_ext_wan_int_x|x)	GigabitEthernet0/0/0
Shutdown(vpn0_tloc_ext_int_shutdown)	☐
Interface Name(lan_parent_int_x|x)	GigabitEthernet0/0/1
Shutdown(lan_parent_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_x|x)	GigabitEthernet0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.144/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	

Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix) [optional]	10.101.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.10
Description(lan_int1_description)	Data Vlan
IPv4 Address(lan_int1_ip_addr|maskbits)	10.101.10.3/24
Shutdown(lan_int1_shutdown)	☐
Priority(lan_int1_vrrp_priority)	100
IP Address(lan_int1_vrrp_ip_addr)	10.101.10.1
Interface Name(lan_int2_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1.20
Description(lan_int2_description)	Voice Vlan
IPv4 Address(lan_int2_ip_addr|maskbits)	10.101.20.3/24
Shutdown(lan_int2_shutdown)	☐
Priority(lan_int2_vrrp_priority)	100
IP Address(lan_int2_vrrp_ip_addr)	10.101.20.1
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.12/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR1-WE2
Location of Device(snmp_device_location)	Branch 1

BR2-WE1: Branch_B_MPLS_INET(DHCP)

Branch 2 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br2-we1
Latitude(system_latitude)	33.4484
Longitude(system_longitude)	-97.335
Device Groups(system_device_groups)	BRANCH,ISR4K,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)	☑

Console Baud Rate (bps)(system_console_baud_rate)	9600
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_x|x)	GigabitEthernet0/0/0
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_x|x)	GigabitEthernet0/0/2
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
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_ x/x)	GigabitEthernet0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.134/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix) [optional]	10.102.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1
Description(lan_int1_description)	To Switch BR2-SW1
IPv4 Address(lan_int1_ip_addr|maskbits)	10.102.10.1/24
Shutdown(lan_int1_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.241.21/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR2-WE1

Location of Device(snmp_device_location)	Branch 2

*Fill in any next hop value for the Internet transport; the dynamic IP gateway value received from DHCP should overwrite this value.

BR3-WE1: Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

Branch 3 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br3-we1
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
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
Console Baud Rate (bps)(system_console_baud_rate)	115200
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_x|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_x|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(lan_parent_int_x|x)	ge0/0
Shutdown(lan_parent_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_x|x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.153/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix) [optional]	10.103.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	ge0/0.10
Description(lan_int1_description)	Data Vlan
IPv4 Address(vpn_int1_ip_addr|maskbits)	10.103.10.1/24
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(lan_int2_x|x_or_x|x.VLAN)	ge0/0.20
Description(lan_int2_description)	Voice Vlan
IPv4 Address(lan_int2_ip_addr|maskbits)	10.103.20.1/24
Shutdown(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(lo0_int_ip_addr|maskbits)	10.255.241.31/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR3-WE1
Location of Device(snmp_device_location)	Branch 3

*Fill in any next hop value for the Internet transport; the dynamic IP gateway value received from DHCP should overwrite this value.

BR4-WE1: Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

Branch 4 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br4-we1
Latitude(system_latitude)	33.754
Longitude(system_longitude)	-84.386
Device Groups(system_device_groups)	BRANCH,ISR4K,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)	☑
Console Baud Rate (bps)(system_console_baud_rate)	9600
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
Network Prefix(bgp_tloc_ext_prefix_to_advertise)	10.104.1.0/30
Interface Name(vpn0_mpls_int_x|x)	GigabitEthernet0/0/2
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
Bandwidth Downstream(vpn0_mpls_int_bandwidth_down)	500000

Interface Name(vpn0_inet_int_x|x.VLAN)	GigabitEthernet0/0/0.102
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_x|x)	GigabitEthernet0/0/0
Shutdown(vpn0_wan_parent_int_shutdown)	☐
Interface Name(vpn0_tloc_ext_int_x|x_or_x|x.VLAN)	GigabitEthernet0/0/0.101
IPv4 Address(vpn0_tloc_ext_int_ip_addr|maskbits)	10.104.1.1/30
TLOC Extension(vpn0_tloc_ext_wan_int_x|x)	GigabitEthernet0/0/2
Shutdown(vpn0_tloc_ext_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_x|x)	GigabitEthernet0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.145/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix) [optional]	10.104.0.0/16
Router ID(lan_ospf_router_id)	10.255.242.41
Interface Name(lan_ospf_int_x|x)	GigabitEthernet0/0/1
Interface Cost(lan_ospf_int_cost)	1
Message Digest Key(lan_ospf_message_digest_key)	cisco123
Address(lan_ospf_area_range_address_0)	10.104.0.0/16
Interface Name(lan_int1_x|x_or_x|x.VLAN)	GigabitEthernet0/0/1
Description(lan_int1_description)	To LAN-SW
IPv4 Address(lan_int1_ip_addr|maskbits)	10.104.0.2/30
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.242.41/32

Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR4-WE1
Location of Device(snmp_device_location)	Branch 4
vedgePolicy/ospf_metric	10

* For IPSEC Tunnel preference, configure a number above 0 (100 in the example) to prefer this device to route traffic to ensure symmetry for DPI.

BR4-WE2: Branch_C_INET_TLOCEXT_SubInt_OSPF

Branch 4 WAN Edge 2 device template variable values

Variable	Value
Hostname(system_host_name)	br4-we2
Latitude(system_latitude)	33.754
Longitude(system_longitude)	-84.386
Device Groups(system_device_groups)	BRANCH,v1000,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)	☑
Console Baud Rate (bps)(system_console_baud_rate)	115200
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_x|x_or_x|x.VLAN)	ge0/0
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	64.100.104.2/28
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_x|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_ext_int_x|x_or_x|x.VLAN)	ge0/2.102
IPv4 Address(vpn0_tloc_ext_int_ip_addr|maskbits)	10.104.2.2/30
TLOC Extension(vpn0_tloc_ext_wan_int_x|x)	ge0/0
Shutdown(vpn0_tloc_ext_int_shutdown)	☐
Interface Name(vpn0_wan_parent_int_x|x)	ge0/2
Shutdown(vpn0_wan_parent_int_shutdown)	☐
Address(vpn512_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_x|x)	mgmt0
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.162/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	
Address(vpn1_lan_next_hop_ip_addr) [optional]	
Prefix(vpn1_omp_aggregate_prefix) [optional]	10.104.0.0/16
Router ID(lan_ospf_router_id)	10.255.242.42
Interface Name(lan_ospf_int_x|x)	ge0/4
Interface Cost(lan_ospf_int_cost)	1
Message Digest Key(lan_ospf_message_digest_key)	cisco123
Address(lan_ospf_area_range_address_0)	10.104.0.0/16
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.242.42/32
Interface Name(lan_int1_x|x_or_x|x.VLAN)	ge0/4
Description(lan_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-WE2
Location of Device(snmp_device_location)	Branch 4

vedgePolicy/ospf_metric	20

BR5-WE1: Branch_D_MPLS_CE_INET_LAN-Static-Routing

Branch 5 WAN Edge 1 device template variable values

Variable	Value
Hostname(system_host_name)	br5-we1
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)	☑
Console Baud Rate (bps)(system_console_baud_rate)	115200
Address(vpn0_mpls_next_hop_ip_addr)	10.105.1.1
Address(vpn0_inet_next_hop_ip_addr)	64.100.105.1
Interface Name(vpn0_inet_int_x|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_x|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_mgt_next_hop_ip_addr)	192.168.255.1
Interface Name(vpn512_mgt_int_x|x_or_x|x)	ge0/1
IPv4 Address (vpn512_mgt_int_ip_addr|maskbits)	192.168.255.156/23
Prefix(vpn1_lan_static_route_prefix|maskbits) [optional]	10.105.0.0/16
Address(vpn1_br_next_hop_ip_addr) [optional]	10.105.0.1
Prefix(vpn1_omp_aggregate_prefix) [optional]	
Interface Name(lan_int1_x|x_or_x|x.VLAN)	ge0/0
Description(lan_int1_description)	To LAN-SW
IPv4 Address(lan_int1_ip_addr|maskbits)	10.105.0.2/30
Shutdown(vpn1_lan_int1_shutdown)	☐
IPv4 Address(lo0_int_ip_addr|maskbits)	10.255.242.51/32
Shutdown (snmp_shutdown)	☐
Name of Device for SNMP(snmp_device_name)	BR5-WE1
Location of Device(snmp_device_location)	Branch 5

Appendix H: WAN Edge router CLI-equivalent configuration

DC1-WE1

```
system
 host-name               dc1-we1
 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]
 !
 user netadmin1
  password [netadmin1 password]
  group    netadmin
 !
 user oper1
  password [oper1 password]
  group    operator
 !
!
logging
 disk
  enable
 !
 server 10.4.48.13
  vpn              1
  source-interface loopback0
 exit
!
ntp
 server time.nist.gov
  version 4
 exit
!
```

```
!
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 ah-no-id none
 !
!
snmp
 no shutdown
 name     DC1-WE1
 location "Datacenter 1"
 view isoALL
  oid 1.3.6.1
 !
 community c1sco123
  view          isoALL
  authorization read-only
 !
 trap target vpn 1 10.4.48.13 162
  group-name       SNMP-GRP
  community-name   c1sco123
  source-interface loopback0
 !
 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          "Internet 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
   allow-service https
  !
  clear-dont-fragment
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
  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
   allow-service https
  !
  clear-dont-fragment
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
  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_PRIMARY_WEDGE
   !
   neighbor 10.4.1.9
    description Agg-Switch1
    no shutdown
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$Ul4PnNm2A2l7VzXLNANucsxgO9rWg92MX8ukYNrfOak=
    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$9UfXCpP2QMNRWlUYX76YcDbKJR/X+HCnqpADfbC2Rxo=
    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
 cloud-qos
 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 1
   match
    address MPLS-Transport
   !
   action reject
   !
  !
  sequence 11
   match
    community Non-SD-WAN-Sites
   !
   action accept
```

```
  !
 !
 sequence 21
  match
   as-path Local-Routes
  !
  action accept
   set
    community 1:100
   !
  !
 !
 default-action reject
!
route-policy BGP_PRIMARY_WEDGE
 sequence 1
  action accept
   set
    metric 50
   !
  !
 !
 default-action reject
!
route-policy BGP_SECONDARY_WEDGE
 sequence 1
  action accept
   set
    metric 100
   !
  !
 !
 default-action reject
!
class-map
 class Queue0 queue 0
 class CRITICAL_DATA queue 1
 class Queue1 queue 1
 class BULK queue 2
```

```
 class Queue2 queue 2
 class CLASS_DEFAULT queue 3
 class Queue3 queue 3
 class INTERACTIVE_VIDEO queue 4
 class Queue4 queue 4
 class CONTROL_SIGNALING queue 5
 class Queue5 queue 5
!
rewrite-rule QOS-REWRITE
 class BULK low dscp 10 layer-2-cos 1
 class BULK high dscp 10 layer-2-cos 1
 class CLASS_DEFAULT low dscp 0
 class CLASS_DEFAULT high dscp 0
 class CONTROL_SIGNALING low dscp 18 layer-2-cos 2
 class CONTROL_SIGNALING high dscp 18 layer-2-cos 2
 class CRITICAL_DATA low dscp 18 layer-2-cos 2
 class CRITICAL_DATA high dscp 18 layer-2-cos 2
 class INTERACTIVE_VIDEO low dscp 34 layer-2-cos 4
 class INTERACTIVE_VIDEO high dscp 34 layer-2-cos 4
!
qos-scheduler QOS_0
 class             Queue0
 bandwidth-percent 10
 buffer-percent    10
 scheduling        llq
!
qos-scheduler QOS_1
 class             Queue1
 bandwidth-percent 30
 buffer-percent    30
 drops             red-drop
!
qos-scheduler QOS_2
 class             Queue2
 bandwidth-percent 10
 buffer-percent    10
 drops             red-drop
!
qos-scheduler QOS_3
```

```
 class             Queue3
 bandwidth-percent 20
 buffer-percent    20
 drops             red-drop
!
qos-scheduler QOS_4
 class             Queue4
 bandwidth-percent 20
 buffer-percent    20
 drops             red-drop
!
qos-scheduler QOS_5
 class             Queue5
 bandwidth-percent 10
 buffer-percent    10
!
qos-map QOS
 qos-scheduler QOS_0
 qos-scheduler QOS_1
 qos-scheduler QOS_2
 qos-scheduler QOS_3
 qos-scheduler QOS_4
 qos-scheduler QOS_5
!
```

BR1-WE1

```
system
 host-name             br1-we1
 gps-location latitude 33.4484
 gps-location longitude -112.074
 device-groups         BRANCH ISR4K Primary UG5 US West
 system-ip             10.255.241.11
 overlay-id            1
 site-id               112001
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 console-baud-rate     9600
```

```
 vbond vbond-21615.cisco.net port 12346
!
banner login c c
banner motd c "This is a private network. It is for authorized use only." c
no service pad
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
no service tcp-small-servers
no service udp-small-servers
hostname br1-we1
!
vrf definition 1
 description Service VPN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Management VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
no ip dhcp use class
ip name-server 64.100.100.125 64.100.100.126
ip prefix-list Default-Route permit 0.0.0.0/0
ip route 0.0.0.0 0.0.0.0 10.101.2.2 1
ip route 0.0.0.0 0.0.0.0 192.168.101.1 1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.255.1 1
no ip rsvp signalling rate-limit
```

```
class-map match-any BULK
 match qos-group 2
!
class-map match-any CLASS_DEFAULT
 match qos-group 3
!
class-map match-any CONTROL_SIGNALING
 match qos-group 5
!
class-map match-any CRITICAL_DATA
 match qos-group 1
!
class-map match-any INTERACTIVE_VIDEO
 match qos-group 4
!
class-map match-any VOICE
 match qos-group 0
!
policy-map QOS
 class BULK
  random-detect
  bandwidth percent 10
 !
 class CLASS_DEFAULT
  random-detect
  bandwidth percent 20
 !
 class CONTROL_SIGNALING
  bandwidth percent 10
 !
 class CRITICAL_DATA
  random-detect
  bandwidth percent 30
 !
 class INTERACTIVE_VIDEO
  random-detect
  bandwidth percent 20
 !
 class VOICE
```

```
  priority percent 10
 !
!
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 192.168.255.143 255.255.254.0
 ip mtu 1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description Internet Interface
 no shutdown
 arp timeout 1200
 ip address 10.101.2.1 255.255.255.252
 ip mtu 1500
 mtu         1500
 negotiation auto
 service-policy output QOS
exit
interface GigabitEthernet0/0/1
 description LAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip mtu 1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/1.10
 no shutdown
 encapsulation dot1Q 10
 vrf forwarding 1
 ip address 10.101.10.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip mtu 1500
```

```
 vrrp 1 address-family ipv4
  vrrpv2
  address 10.101.10.1
  priority 200
  track 1 shutdown
 exit
exit
interface GigabitEthernet0/0/1.20
 no shutdown
 encapsulation dot1Q 20
 vrf forwarding 1
 ip address 10.101.20.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip mtu 1500
 vrrp 2 address-family ipv4
  vrrpv2
  address 10.101.20.1
  priority 200
  track 1 shutdown
 exit
exit
interface GigabitEthernet0/0/2
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 192.168.101.2 255.255.255.252
 ip mtu 1500
 mtu         1500
 negotiation auto
 service-policy output QOS
exit
interface GigabitEthernet0/1/0
 description TLOC Extension Interface
 no shutdown
 arp timeout 1200
 ip address 10.101.1.1 255.255.255.252
 ip mtu 1500
 mtu         1500
 negotiation auto
```

```
exit
interface GigabitEthernet0/1/1
 no shutdown
 no ip address
exit
interface Loopback0
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.255.241.11 255.255.255.255
 ip mtu 1500
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/2
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/2
 tunnel mode sdwan
exit
route-map DENY-ALL deny 10
!
route-map OSPF_WEDGE_PREFER permit 10
 set metric 0
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging host 10.4.48.13 vrf 1
```

```
no logging rate-limit
logging source-interface loopback0 vrf 1
logging persistent
aaa authentication login default local
aaa authorization exec default local
track 1 list boolean or
 object 2
!
track 2 ip route 0.0.0.0 0.0.0.0 reachability
 ip vrf 1
!
router bgp 65201
 bgp router-id        10.255.241.11
 bgp log-neighbor-changes
 distance bgp 20 200 20
 maximum-paths eibgp 2
 neighbor 192.168.101.1 remote-as 102
 neighbor 192.168.101.1 description MPLS BGP Service Provider
 neighbor 192.168.101.1 ebgp-multihop 1
 neighbor 192.168.101.1 maximum-prefix 2147483647 100
 neighbor 192.168.101.1 route-map DENY-ALL in
 address-family ipv4 unicast
  redistribute connected
  exit-address-family
 !
 timers bgp 60 180
!
no router rip
snmp-server community c1sco123 view isoALL RO
snmp-server enable traps
snmp-server host 10.4.48.13 vrf 1 version 2c c1sco123 udp-port 162
snmp-server location Branch 1
snmp-server view isoALL 1.3.6.1 included
!
ntp server time.nist.gov version 4
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec preference 100 weight 1
```

```
  color biz-internet
  no last-resort-circuit
  vmanage-connection-preference 5
  no allow-service all
  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
  allow-service https
 exit
 rewrite-rule QOS-REWRITE
exit
interface GigabitEthernet0/0/2
 tunnel-interface
  encapsulation ipsec preference 100 weight 1
  color mpls restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  no allow-service all
  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
  allow-service https
 exit
 rewrite-rule QOS-REWRITE
exit
interface GigabitEthernet0/1/0
 tloc-extension GigabitEthernet0/0/2
```

```
 exit
 omp
  no shutdown
  send-path-limit  16
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise connected
   advertise aggregate 10.101.0.0/16 aggregate-only
  !
 !
!
routing-policy defined-sets prefix-sets prefix-set Default-Route
 config prefix-set-name Default-Route
!
routing-policy policy-definitions policy-definition DENY-ALL
 config name DENY-ALL
!
routing-policy policy-definitions policy-definition OSPF_WEDGE_PREFER
 config name OSPF_WEDGE_PREFER
!
bfd app-route multiplier 6
bfd app-route poll-interval 120000
security
 ipsec
  rekey               86400
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac ah-no-id none
 !
policy
 app-visibility
 flow-visibility
 no implicit-acl-logging
```

```
 log-frequency        1000
 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
 !
```

BR2-WE1 (partial)

```
system
 host-name             br2-we1
 gps-location latitude 33.4484
 gps-location longitude -97.335
 device-groups         BRANCH ISR4K Primary UG4 US West
 system-ip             10.255.241.21
 overlay-id            1
 site-id               111002
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 console-baud-rate     9600
 vbond vbond-21615.cisco.net port 12346
!
```

```
no ip dhcp use class
ip name-server 64.100.100.125 64.100.100.126
ip prefix-list Default-Route permit 0.0.0.0/0
ip route 0.0.0.0 0.0.0.0 64.100.102.1 1
ip route 0.0.0.0 0.0.0.0 192.168.102.1 1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 192.168.255.1 1
no ip rsvp signalling rate-limit
class-map match-any BULK
 match qos-group 2
!
class-map match-any CLASS_DEFAULT
 match qos-group 3
!
class-map match-any CONTROL_SIGNALING
 match qos-group 5
!
class-map match-any CRITICAL_DATA
 match qos-group 1
!
class-map match-any INTERACTIVE_VIDEO
 match qos-group 4
!
class-map match-any VOICE
 match qos-group 0
!
policy-map QOS
 class BULK
  random-detect
  bandwidth percent 10
 !
 class CLASS_DEFAULT
  random-detect
  bandwidth percent 20
 !
 class CONTROL_SIGNALING
  bandwidth percent 10
 !
 class CRITICAL_DATA
  random-detect
```

```
  bandwidth percent 30
 !
 class INTERACTIVE_VIDEO
  random-detect
  bandwidth percent 20
 !
 class VOICE
  priority percent 10
 !
!
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 192.168.255.134 255.255.254.0
 ip mtu 1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description Internet Interface
 no shutdown
 arp timeout 1200
 ip address dhcp client-id GigabitEthernet0/0/0
 ip dhcp client default-router distance 1
 ip mtu 1500
 mtu         1500
 negotiation auto
 service-policy output QOS
exit
interface GigabitEthernet0/0/1
 description To Switch BR2-SW1
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.102.10.1 255.255.255.252
 ip helper-address 10.4.48.10
 ip mtu 1500
```

```
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/2
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 192.168.102.2 255.255.255.252
 ip mtu 1500
 mtu         1500
 negotiation auto
 service-policy output QOS
exit
interface Loopback0
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.255.241.21 255.255.255.255
 ip mtu 1500
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/2
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/2
 tunnel mode sdwan
exit
sdwan
```

```
interface GigabitEthernet0/0/0
 tunnel-interface
  encapsulation ipsec preference 0 weight 1
  color biz-internet
  no last-resort-circuit
  vmanage-connection-preference 5
  no allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
 exit
 rewrite-rule QOS-REWRITE
exit
interface GigabitEthernet0/0/2
 tunnel-interface
  encapsulation ipsec preference 0 weight 1
  color mpls restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  no allow-service all
  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
  allow-service https
 exit
 rewrite-rule QOS-REWRITE
```

```
 exit
 omp
  no shutdown
  send-path-limit  16
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise connected
   advertise aggregate 10.102.0.0/16 aggregate-only
  !
 !
routing-policy defined-sets prefix-sets prefix-set Default-Route
 config prefix-set-name Default-Route
!
policy
 app-visibility
 flow-visibility
 no implicit-acl-logging
 log-frequency        1000
 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
 !
```

BR3-WE1 (partial)

```
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 "LAN Parent Interface"
  mtu         1504
  no shutdown
 !
 interface ge0/2
  description          "MPLS Interface"
  ip address 192.168.103.2/30
  tunnel-interface
   encapsulation ipsec preference 0
   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
   allow-service https
  !
  clear-dont-fragment
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
```

```
  bandwidth-upstream   500000
  bandwidth-downstream 500000
 !
 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
   allow-service https
  !
  clear-dont-fragment
  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
 !
```

BR4-WE1 (partial)

```
ip route 0.0.0.0 0.0.0.0 10.104.2.2 1
ip route 0.0.0.0 0.0.0.0 192.168.104.1 1
!
interface GigabitEthernet0/0/0
 description WAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip mtu 1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/0.101
 no shutdown
 encapsulation dot1Q 101
 ip address 10.104.1.1 255.255.255.252
 ip mtu 1500
exit
interface GigabitEthernet0/0/0.102
 no shutdown
 encapsulation dot1Q 102
 ip address 10.104.2.1 255.255.255.252
 ip mtu 1500
exit
interface GigabitEthernet0/0/1
 description To LAN-SW
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.104.0.2 255.255.255.252
 ip helper-address 10.4.48.10
 ip mtu 1500
 ip ospf 1 area 0
 ip ospf authentication message-digest
 ip ospf network point-to-point
 ip ospf message-digest-key 22 md5 0 cisco123
 mtu         1500
 negotiation auto
```

```
exit
interface GigabitEthernet0/0/2
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 192.168.104.2 255.255.255.252
 ip mtu 1500
 mtu         1500
 negotiation auto
 service-policy output QOS
exit
interface Loopback0
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.255.242.41 255.255.255.255
 ip mtu 1500
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/2
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/2
 tunnel mode sdwan
exit
interface Tunnel102000
 no shutdown
 ip unnumbered GigabitEthernet0/0/0.102
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0.102
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0.102
 tunnel mode sdwan
exit
route-map DENY-ALL deny 10
!
route-map OSPF_WEDGE_PREFER permit 10
```

```
 set metric 10
!
router bgp 65204
 bgp router-id        10.255.242.41
 bgp log-neighbor-changes
 distance bgp 20 200 20
 maximum-paths eibgp 2
 neighbor 192.168.104.1 remote-as 102
 neighbor 192.168.104.1 description MPLS BGP Service Provider
 neighbor 192.168.104.1 ebgp-multihop 1
 neighbor 192.168.104.1 maximum-prefix 2147483647 100
 neighbor 192.168.104.1 route-map DENY-ALL in
 address-family ipv4 unicast
  redistribute connected
  exit-address-family
 !
 timers bgp 60 180
!
router ospf 1 vrf 1
 auto-cost reference-bandwidth 100000
 max-metric router-lsa
 timers throttle spf 200 1000 10000
 router-id 10.255.242.41
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets route-map OSPF_WEDGE_PREFER
!
sdwan
 interface GigabitEthernet0/0/0.101
  tloc-extension GigabitEthernet0/0/2
 exit
 interface GigabitEthernet0/0/0.102
  tunnel-interface
   encapsulation ipsec preference 100 weight 1
   color biz-internet
   no last-resort-circuit
   vmanage-connection-preference 5
```

```
  no allow-service all
  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
  allow-service https
 exit
exit
interface GigabitEthernet0/0/2
 tunnel-interface
  encapsulation ipsec preference 100 weight 1
  color mpls restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  no allow-service all
  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
  allow-service https
 exit
 rewrite-rule QOS-REWRITE
exit
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
 timers
```

```
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise connected
   advertise aggregate 10.104.0.0/16 aggregate-only
  !
```

BR4-WE2 (partial)

```
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          "Internet Interface"
  ip address 64.100.104.2/28
  nat
  !
  tunnel-interface
   encapsulation ipsec preference 0
   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
   allow-service https
  !
  clear-dont-fragment
  no shutdown
  qos-map              QOS
  rewrite-rule QOS-REWRITE
```

```
 bandwidth-upstream   500000
 bandwidth-downstream 500000
!
interface ge0/2
 description "WAN Parent Interface"
 mtu         1504
 no shutdown
!
interface ge0/2.101
 description          "MPLS Interface"
 ip address 10.104.1.2/30
 tunnel-interface
  encapsulation ipsec preference 0
  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
  allow-service https
 !
 clear-dont-fragment
 no shutdown
 bandwidth-upstream   500000
 bandwidth-downstream 500000
!
interface ge0/2.102
 description    "TLOC Extension Interface"
 ip address 10.104.2.2/30
 tloc-extension ge0/0
 no shutdown
!
ip route 0.0.0.0/0 10.104.1.1
ip route 0.0.0.0/0 64.100.104.1
!
```

```
vpn 1
 name "Service VPN"
 ecmp-hash-key layer4
 router
  ospf
   router-id 10.255.242.42
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp route-policy OSPF_WEDGE_PREFER
   area 0
    interface ge0/4
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5
$8$8XW8DMhTKnu8yxFoHXIcpUNXsPSlao6kJb7WGDFbFoU=
    exit
    range 10.104.0.0/16
   exit
  !
interface ge0/4
  description "To LAN-SW"
  ip address 10.104.0.6/30
  dhcp-helper 10.4.48.10
  no shutdown
 !
 interface loopback0
  ip address 10.255.242.42/32
  no shutdown
 !
 omp
  advertise connected
  advertise aggregate 10.104.0.0/16 aggregate-only
 !
!
vpn 512
 name "Management VPN"
 interface mgmt0
```

```
  description "Management Interface"
  ip address 192.168.255.162/23
  no shutdown
 !
 ip route 0.0.0.0/0 192.168.255.1
!
```

BR5-WE1 (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 connected
  advertise aggregate 10.105.0.0/16 aggregate-only
 !
```

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
   dscp             16
   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 drop
 !
!
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 ftp-data
 app ftp_data
 app ftps
 app imap
 app imap-secure
 app imaps
 app live_hotmail
 app livemail_mobile
 app lotus-notes
 app lotusnotes
 app outlook-web-service
 app owa
 app pop3
 app pop3s
 app secure-ftp
 app secure-pop3
 app secure-smtp
 app smtp
 app smtps
 app tftp
!
app-list APPS_NETWORK_CONTROL
 app ntp
 app radius
 app ssh
 app sshell
 app tacacs
```

```
 app tacacs_plus
 app telnet
!
app-list APPS_SCAVENGER
 app apple-updates
 app apple_update
 app facebook
 app facebook_live
 app facebook_mail
 app facebook_messenger
 app fbcdn
 app google-play
 app instagram
 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 route
    site-list Low_BW_US_Sites
   !
   action reject
   !
  !
  sequence 11
   match tloc
    site-list Low_BW_US_Sites
   !
   action reject
   !
  !
  default-action accept
 !
 control-policy control_-1988590079
  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_-1988590079 out
!
site-list Low_BW_West_Branches
 control-policy control_-1988590079 out
!
```

About this guide

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2019 Cisco Systems, Inc. All rights reserved.

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.