思科软件定义广域网端到端部署指南

18.3.5/16.9.4 版

2020 年 4 月

目录

简介

思科® SD-WAN 解决方案是企业级重叠广域网架构，可推动企业实现全数字化转型，并过渡到云。该解决方案可以在大规模网络中完全集成路由、安全、集中策略和协调功能，具有多租户、云交付、高度自动化、安全、可扩展、应用感知和丰富的分析等特点。思科 SD-WAN 技术解决了常见广域网部署的各种问题和挑战。

本指南介绍思科软件定义广域网网络实施，展示组织常用的一些部署模式和功能。本指南并不会详尽地介绍所有部署选项，而只重点介绍最佳实践，并帮助成功配置和部署思科 SD-WAN 网络。

示例 SD-WAN 网络包含一个数据中心（具有两台思科 vEdge 5000 路由器）和五个远程站点（混合使用运行 SD-WAN 软件映像的思科 vEdge 1000 路由器、思科 vEdge 100 路由器以及思科 ISR 4351 和 4331 路由器）。利用我们所介绍的数据中心现有环境部署，可以在从广域网向软件定义广域网迁移期间，通过数据中心连接至非软件定义广域网站点。本指南将介绍远程站点新环境部署，但是其中的配置概念也适用于现有环境部署。

注意：运行 SD-WAN 软件映像的思科 ISR 4000 和 1000 路由器以及思科 ASR 1000 路由器也称为 IOS XE SD-WAN 路由器。思科 IOS XE SD-WAN 路由器与思科 vEdge 路由器一起，统称为思科广域网边缘路由器。

开始部署的必备条件:

- 已安装思科广域网边缘路由器，并且这些路由器随时可进行配置。IOS XE SD-WAN 路由器应该已从 IOS XE 转换为 SD-WAN 代码。有关转换的信息，请参阅附录 B。
- 已配置与思科广域网边缘路由器邻接的设备。
- 已使用思科云托管服务设置并部署 SD-WAN 控制器。
- 理解思科 SD-WAN 解决方案及其相关概念，但无需具备部署经验。有关 SD-WAN 解决方案的背景信息，请参阅《软件定义广域网设计指南》，网址为：https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf。

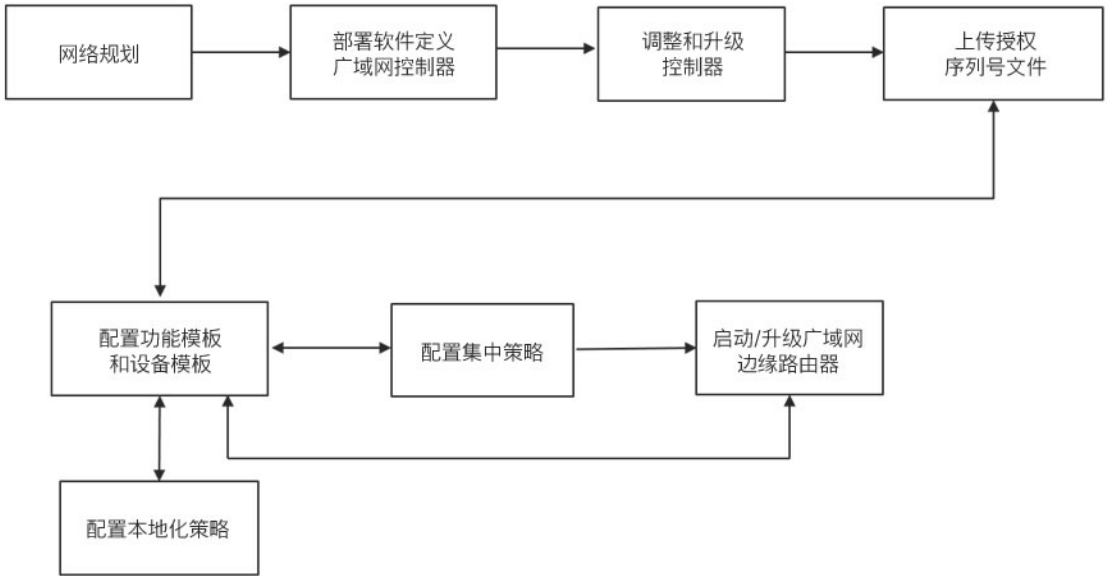
有关本部署指南中使用的硬件型号和软件版本，请参阅附录 A。有关部分配套的网络设备配置，请参阅附录 F。有关 vEdge 设备的配置摘要，请参阅附录 G 和 H。

有关其他文档（包括面向 SaaS 的 Cloud onRamp 部署指南），请参阅 http://www.cisco.com/go/cvd 上的设计区。

SD-WAN 部署概述

为了获得功能完备的 SD-WAN 重叠，需要执行一系列步骤。下图展示的是一个工作流程示例。

图 1　部署流程图



1. 网络规划 - 规划设备布局、系统 IP 地址和站点 ID；规划广域网边缘设备配置、策略和代码版本；规划配套的设备配置，包括为满足广域网边缘通信需求而必须开放的任何防火墙端口。制定详细的迁移计划。

2. 部署软件定义广域网控制器 - 应部署 vManage、vSmart 控制器和 vBond 协调器；应安装证书；并且这些控制器应相互执行身份验证。

3. 调整并升级控制器 - 可以验证软件定义广域网控制器状态，并根据常用最佳实践配置适当进行调整。必要时，可以升级这些控制器。

4. 上传授权序列号文件 - 授权序列号文件包含所有经授权可以进入网络的广域网边缘路由器的序列号和机箱编号，应上传到 vManage 中。该文件上传到 vManage 中或完成同步后，将分发给 vBond 和 vSmart 控制器。请注意，可以上传多个授权序列号文件，重复的设备条目会被忽略。

5. 配置功能模板和设备模板 - 配置功能模板和设备模板，并将这些模板与广域网边缘设备关联，必要时为参数值创建变量。vManage 会构建完整配置并将其推送到广域网边缘设备。建议在部署分支机构之前，先部署数据中心。

6. 配置本地化策略 - 配置本地化策略，并将该策略与目标设备模板关联。请注意，如果设备模板已与广域网边缘设备关联，则需要首先关联本地化策略，再在功能模板中执行任何策略引用。

7. 配置集中策略 - 使用 vManage 配置所有集中策略，这些策略将下载到网络中的 vSmart 控制器上。

8. 启动/升级广域网边缘路由器 - 启动广域网边缘路由器，以与 vBond、vSmart 和 vManage 设备建立控制连接。此操作可以通过手动引导配置或自动调配过程完成。自动调配包括适用于 vEdge 路由器的非接触调配 (ZTP) 流程，或适用于 IOS XE SD-WAN 路由器的思科网络即插即用 (PnP) 流程。此外，请根据需要升级广域网边缘路由器，可以通过 vManage GUI 手动执行，也可以在自动调配过程中自动执行。

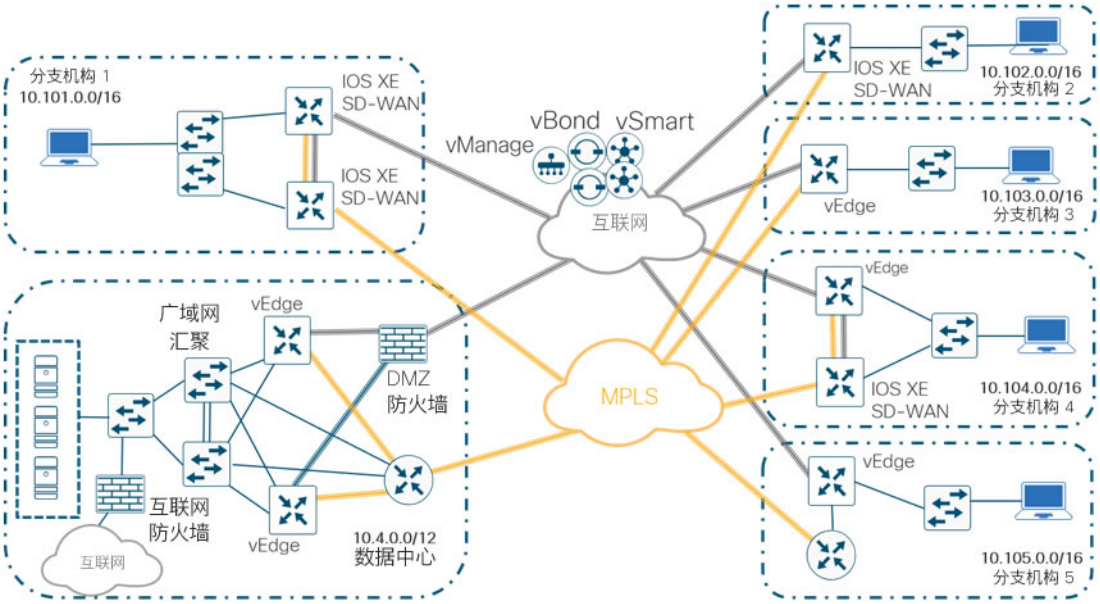
请注意，上述步骤的顺序可灵活调整，但以下几点例外:

- 网络规划和 SD-WAN 控制器部署应首先执行。
- 计划升级到新代码版本时，应首先升级 vManage 设备，然后升级 vBond 和 vSmart 控制器，再升级广域网边缘路由器。
- 需要先上传授权序列号文件，然后才能成功使任何广域网边缘路由器上线。
- 必须在 vManage GUI 中将设备模板与广域网边缘路由器关联，才能通过 ZTP 或 PnP 流程成功使这些路由器上线。
- 本地化策略需与设备模板关联。如果设备模板已与 vEdge 设备关联，则必须先关联本地化策略，然后才可以在设备模板内引用任何策略组件（路由器策略、前缀列表等）。

部署示例

下图是本部署指南中所述示例网络拓扑的简要概况。

图 2　软件定义广域网网络示例



在此拓扑中，有一个数据中心和五个远程站点。图中所示的传输链路为一个 MPLS 和一个互联网运营商。SD-WAN 控制器已使用思科的云托管服务进行部署，并且可以通过互联网传输链路访问。其中一台 vManage、一台 vSmart 控制器和一台 vBond 协调器部署于美国西海岸，一台 vSmart 控制器和一台 vBond 协调器部署于美国东海岸。

每台广域网边缘路由器都会尝试通过每条传输链路与控制器建立连接。vEdge 路由器将首先通过每个传输链路连接 vBond，然后连接两台 vSmart 控制器。从该站点只会建立一个 vManage 连接，具体取决于首先与之连接的是哪个传输链路，但这个首选项是可以配置的。广域网边缘路由器通过互联网传输链路直接连接控制器。广域网边缘路由器通过 IPSec 隧道路由至数据中心，然后沿着互联网防火墙的默认路由到达互联网传输链路，从而通过 MPLS 传输链路连接控制器。

数据中心详细信息

在示例 SD-WAN 网络中，主数据中心中内布置了两台思科 vEdge 5000 路由器（标有 DC1-WE1 和 DC1-WE2）（见图 3）。

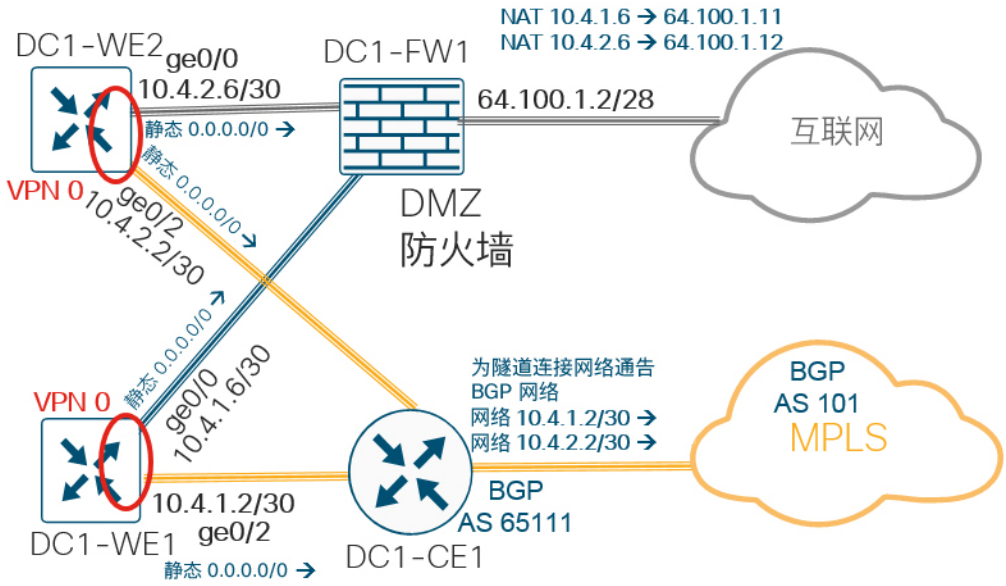
传输端

传输端 VPN（即 VPN 0）包含每台 vEdge 路由器上用于互联网传输链路的接口 ge0/0 和用于 MPLS 传输链路的 ge0/2。

每台 vEdge 路由器的接口 ge0/0 均连接到一台 DMZ 交换机，该交换机使用 DMZ 接口连接到一台思科自适应安全设备 (ASA) 5500（标有 DC1-FW1）。每台 vEdge 路由器的面向互联网的接口将分配到一个 IP 地址，该地址需要能够在互联网中路由，因为它将用作基于互联网的 VPN 隧道连接的终端。为此，可以直接向 vEdge 路由器分配一个可路由的地址；也可以直接向 vEdge 路由器分配一个不可路由的 RFC-1918 地址，并在 ASA 5500 上采用网络地址转换 (NAT)，将此专用 IP 地址转换为可路由的 IP 地址。此设计假设在思科 ASA 5500 上为每个 vEdge 互联网隧道终端地址配置一个静态 NAT。这相当于完全圆锥型 NAT 或一对一 NAT，可以将内部地址/端口对映射为外部地址/端口对，并且允许外部主机向网络内部发起流量。建议数据中心或控制中心站点使用一对一 NAT，以防与其他 vEdge 路由器连接时出现问题。vEdge 路由器将在 VPN 0 中使用静态默认路由将隧道终端路由至互联网传输链路。

每台 vEdge 路由器上的接口 ge0/2 均连接至客户边缘 (CE) 路由器（标有 DC1-CE1），CE 路由器则连接至运营商的 MPLS 运营商边缘 (PE) 路由器并通过外部边界网关协议 (eBGP) 连接与其建立对等关系。通过将经由 BGP 连接至 vEdge 路由器的子网通告给运营商云，为 vEdge MPLS 隧道终端分配的专用地址将从 CE 路由器进行通告，使位于 MPLS 传输链路上的其他广域网边缘路由器可以访问该隧道终端。vEdge 将在 VPN 0 中使用静态默认路由将隧道终端路由至 MPLS 传输链路。

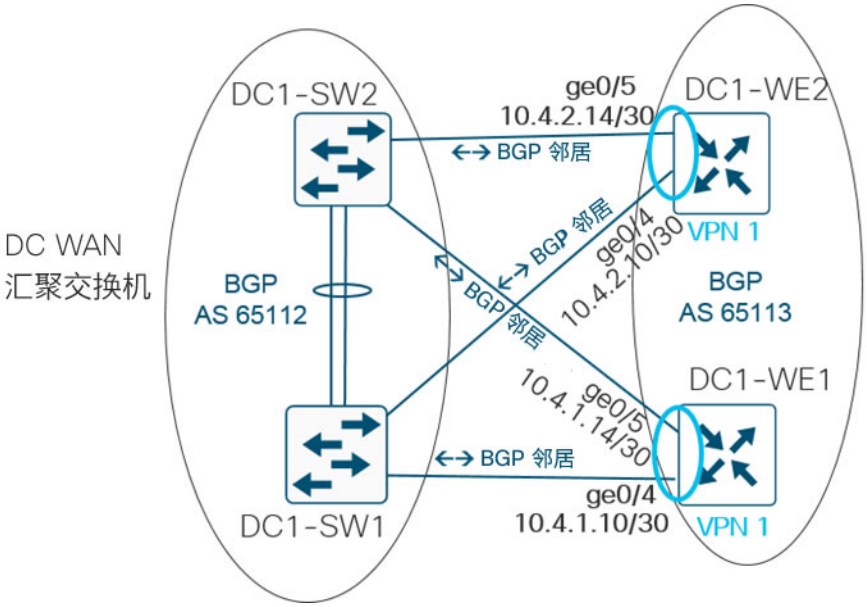
图 3　数据中心网络传输端



服务端

服务端 VPN（即 VPN 1）包含接口 ge0/4 和 ge0/5，用于连接至广域网汇聚交换机。每台 vEdge 的接口 ge0/4 均连接到网络中的数据中心广域网汇聚交换机 1（标有 DC1-SW1），而接口 ge0/5 连接到数据中心广域网汇聚交换机 2（标有 DC1-SW2）。每台 vEdge 均使用接口地址通过 eBGP 与每台交换机建立对等连接，所以这些交换机使用 BGP next-hop-self 确保从每台 vEdge 均可到达所有路由的下一跳。

图 4　数据中心网络服务端



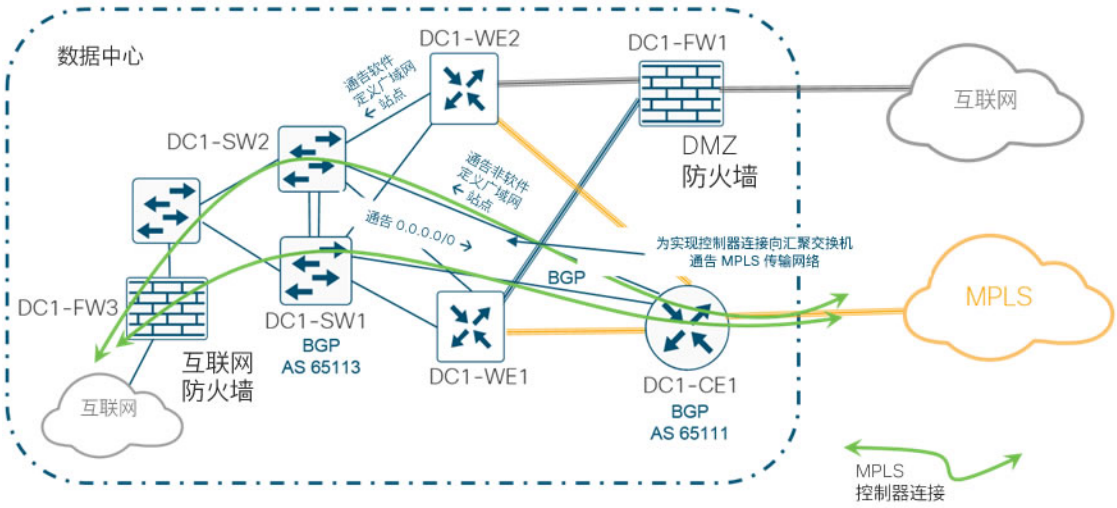
数据中心边缘 IP 地址

主机名	ge0/0 互联网	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 路由

数据中心的 CE 路由器通过 eBGP 与广域网汇聚交换机建立对等连接。CE 通告非软件定义广域网站点网络，而 vEdge 路由器通告软件定义广域网站点网络。对于 MPLS 控制器连接，汇聚交换机向 CE 路由器通告默认路由，因此来自 MPLS 传输链路的控制连接可沿着该路由到达互联网防火墙以连接控制器。此互联网防火墙 DC1-FW3 配置为使用地址池执行动态 NAT，因此与控制器的广域网边缘控制连接以可路由的互联网地址作为源。CE 还必须将 MPLS 隧道终端（包括传输位置 [TLOC] 扩展子网）通告给汇聚交换机，使来自互联网传输链路的控制器可以访问位于 MPLS 传输链路的 vEdge 路由器。

图 5　数据中心路由



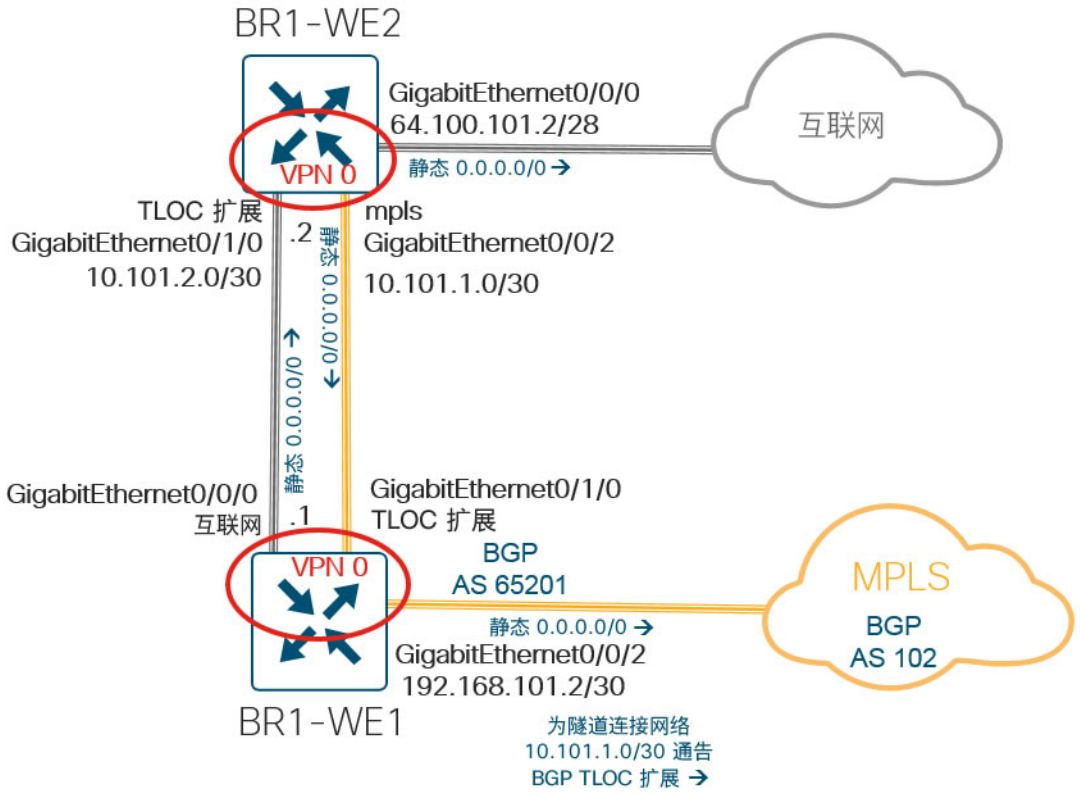
分支机构详细信息

分支机构 1：双路由器/TLOC 扩展/第 2 层中继局域网交换机/VRRP 站点

传输端

分支机构 1 包含两台 ISR 4351 IOS XE SD-WAN 路由器，每台路由器都与传输链路运营商直连。此站点在路由器之间配置了 TLOC 扩展链路，使每台路由器都可以访问这两条传输链路。广域网边缘 1（标有 BR1-WE1）在传输端 VPN 中运行 BGP，以将 TLOC 扩展链路子网通告给 MPLS 云，因此广域网边缘 2（标有 BR1-WE2）可以通过数据中心访问控制器和 MPLS 传输链路上的其他广域网边缘路由器，从而建立 IPSec 隧道。这两台路由器上都配置了指向下一跳网关的静态默认路由，用于在两台广域网边缘路由器上的 MPLS (GigabitEthernet0/0/2) 和互联网 (GigabitEthernet0/0/0) 链路上建立隧道。TLOC 扩展接口无需执行任何特殊的路由配置，因为它用于将隧道和控制流量路由至下一跳，而下一跳是直连的。

图 6　分支机构 1 传输端

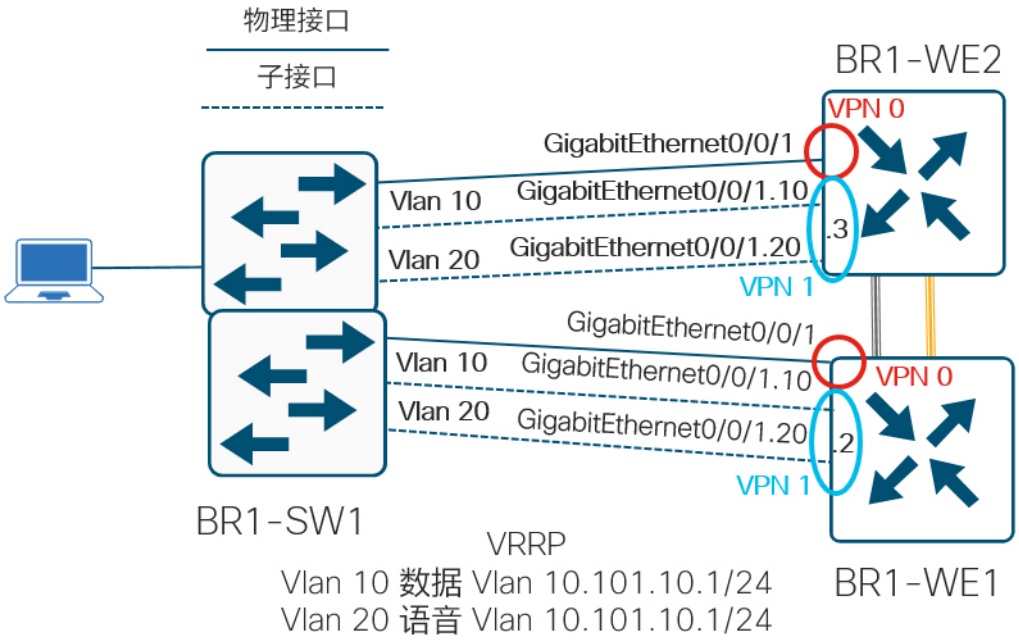


服务端

每台广域网边缘路由器均通过中继接口连接至局域网交换机堆叠（标有 BR1-SW1）。每台广域网边缘路由器上只有一条链路连接到堆叠中的单个局域网交换机。这样可以简化设计，因为目前不支持通道或生成树，而且如果您配置从每台广域网边缘路由器通往每台局域网交换机的链路，就需要配置集成路由和桥接 (IRB)，从而增加复杂性。

每条中继链路分别配置两个 VLAN：VLAN 10（数据）和 VLAN 20（语音），在每台广域网边缘路由器上，这两个 VLAN 转换为两个不同的子接口。物理链路 GigabitEthernet0/0/1 配置在 VPN 0 中，而每个子接口都是服务端 VPN（即 VPN 1）的一部分。利用虚拟路由器冗余协议 (VRRP)，广域网边缘路由器将成为分支机构中主机的 IP 网关。在每个子接口上，使用 .1 主机地址分别为 10.101.10.0/24 和 10.101.20.0/24 这两个子网配置 VRRP。

图 7　分支机构 1 服务端



分支机构 1 边缘 IP 地址

主机名	Gigabit Ethernet0/0/0 互联网	Gigabit Ethernet0/0/2 MPLS	Gigabit Ethernet0/1/0 TLOC 扩展	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

分支机构 2：单路由器/互联网 DHCP 地址/第 2 层局域网交换机站点

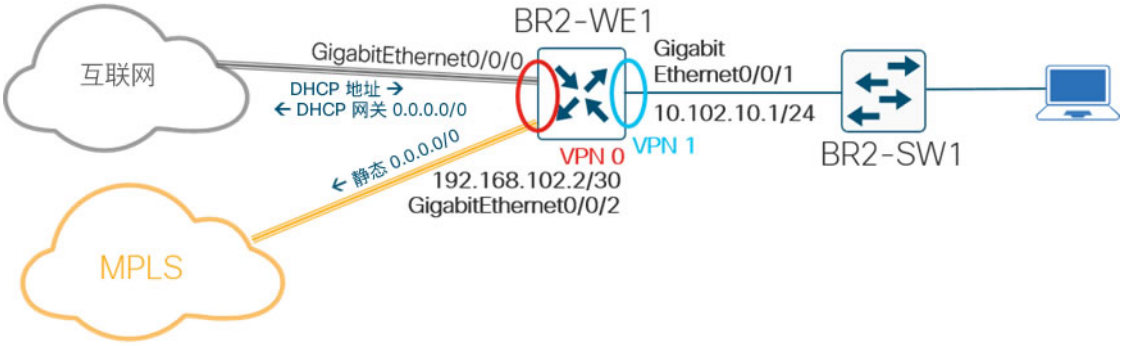
传输端

分支机构 2 包含一台思科 4331 IOS XE SD-WAN 路由器（标有 BR2-WE1），该路由器同时连接到 MPLS 传输链路和互联网传输链路。互联网传输接口 (GigabitEthernet0/0/0) 配置为使用动态主机配置协议 (DHCP) 以动态获取 IP 和网关地址。配置一条指向下一跳网关的静态默认路由，用于在 MPLS 传输链路 (GigabitEthernet0/0/2) 上建立隧道。

服务端

分支机构 2 的广域网边缘路由器使用 GigabitEthernet0/0/1 连接到第 2 层交换机（标有 BR2-SW1）。

图 8　分支机构 2 传输端和服务端



分支机构 2 边缘 IP 地址

主机名	GigabitEthernet0/0/0 互联网	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

分支机构 3：单路由器/第 2 层中继局域网交换机站点

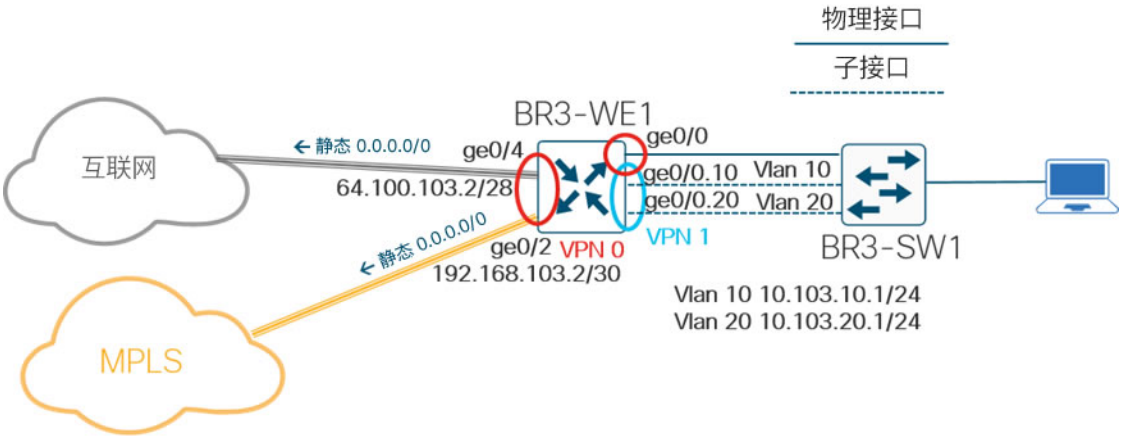
传输端

分支机构 3 包含一台 vEdge 100b 路由器（标有 BR3-WE1），该路由器同时连接到 MPLS 传输链路和互联网传输链路。配置一条指向下一跳网关的静态默认路由，用于在互联网 (ge0/4) 和 MPLS (ge0/2) 传输链路上建立隧道。

服务端

分支机构 3 的 vEdge 路由器中继到第 2 层交换机（标有 BR3-SW1）。该中继链路配置两个 VLAN：vlan 10（数据）和 vlan 20（语音），在 vEdge 路由器端这两个 VLAN 转换为两个不同的子接口。物理链路 ge0/0 配置在 VPN 0 中，而每个子接口都是服务端 VPN（即 VPN 1）的一部分。

图 9　分支机构 3 传输端和服务端



分支机构 3 边缘 IP 地址

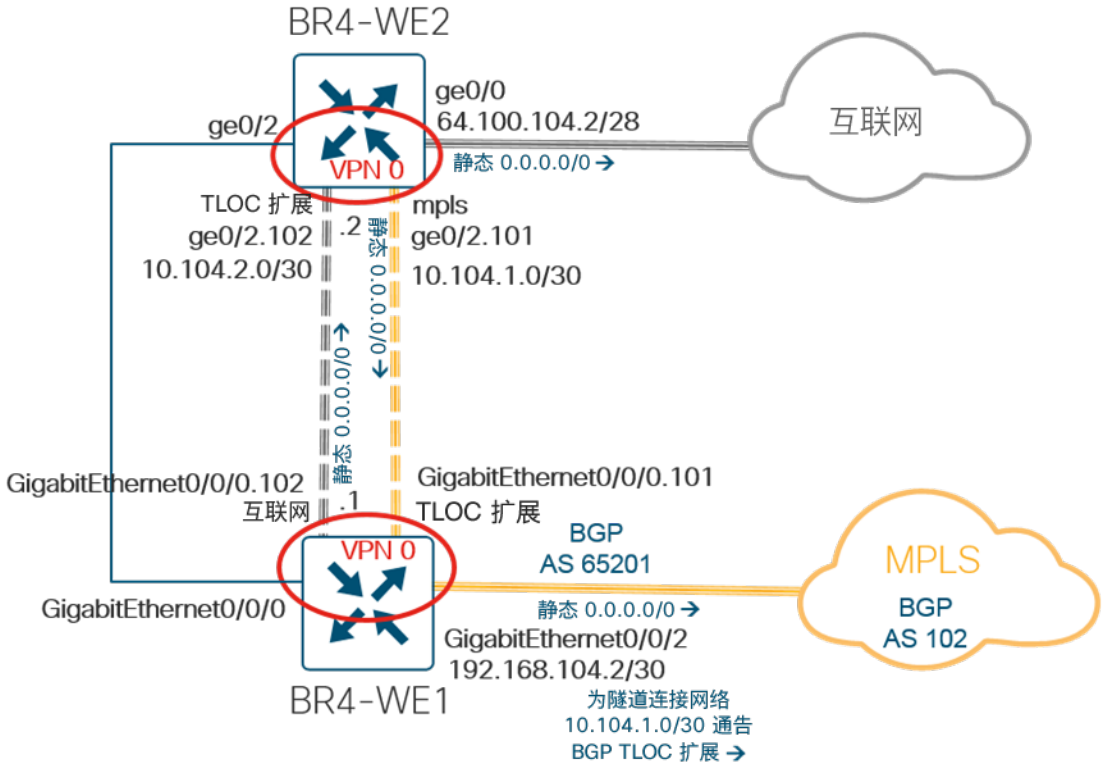
主机名	ge0/4 互联网	ge0/2 MPLS	ge0/0 BR3-SW1 VLAN 10	ge0/0 BR3-SW1 VLAN 20
BR3-WE1	64.100.103.2/28	192.168.103.2/30	10.103.10.1/24	10.103.20.1/24

分支机构 4：子接口 TLOC 扩展/第 3 层 OSPF 路由站点

传输端

分支机构 4 包含一台与互联网运营商直连的思科 vEdge 1000 路由器，以及一台与 MPLS 运营商直连的思科 ISR4351 IOS XE SD-WAN 路由器。此站点在两台广域网边缘路由器之间配置了一条 TLOC 扩展链路，使每台广域网边缘路由器都可以访问这两条传输链路。TLOC 扩展链路利用多个子接口。IOS XE SD-WAN 路由器（标有 BR4-WE1）在传输端 VPN 中运行 BGP，以将 TLOC 扩展链路子网通告给 MPLS 云，因此 vEdge 路由器（标有 BR4-WE2）可以通过数据中心访问控制器和 MPLS 传输链路上的其他广域网边缘路由器，从而建立 IPSec 隧道。这两台广域网边缘路由器上都配置了指向下一跳网关的静态默认路由，用于在 MPLS 和互联网链路上建立隧道。TLOC 扩展子接口无需执行任何特殊的路由配置，因为它用于将隧道和控制流量路由至下一跳，而下一跳是直连的。广域网边缘 1 和广域网边缘 2 上的物理链路以及子接口都配置在 VPN 0 中。

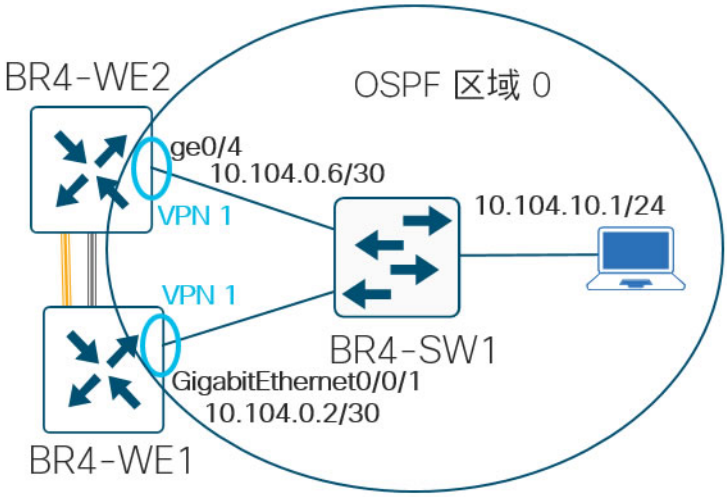
图 10　分支机构 4 传输端



服务端

分支机构 4 有两台广域网边缘路由器连接到第 3 层交换机（标有 BR4-SW1），并且它们之间运行开放最短路径优先 (OSPF) 协议。所有设备都位于区域 0 中。路由器的接口配置为在每个接口上都与第 3 层交换机建立 OSPF 网络点对点连接。

图 11　分支机构 4 服务端



分支机构 4 边缘 1 IP 地址

主机名	Gigabit Ethernet0/0/0.102 互联网	Gigabit Ethernet0/0/2 MPLS	Gigabit Ethernet0/0/0.101 TLOC 扩展	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

分支机构 4 边缘 2 IP 地址

主机名	ge0/0 互联网	ge0/2.101 MPLS	ge0/2.102 TLOC 扩展	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

分支机构 5：CE 路由器/第 3 层交换机/静态局域网路由站点

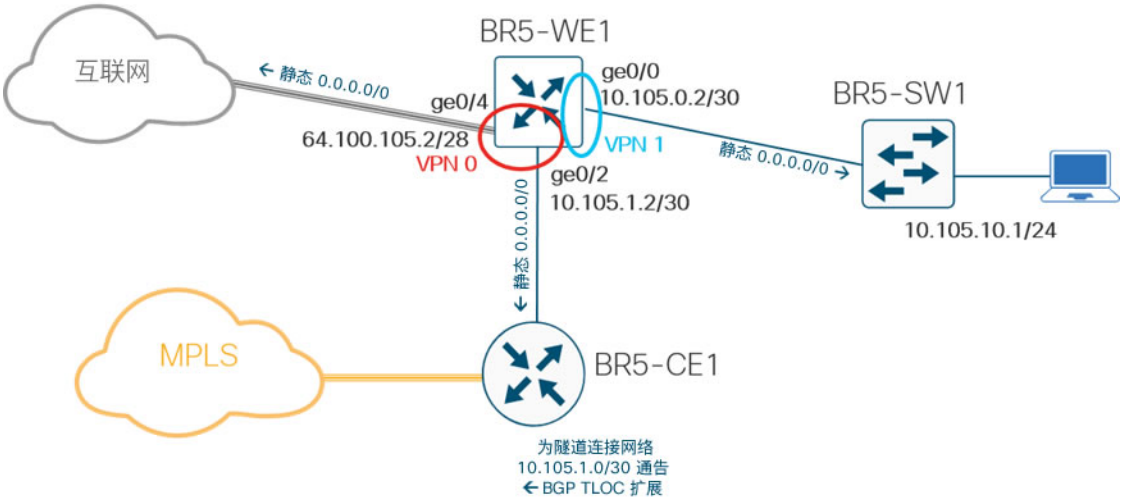
传输端

分支机构 5 有一台 vEdge 100b（标有 BR5-WE1）与互联网传输链路直连，此外还连接了一台 CE 路由器（标有 BR5-CE1），而该 CE 路由器则与 MPLS 传输链路连接。配置一条指向下一跳网关的静态默认路由，用于在互联网 (ge0/4) 和 MPLS (ge0/2) 传输链路上建立隧道。CE 路由器上配置的 BGP 通告 vEdge MPLS 子网，因此 vEdge 路由器可以访问 MPLS 传输链路上的其他广域网边缘路由器并且可以通过数据中心连接控制器。

服务端

位于分支机构 5 的 vEdge 路由器连接到第 3 层交换机（标有 BR5-SW1），并且局域网交换机和 vEdge 路由器之间配置了静态路由。

图 12　分支机构 5 传输端和服务端



分支机构 5 边缘 IP 地址

主机名	ge0/4 互联网	ge0/2 MPLS	ge0/0 BR5-SW1
BR5-WE1	64.100.105.2/28	10.105.1.2/30	10.105.0.2/30

其他详情

端口编号

下表是本部署指南选择的端口编号方案。“互联网” 列显示了各个 vEdge 型号上的 ZTP 端口。PnP 并不限定于 IOS XE SD-WAN 路由器上的特定端口。

端口编号方案

广域网边缘路由器型号	互联网	MPLS	局域网	TLOC 扩展
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	--

系统 IP 地址和站点 ID

在此示例网络中，10.255.240.0/12 范围内的系统 IP 地址特定于北美，第三个八位组代表地区（美国西部或东部），第四个八位组代表分支机构编号。

此示例网络的站点 ID 类似于《软件定义广域网设计指南 》中指定的方案，但使用的是六位数而不是九位数。分支机构的编号嵌入站点类型数位中，而没有额外使用三位数进行标识。

六位数的站点 ID 示例

主机名	GigabitEthernet0/0/0 互联网	GigabitEthernet0/0/2 MPLS
1	国家/地区/大洲	1 = 北美，2 = 欧洲，3 = 亚太地区
2	地区	1 = 美国西部，2 = 美国东部，3 = 加拿大西部，4 = 加拿大东部
3-6	站点类型	0000-0099 = 控制中心位置，1000-1999 = 类型 1 站点，2000-2999 = 类型 2 站点，3000-3999 = 类型 3 站点，4000-4999 = 类型 4 站点，5000-9999 = 供将来使用

示例网络站点类型说明

站点类型	说明
站点类型 1 (1000-1999)	低带宽网站点，其中没有全网状流量。流量必须经过控制中心（分支机构 2 和 5）
站点类型 2 (2000-2999)	此类站点为访客提供直接互联网接入 (DIA)（分支机构 1 和 4）（本指南中未实施）
站点类型 3 (3000-3999)	此类站点要求在 MPLS 上传输语音流量，而所有其他流量则使用互联网传输链路（分支机构 3）（本指南中未实施）
站点类型 4 (4000-4999)	此类站点要求企业流量使用中心防火墙来与其他站点直接通信（本指南中未实施）

下表总结了此示例网络的站点 ID 和系统 IP 地址。

示例网络站点 ID 和系统 IP 地址

主机名	位置	站点 ID	系统 IP
DC1-WE1	数据中心 1/西部	110001	10.255.241.101
DC1-WE2	数据中心 1/西部	110001	10.255.241.102
BR1-WE1	分支机构 1/西部	112001	10.255.241.11
BR1-WE2	分支机构 1/西部	112001	10.255.241.12
BR2-WE1	分支机构 2/西部	111002	10.255.241.21
BR3-WE1	分支机构 3/西部	113003	10.255.241.31
BR4-WE1	分支机构 4/东部	122004	10.255.242.41

主机名	位置	站点 ID	系统 IP
BR4-WE2	分支机构 4/东部	122004	10.255.242.42
BR5-WE1	分支机构 5/东部	121005	10.255.242.51

颜色

在示例网络中，MPLS 颜色用于 MPLS 传输链路。MPLS 控制流量使用 NAT 通过数据中心到达互联网中的控制器，但由于 MPLS 是专用颜色，因此 vEdge 路由器使用专用地址（或 NAT 转换前地址）通过 MPLS 传输链路建立隧道。

企业互联网是公共颜色，用于互联网传输链路，这意味着如果有 NAT 转换后地址可用，则 vEdge 路由器将使用 NAT 转换后地址通过互联网传输链路与其他 vEdge 路由器建立隧道。

其他设计参数

本部署指南使用某些标准设计参数，并且引用不在广域网中的各种网络基础设施服务。这些参数在下表中列出。

通用设计参数

主机名	位置
网络服务	IP 地址
域名	cisco.local
Active Directory、DHCP 服务器	10.4.48.10
DNS 服务器	10.4.48.10（内部）、64.100.100.125、64.100.100.126
日志记录、SNMP 服务器	10.4.48.13
思科身份服务引擎 (ISE)	10.4.48.15
网络时间协议 (NTP) 服务器	10.4.48.17（内部）、time.nist.gov

部署详细信息

技术提示：此部分中程序提供的示例适用于大多数设置。您使用的实际设置和值取决于您的当前网络配置。

部署详细信息包括以下内容：

- 调整控制器配置 – 这包括验证控制器是否已启动，并按照最佳实践修改其配置。此外，还包括上传授权序列号文件。
- 准备软件升级并升级控制器。
- 部署数据中心广域网边缘路由器 – 这包括启动广域网边缘路由器以使其连接到控制器，升级代码，配置设备模板和功能模板，以及部署本地化策略。
- 部署远程站点广域网边缘路由器 – 这包括采用 ZTP 和 PnP 流程将广域网边缘路由器连接到控制器，升级代码，配置设备模板和功能模板，以及部署本地化策略。
- 部署本地化策略。
- 部署应用感知路由策略。
- 配置流量对称。
- 部署服务质量 (QoS)。

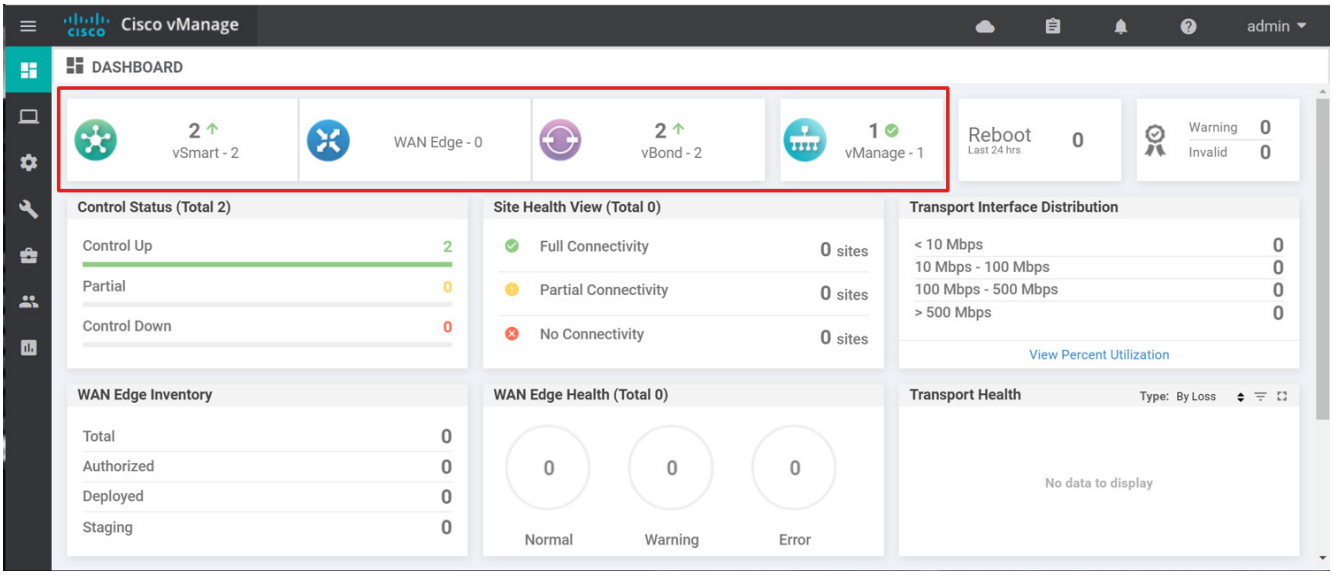
调整控制器配置

在此部署中，控制器包括一台 vManage、两台 vSmart 控制器和两台 vBond 协调器。vManage 和 vBond 协调器处于命令行界面 (CLI) 模式下，而 vSmart 控制器使用基于 CLI 的模板处于 vManage 模式下。vManage 和 vBond 协调器的配置可以直接使用 CLI 进行修改，而 vSmart 控制器必须使用 vManage 进行配置。

下一节介绍如何查看控制器可访问性，如何修改控制器配置，以及如何上传 vEdge 序列号文件。

程序 1：验证控制器是否已启动并准备就绪

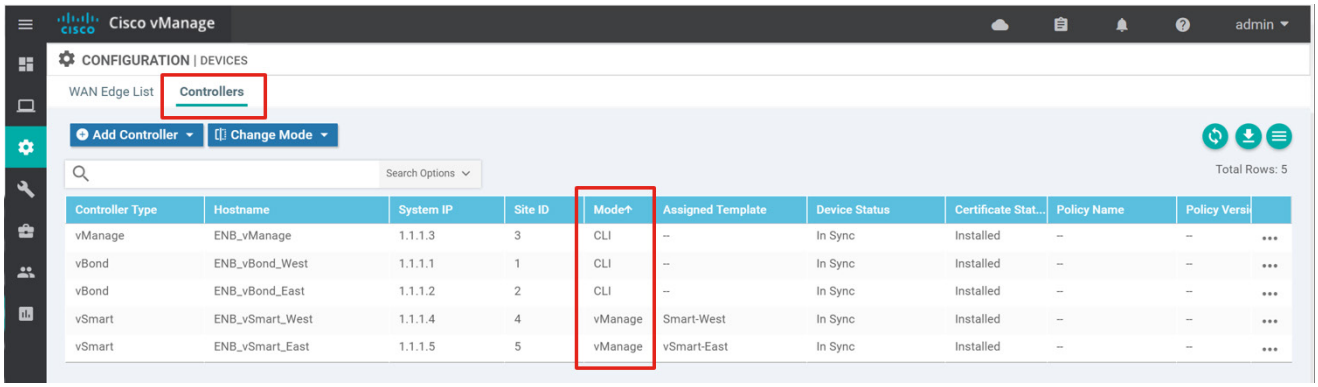
1. 使用 Web 浏览器访问 vManage Web 实例。例如：*https://vmanage1.cisco.com:8443/*
2. 使用用户名和密码凭证登录。
3. 系统将显示 vManage 控制面板。该控制面板顶部将显示用于指示可访问性的状态，包括已安装并添加至 vManage 中的所有 vSmart 控制器、vEdge 路由器和 vBond 协调器的可访问性。验证控制器是否均已显示，再继续其他操作。控制器数量旁边将显示一个绿色向上箭头（表示可访问）或红色箭头（表示不可访问）。



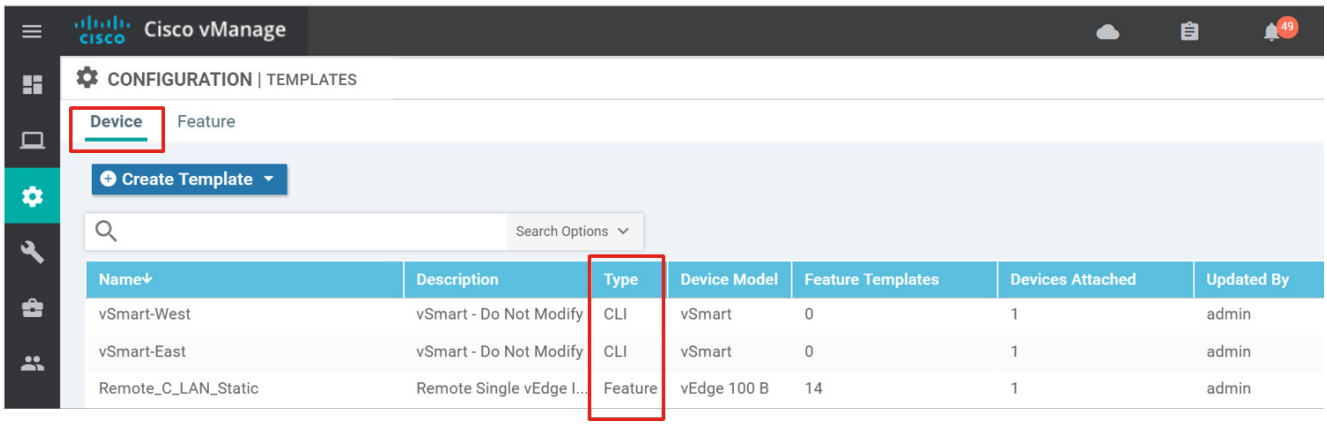
程序 2：确定控制器配置模式

要确定控制器配置模式，请按照以下步骤操作：

1. 依次转到**配置 > 设备**，然后选择**控制器**选项卡。
2. 选中**模式**列。vManage 和 vBond 控制器都处于 CLI 模式下，而 vSmart 控制器处于 vManage 模式下。



3. 要查看 vSmart 控制器使用的模板类型，请依次转到**配置 > 模板**，并确保选择**设备**选项卡。该列显示 vSmart 控制器正在使用 CLI 模板，而不是功能模板。



程序 3：调整配置设置（在所有控制器上均可选）

一些可能需要修改的配置设置如下：

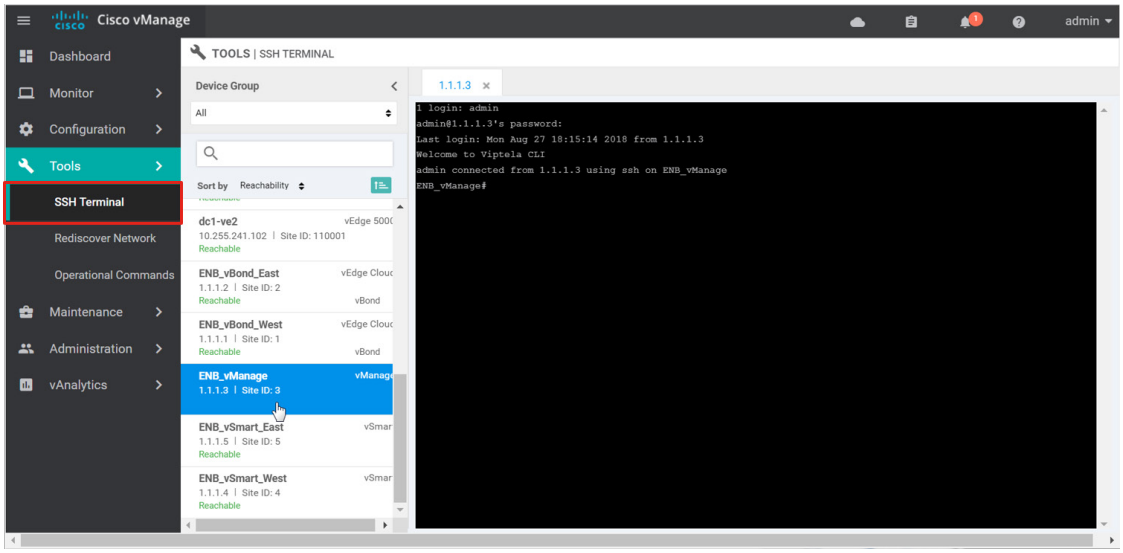
- 管理员密码（所有控制器）- 如果使用本地身份验证，则可能需要更改控制器的管理员密码。
- TLS（vSmart 控制器和 vManage）- 如果可能，请运行传输层安全 (TLS) 协议，作为 vEdge 与控制器之间以及控制器与控制器之间的安全协议。这不适用于 vBond 控制器。TLS 基于传输控制协议 (TCP)，并使用握手和确认。

  技术提示：请注意，更改控制器的安全协议可能会造成非常严重的中断。当前会话会中断，因此请谨慎执行此配置。

- 发送备份路径（仅适用于 vSmart 控制器）- 默认情况下，在有多条等价路径的情况下，重叠管理协议 (OMP) 仅通告最佳路由。启用“发送备份路径”命令时，OMP 还可以在发送最佳路由之外发送次佳路由。这有助于改善收敛。
- 发送路径限制（仅适用于 vSmart 控制器）- 默认情况下，每个前缀通告的等价路由数量为四个。建议将此值增至最大值 16 个。

要修改配置设置，请按照以下步骤操作：

1. 要在 CLI 模式下修改控制器，请使用安全外壳 (SSH) 连接所需控制器。如果有 IP 地址，可以直接执行 SSH 连接。否则，也可以按照以下步骤通过 vManage 进行 SSH 连接：依次转至**工具 > SSH 终端**，然后在左侧选择设备。选择 vManage 控制器。主面板中将显示 SSH 窗口。输入用户名和密码。



2. 在 vManage 控制器上，输入以下命令更改管理员密码并启用 TLS:

```
config terminal
system
 aaa
  user admin password admin
security
 control protocol tls
commit and-quit
```

请注意，您输入的密码是明文版本。它会自动在配置中转换为加密字符串。

3. 对 vBond 控制器重复第 1 步和第 2 步。您不能将控制协议改为 TLS，因为仅可以使用 DTLS。

4. 在 vManage 上，依次转到**配置 > 模板**，找到所需的 CLI 模板名称 (**vSmart-East**)。

5. 选择最右侧的 **...**，然后选择**编辑**

6. 通过添加以下命令修改 CLI 模板。当您将配置插入 CLI 模板中时，可以按任意顺序放置，但必须放在适当的类别标题（系统、OMP、安全）下。否则，配置被推送到设备时可能会出现错误。以下是一个配置代码片段:

```
omp
 no shutdown
 send-path-limit  16
 graceful-restart
```

```
 send-backup-paths
 !
security
 control
  protocol tls
!
```

如要在 CLI 模板中调整 AAA 密码，则需要配置密码加密形式。通过创建变量可轻松完成这种密码更改。变量的值应采用明文形式，在该变量插入配置中并推送至设备之前，系统会自动对它进行加密。

7. 在 CLI 模板中，突出显示加密密码，然后选择**创建变量**。

8. 系统将弹出一个窗口，要求提供替换该文本的变量名称。在**变量名称**文本框中，输入 **admin_password**，然后选择**创建变量**。

9. 选择**更新**。

10. 选择设备右侧的 **...**，然后从下拉菜单中选择**编辑设备模板**。

11. 在文本框中填入新的管理员密码，然后选择**更新**。

12. 选择**下一步**，然后选择**配置设备**。配置将被推送至设备。状态应该会标记为 “成功”。

13. 对 vSmart-West 控制器重复第 4 至 12 步。

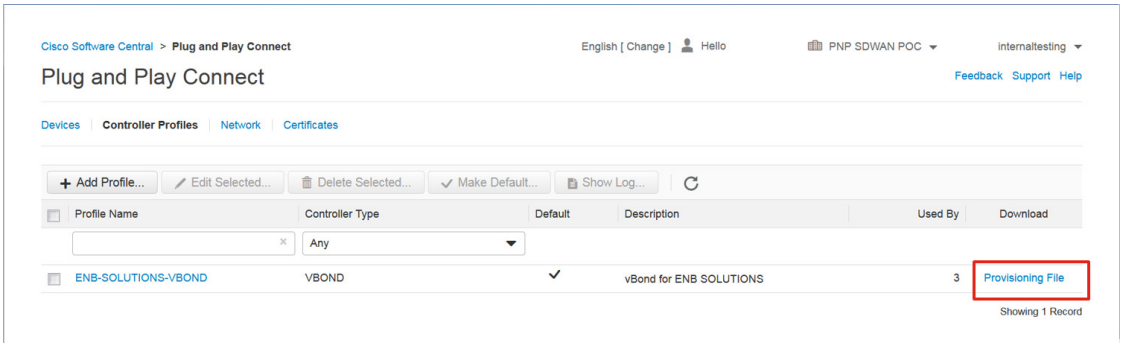
程序 4：检索授权广域网边缘设备序列号文件

要在重叠中启动并激活广域网边缘设备，必须向 vManage 上传有效的授权序列号文件。这种授权序列号文件列出允许进入网络的所有广域网边缘路由器的序列号和机箱编号。vManage 会将此文件发送到控制器，只有与此列表中的序列号匹配的设备才会成功通过控制器的验证和身份验证。

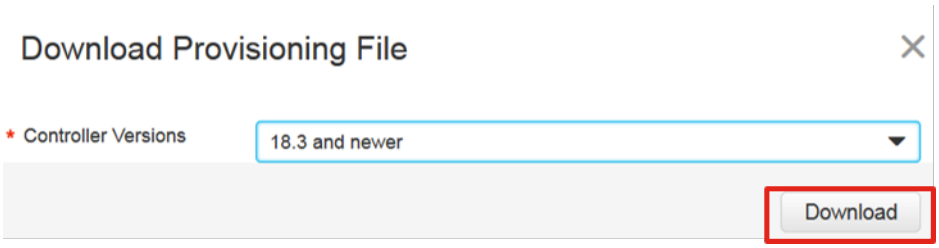
旧的 vEdge 路由器授权序列号文件位于思科 SD-WAN 支持网站上，但这些文件现在已迁移到即插即用 (PnP) 连接门户。PnP 连接门户上的授权序列号文件还包含 IOS XE SD-WAN 路由器信息。有关如何在下载授权序列号文件之前根据需要将任何广域网边缘设备添加到门户的信息，请参阅附录 C。请注意，您可以将多个授权序列号文件上传到 vManage，重复项应该会被过滤掉。

PnP 连接门户

1. 导航至 https://software.cisco.com。
2. 在**网络即插即用**部分下，点击**即插即用连接**。
3. 确保右上角选择的虚拟账户正确。
4. 点击**控制器配置文件**。
5. 在正确的控制器配置文件 (**ENB-SOLUTIONS-VBOND**) 旁边，点击**调配文件**文本。



6. 在弹出窗口中，从下拉列表框中选择控制器版本。请选择 **18.3 版及更高版本**。点击**下载**并将文件保存到您的计算机上。默认情况下，文件将另存为 **serialFile.viptela**。



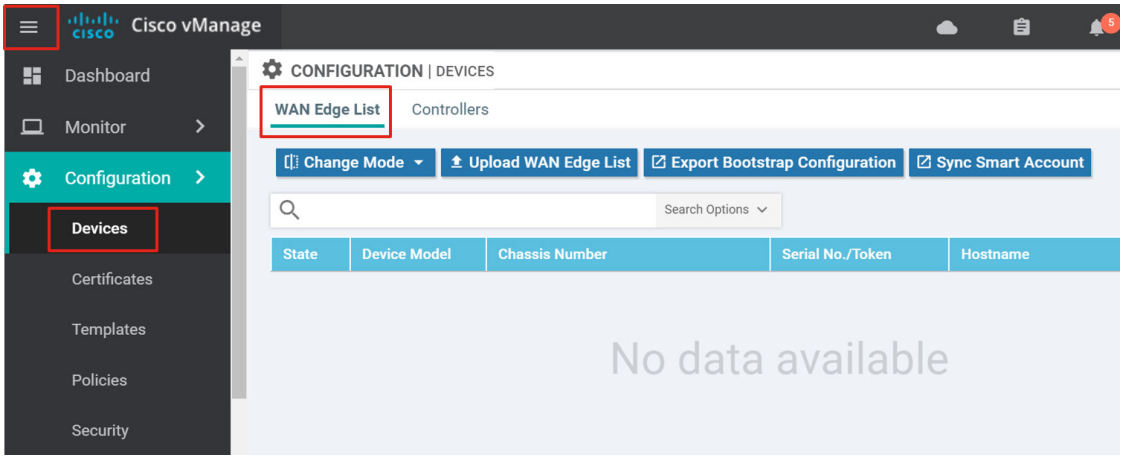
程序 5：上传授权广域网边缘设备序列号文件

将广域网边缘设备序列号文件加载到 vManage 中有两种方法：

- 将列表手动加载到 vManage 中
- 从 vManage 与 PnP 连接门户上的智能账户同步

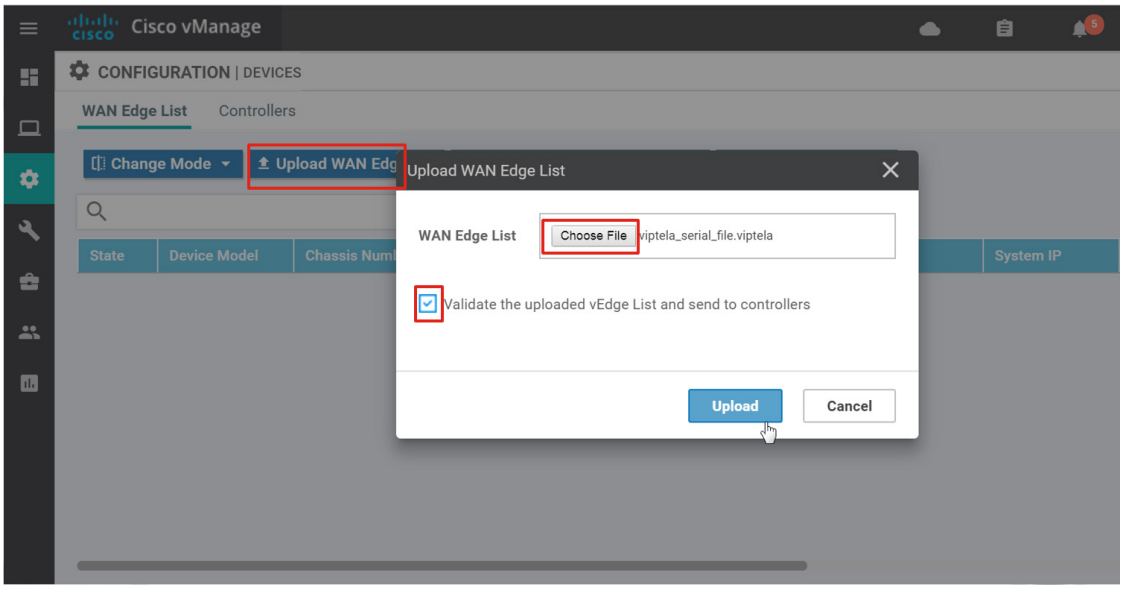
手动加载列表

1. 在 vManage GUI 中，依次转到左侧窗格的**配置 > 设备**。或者，也可以选择 GUI 左上角的三条横杠图标以展开左侧窗格，然后依次选择**配置 > 设备**。确保选择**广域网边缘设备列表**选项卡。



2. 选择**上传广域网边缘设备列表**按钮。系统将显示一个弹出窗口。选择**选择文件**。浏览并选择序列号文件。选择**打开**。

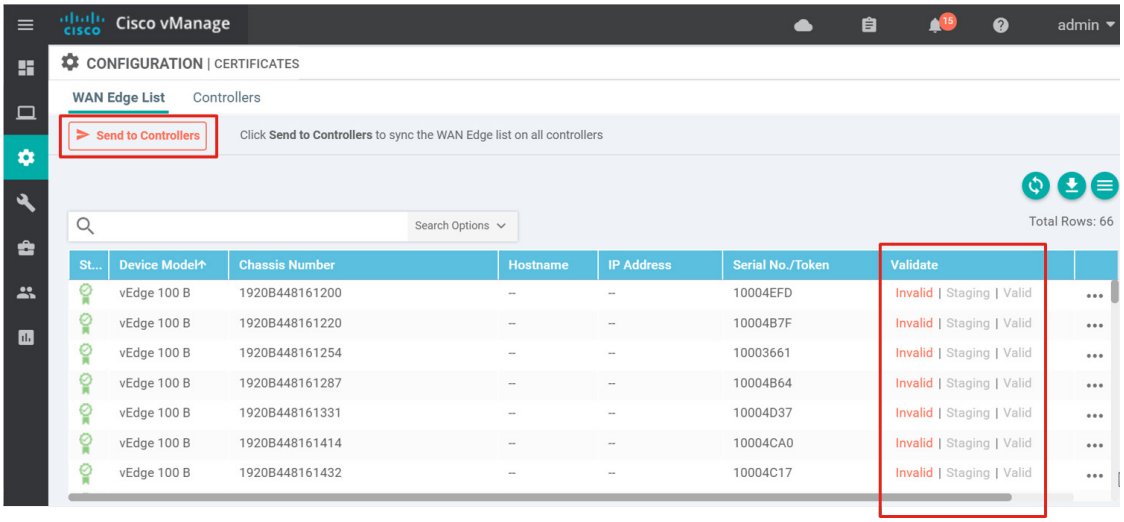
3. 现在已经选择了文件，接下来请选中相应复选框，以便验证列表并将其发送到控制器。选择**上传**按钮。如果选中了前述复选框，这将使列表上的所有设备进入有效状态，也就是说这些设备可以随时连接到网络中并开始转发流量。如果不选中**验证**，所有设备将显示为无效，而且如果您想要将这些设备连接到网络中并加入重叠，则需要逐一将其更改为有效状态。



4. 在接下来显示的确认框中选择**确定**。

5. 系统将显示一个弹出窗口，通知您列表上传成功，并且会告知您成功上传的路由器数量。点击**确定**。系统将显示一个页面，指出已将列表成功推送至 vBond 和 vSmart 控制器。

6. 如果没有选中用于验证已上传列表并将其发送至控制器的复选框，可依次转到**配置 > 证书**，确保选择**广域网边缘设备列表**选项卡，然后选择屏幕左上角的**发送至控制器**按钮。这会将广域网边缘路由器的列表分发给所有控制器。系统将显示一个页面，指出已将列表成功推送至 vBond 和 vSmart 控制器。所有设备都将处于无效状态。

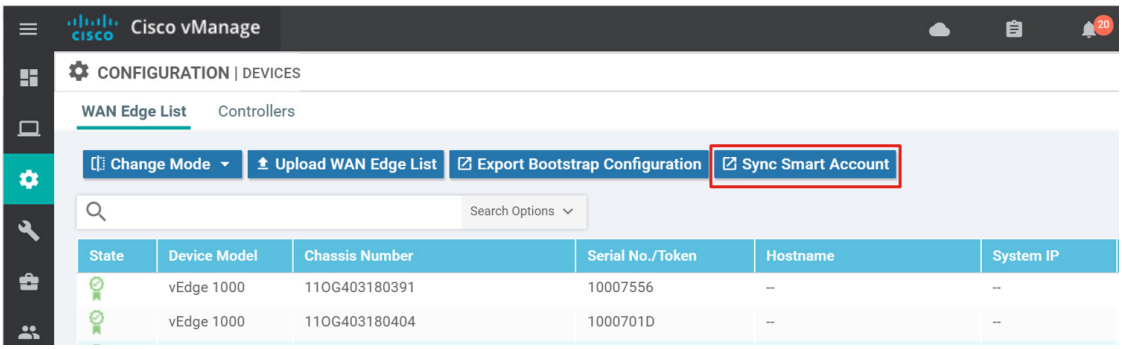


与智能账户同步

从 18.3 版起，vManage 开始提供**同步智能账户**选项，此选项可让 vManage 自动连接到 PnP 连接门户，并拉取授权广域网边缘设备序列号文件。

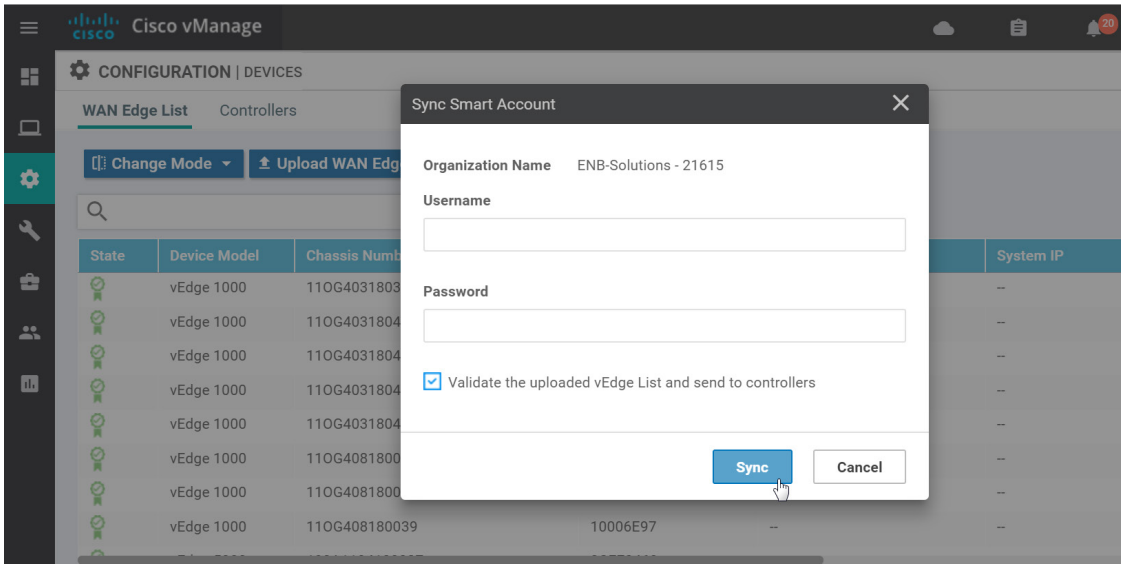
1. 在 vManage GUI 中，依次转到**配置 > 设备**，并确保选择**广域网边缘设备列表**选项卡。

2. 点击**同步智能账户**，系统会弹出一个窗口，提示您输入**用户名**和**密码**。



3. 输入您的思科网站用户名和密码。默认情况下，用于验证已上传列表的复选框已选中。请注意，即使已选中该复选框，与 vManage 同步后仍需将列表分发给其他控制器。

4. 点击**同步**。vManage 将使用 SSL 连接到思科服务器，并使用 REST API 下载授权列表。



5. 在 vManage 中，依次转到**配置 > 证书**，查看已上传的列表。设备应全部处于有效状态。

6. 点击 GUI 左上角的**发送至控制器**按钮，以便使用有效的广域网边缘设备列表更新所有控制器。完成后，操作应该表示成功。

准备软件升级和升级控制器

SD-WAN 软件可以从 https://software.cisco.com 下载，更具体的网址是 https://software.cisco.com/download/home/286320954。

以下是 SD-WAN 产品的文件命名约定。

SD-WAN 文件命名约定

主机名	位置
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

迁移到特定的代码版本时，必须先在 vManage 上升级代码，然后在控制器（vBond 和 vSmart） 上升级代码，最后在广域网边缘路由器上升级代码。将广域网边缘路由器升级至目标代码版本之前，请确保 vManage 和控制器代码版本正确。广域网边缘路由器可以在上线后立即升级，也可以在 ZTP 或 PnP 流程最后部分进行升级；如有必要，甚至可以在部署之前手动升级。vEdge 路由器版本不一定要与控制器相同，但是建议采用相同的版本，否则 vManage GUI 中支持的配置可能在运行较低代码版本的 vEdge 路由器上不受支持。

以下是升级软件时可以采用的一些最佳实践:

1. 升级 vManage，接着升级 vBond 协调器，然后升级半数的 vSmart 控制器。让控制器稳定运行 24 小时。然后升级其余 vSmart 控制器。

2. 将广域网边缘路由器划分为不同的升级组。可以在系统模板中设备组字段内用标记进行标识。选定一个或多个目标测试站点，然后将那些广域网边缘路由器放入第一个升级组。在双广域网边缘路由器站点中，将每台路由器放入不同的升级组，并且不要同时升级两台路由器。一个升级组中的所有广域网边缘路由器可以同时升级（最多 32 台广域网边缘路由器），但也应考虑 vManage 或远程文件服务器向广域网边缘路由器并行传输文件的处理能力。

3. 升级第一个升级组，让代码稳定运行预定的一段时间，然后继续升级其他升级组。

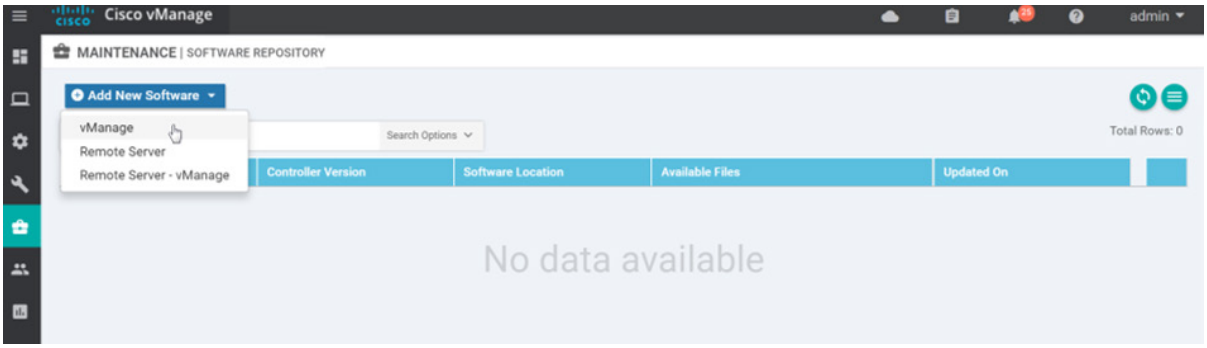
当使用 vManage 执行升级时，您可以使用一个直接上传到 vManage 或远程 vManage 的代码映像进行升级，也可以使用位于远程文件服务器上的代码映像进行升级。

程序 1：准备并配置 vManage 以进行软件升级

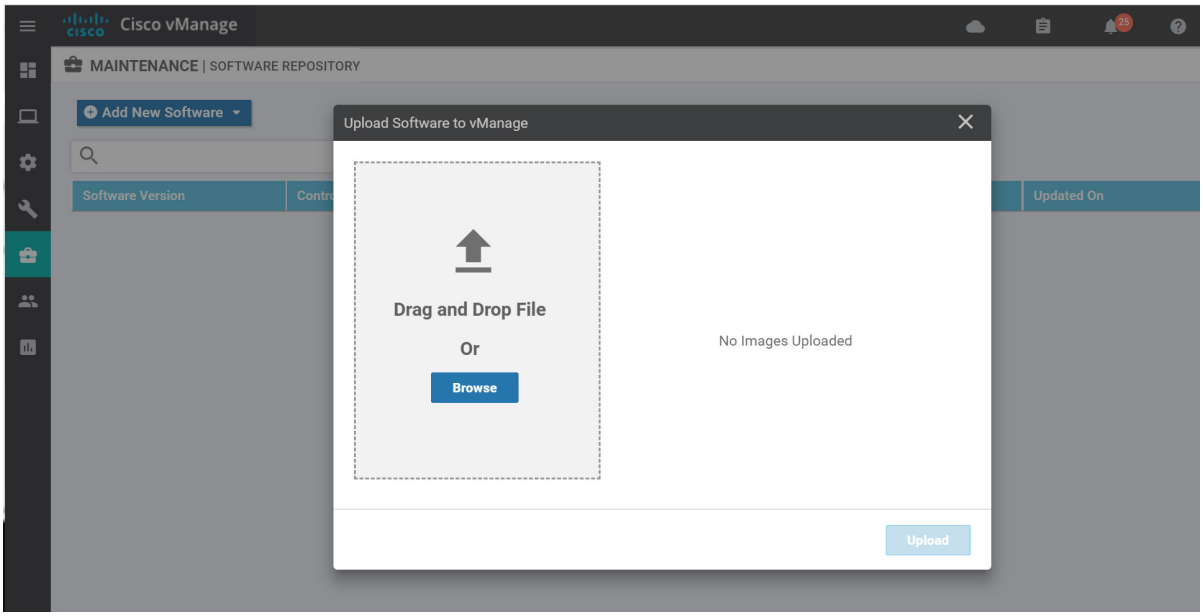
在此程序中，需要将用于任何控制器和广域网边缘路由器的软件上传至 vManage 和远程文件服务器中，然后配置并准备 vManage 软件存储库以升级设备。数据中心设备将使用远程服务器进行升级，而其他设备将使用 vManage 上存储的映像进行升级。

1. 依次转到**维护 > 软件存储库**。存储库会将映像存储在 vManage 本地；在使用远程文件服务器或远程 vManage 的情况下，存储库会指示检索映像的位置。

2. 选择**添加新软件**，系统将显示下拉菜单，您可以从中选择 **vManage**、**远程服务器**或**远程服务器 - vManage**。

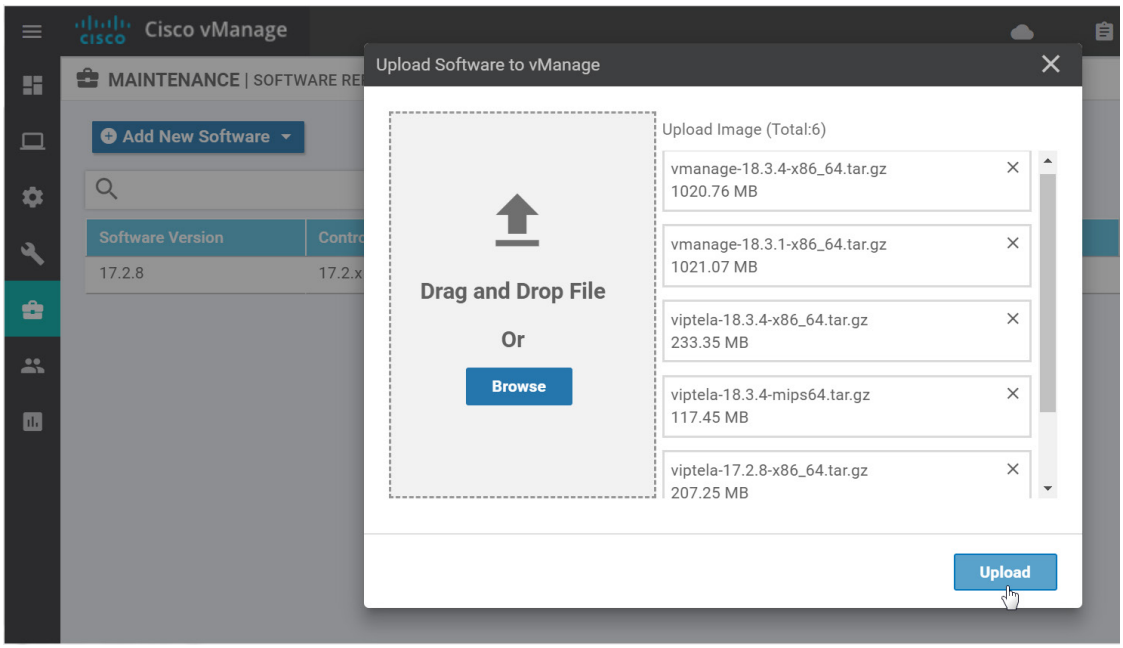


3. 选择 **vManage**。系统将显示一个窗口，提示您放置映像文件或浏览本地计算机上的映像。



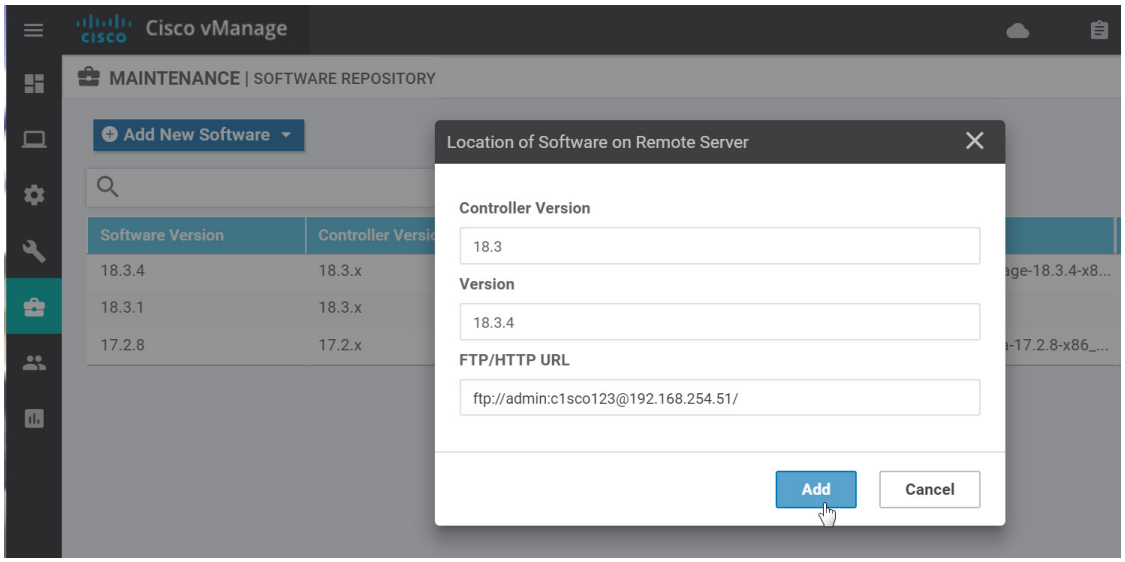
4. 通过放置映像或点击 “浏览” 按钮选择映像，将所需映像加载到窗口中。

5. 点击**上传**按钮。



系统将显示一个窗口，指出正在将相应代码版本加载到 vManage 中。完成后，系统会显示一条消息，指出映像上传成功，并且相应版本、软件位置 (vManage) 和可用文件将添加到存储库中。

6. 要使用远程文件服务器升级设备，请将所需文件上传到远程文件服务器，然后在 vManage 上配置 URL 信息。依次转到**维护 > 软件存储库**。点击**添加新软件**，然后从下拉菜单中选择**远程服务器**。系统将弹出一个窗口。填写**控制器版本** (**18.3**)、映像的代码版本 (**18.3.4**) 以及文件服务器的 FTP 或 HTTP URL，视需要执行身份验证 (**ftp://admin:c1sco123@192.168.254.51/**)。点击**添加**。控制器版本、软件版本、软件位置（远程）和软件 URL 将添加到存储库列表中。



程序 2：升级 vManage（可选）

建议在升级 vManage 之前备份数据。

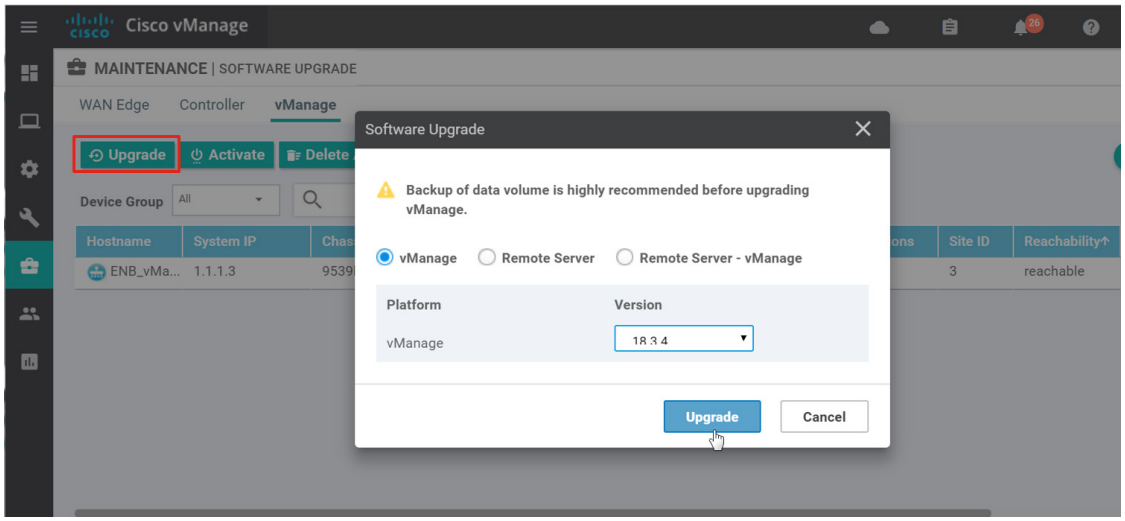
请在升级前查阅版本说明：https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.3/Release_Notes/Release_Notes_for_IOS_XE_SD-WAN_Release_16.9_and_SD-WAN_Release_18.3#Upgrade_to_SD-WAN_Software_Release_18.3

技术提示：升级后无法将 vManage 降级为更低的主要版本。例如，如果运行的是 18.3.x 版本，则无法降级为 18.2.x 或更低版本。虽然您可以将更低的代码版本安装到 vManage 服务器上，但无法激活它。

1. 依次转到**维护 > 软件升级**，然后选择 **vManage** 选项卡。

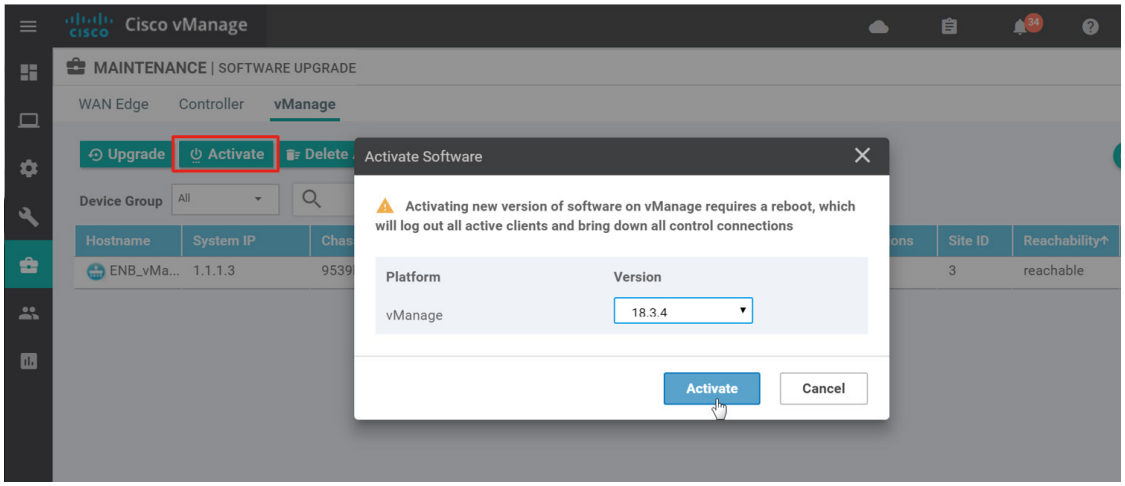
2. 选择页面左上角的**升级**按钮。系统随即开始安装软件，但直到您使用**激活**按钮之后，vManage 才会重新启动并加载新软件。

3. 系统将弹出一个窗口。从下拉列表框中选择所需软件 (**18.3.4**)。系统默认从 vManage 加载映像。选择**升级**。



4. 系统将指出软件安装成功。返回到**维护> 软件升级**并选择 **vManage** 选项卡。然后，选择**激活**按钮。

5. 系统将弹出一个窗口，指出在 vManage 上激活新版本软件需要重新启动，这将注销活动客户端，使 vManage 的控制连接断开。从下拉列表框中选择软件版本 (**18.3.4**)，然后选择**激活**。



6. vManage 再次上线后，重新登录，然后依次转到**维护 > 软件升级**并选择 **vManage** 选项卡，在**当前版本**列下验证当前运行的版本。

程序 3：升级 vBond 和 vSmart 控制器

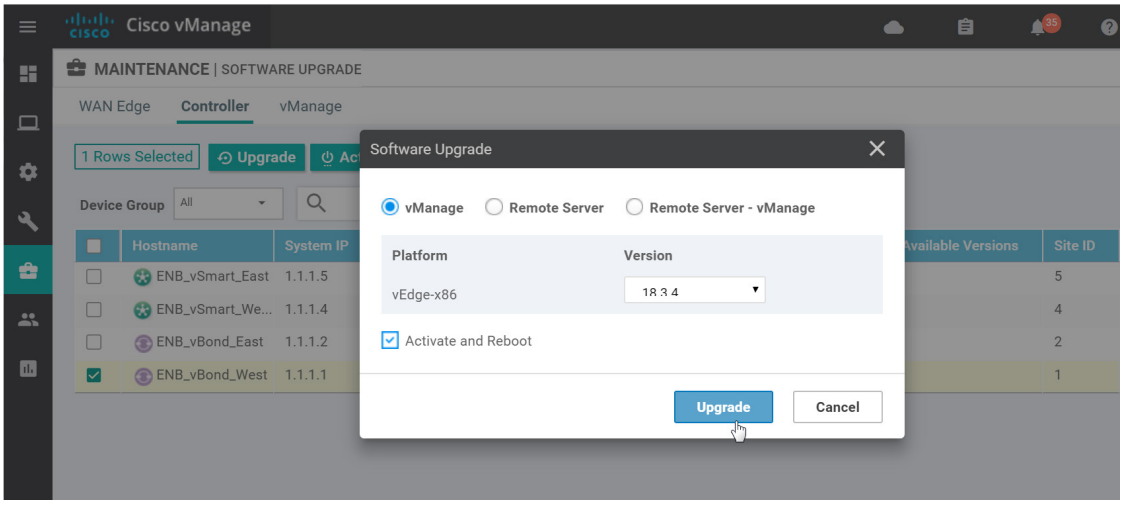
在此程序中，控制器直接从 vManage 上的映像升级。

1. 依次转到**维护 > 软件升级**，然后选择**控制器**选项卡。

2. 选择要升级的 vBond 控制器旁的复选框，然后选择页面左上角的**升级**按钮。

3. 系统将弹出一个窗口。选择软件版本 (**18.3.4**)，并保持 vManage 单选按钮选中状态。

4. 如果要在安装软件后立即激活并重新启动，请选中**激活并重新启动**复选框。如果不选中该复选框，则需要返回到**维护 > 软件升级**，然后选择**控制器**选项卡以单独激活软件，这将重新启动控制器并运行新软件。确保选中**激活并重新启动**所对应的复选框，然后选择**升级**。



5. 依次重复第 1 至 4 步，升级其余控制器。一次可以选择多台控制器。

部署数据中心广域网边缘路由器

本部分假设已配置数据中心防火墙、汇聚交换机和 CE 路由器。附录 F 列出了这些设备上的相关代码部分。

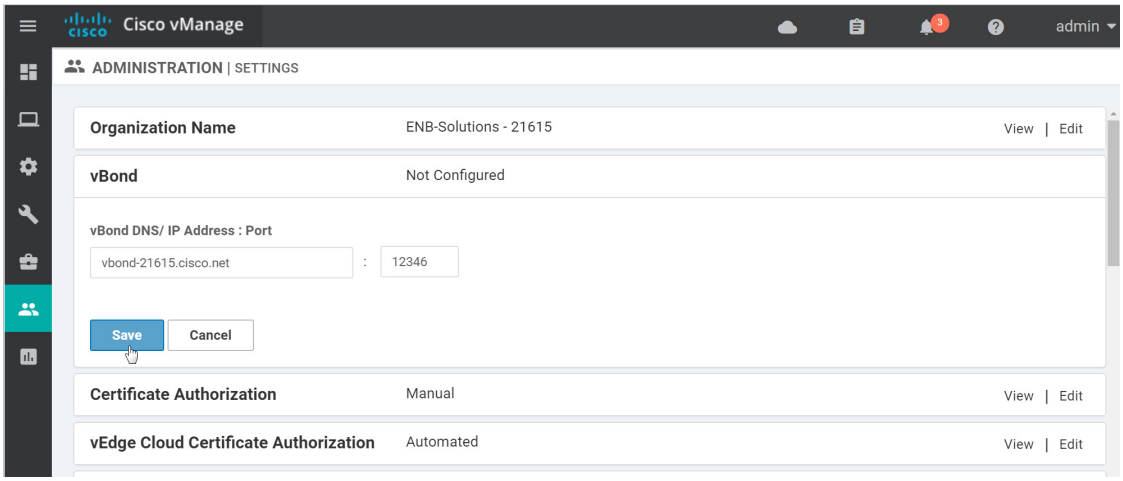
尽管可以执行 ZTP 流程，但数据中心内的 vEdge 路由器仍需手动引导才能连接至 vBond 协调器。

程序 1：验证全局 vBond 地址

您不能通过功能模板修改 vBond IP 地址或主机名；vManage 管理设置下列出的 vBond 协调器 IP 地址或主机名将使用功能模板插入广域网边缘路由器配置中。如果未配置此设置，则在您尝试配置您的第一个设备模板时，系统会将您重定向至此处进行配置。

1. 在 vManage GUI 中，依次转到**管理 > 设置**。**vBond** 配置行应已填入 vBond 主机名和端口号。否则，它会显示*未配置*。

2. 要配置或修改此设置，请在 vBond 配置行右侧选择**编辑**，然后输入 vBond 的 IP 或 DNS 地址 (**vbond-21615.cisco.net**)。选择**保存**。



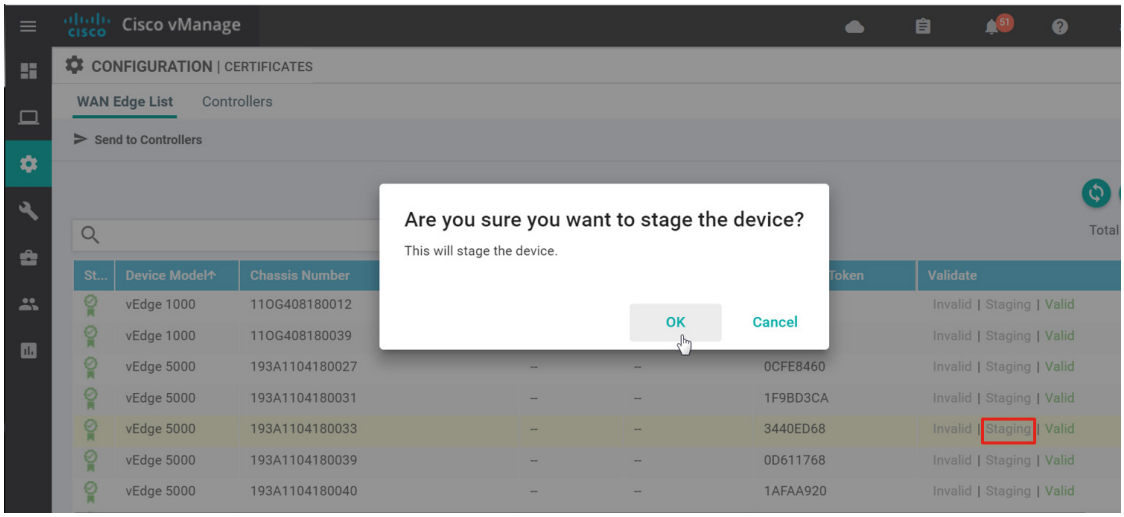
程序 2：将广域网边缘路由器置于试运行状态（可选）

在将广域网边缘路由器连接到网络中之前，我们可以选择首先试运行一下这些路由器。这样我们就可以将其与控制平面相结合，但是直到我们将其设置为有效状态之前它们都不会加入重叠并转发流量。广域网边缘路由器将与 vSmart 控制器建立 OMP 对等关系，但不会发送任何 OMP 路由，也不会有任何本地路由重新分发至 OMP。

1. 在 vManage GUI 中，依次转到**配置 > 证书**。查找属于 DC1 的 vEdge 路由器。为此，您可以目视检查路由器本身并与机箱编号列中的机箱序列号进行核对，也可以在 vEdge 路由器控制台中执行 show hardware inventory 命令：

```
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. 在目标 vEdge 路由器右侧，选择**试运行**。系统将显示一个弹出窗口，询问您是否确定要执行试运行。选择**确定**。



3. 对其他 vEdge 路由器重复第 2 步。

4. 完成后，务必选择屏幕左上角的**发送至控制器**按钮。

程序 3：通过 CLI 配置广域网边缘路由器以连接控制器

1. 通过控制台连接至将要成为 dc1-ve1 的 vEdge 设备。您将会看到登录提示。输入用户名和密码（默认情况下为 **admin/admin**）。如果这是您首次登录，vEdge 配置应该还是出厂默认设置。如要恢复出厂默认设置（不常用）或查看出厂默认配置，请参阅附录 D。

技术提示：如果尝试连接到网络中的 vEdge 5000 的代码版本低于 17.2.5，在启动控制平面时可能会遇到问题。如果遇到问题，可以将 vEdge 路由器手动升级至 17.2.8 或更高版本，然后再尝试将 vEdge 连接到网络。有关手动升级步骤，请参阅附录 E。

---

2. 配置 VPN 0 和将要连接到网络以访问 vBond 的物理接口。需要定义 DNS 服务器以解析 vBond 主机名，并且需要定义一条默认路由以将控制数据包导向下一跳。复制并粘贴以下 CLI 命令：

```
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. 在控制台中向 **vbond-21615.cisco.net** 发出 Ping 请求，测试与 vBond 协调器的连接。确保连接成功，再继续操作。

```
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. 配置必要的系统参数。这些参数包括**系统 IP**、**站点 ID**、**组织名称**和 **vBond** IP 地址或主机名。此外还要定义**系统主机名**，使这些设备在 vManage 中更易于识别。复制并粘贴以下 CLI 命令：

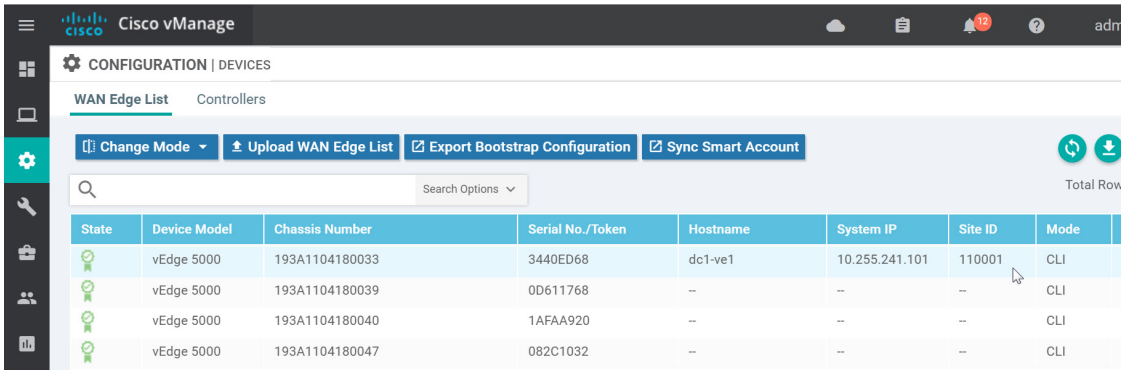
```
config t
system
 host-name dc1-we1
 system-ip 10.255.241.101
 site-id 110001
 organization-name "ENB-Solutions - 21615"
 vbond vbond-21615.cisco.net
commit and-quit
```

5. 验证控制连接。一开始运行 **show control summary** 命令时，系统会显示四个连接：一个连接至 vBond 协调器，一个连接至 vManage，还有两个分别连接至一台 vSmart 控制器。然后 vBond 连接将终止，而与 vManage 和 vSmart 控制器的连接将保持运行。

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

运行命令 **show control connections** 可以显示更多详细信息。

在 vManage 上，**配置 > 设备**输出中将显示 vEdge 路由器。



6. 使用以下引导配置命令对第二台 vEdge 路由器重复第 2 至 5 步：

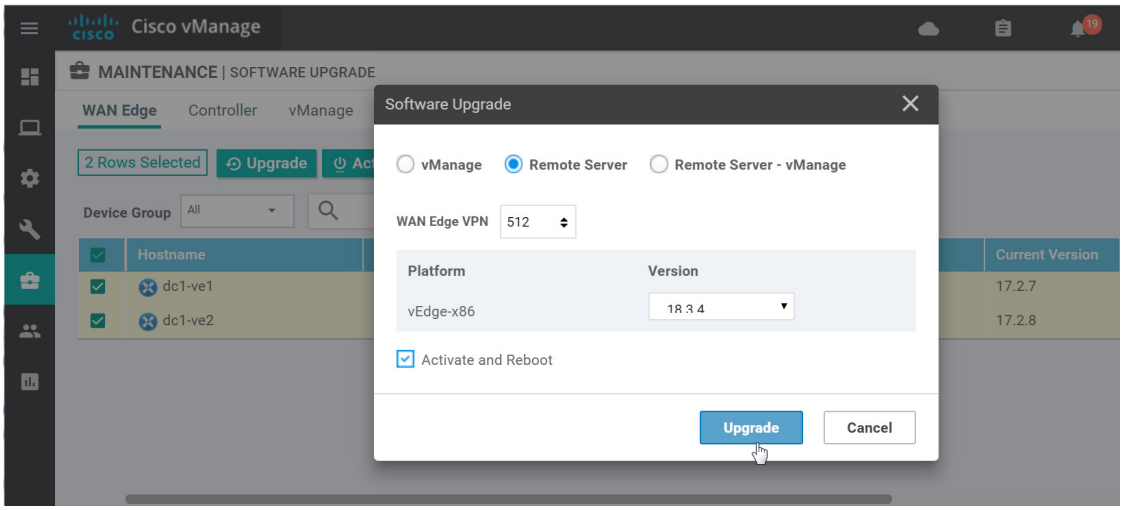
```
config t
vpn 0
 dns 64.100.100.125 primary
 ip route 0.0.0.0/0 10.4.2.5
 interface ge0/0
  ip address 10.4.2.6/30
  tunnel-interface
   encapsulation ipsec
   color biz-internet
vpn 512
interface mgmt0
ip address 192.168.255.168/23
system
 host-name dc1-we2
 system-ip 10.255.241.102
 site-id 110001
 organization-name "ENB-Solutions - 21615"
 vbond vbond-21615.cisco.net
commit and-quit
```

当第二台 vEdge 显示在 vManage 中时，如果您要查看它，可以刷新 vManage 页面。

程序 4：视需要升级 vEdge 路由器

技术提示：将 vEdge 路由器升级为 18.3.0 或更高版本后，就无法再安装 18.2.0 或更低版本的映像。如果 vEdge 上在升级前已经存在映像，则可以激活已经存在的版本较低的映像（一周内）。在 vEdge 路由器上安装并激活 18.3.1 版或更高版本一周后，所有 18.1 版及更低版本的软件映像都会从路由器中删除并且无法再重新安装。请参阅位于以下网址的版本说明：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. 依次转到**维护 > 软件升级**，检查代码版本（请查看**当前版本**列）。
2. 如果需要升级，请选中两台 vEdge 路由器旁的复选框，然后选择**升级**。系统将弹出一个窗口。
3. 从下拉列表框中选择新代码版本，然后选择**远程服务器**单选按钮。选择 vEdge 可以通过哪个 VPN 到达远程服务器。在本例中，我们选择 VPN 512。选中**激活并重新启动**复选框，然后选择**升级**。vEdge 设备将从远程文件服务器检索软件并进行安装，然后重新启动以激活该软件。



程序 5：配置功能模板的基本信息部分

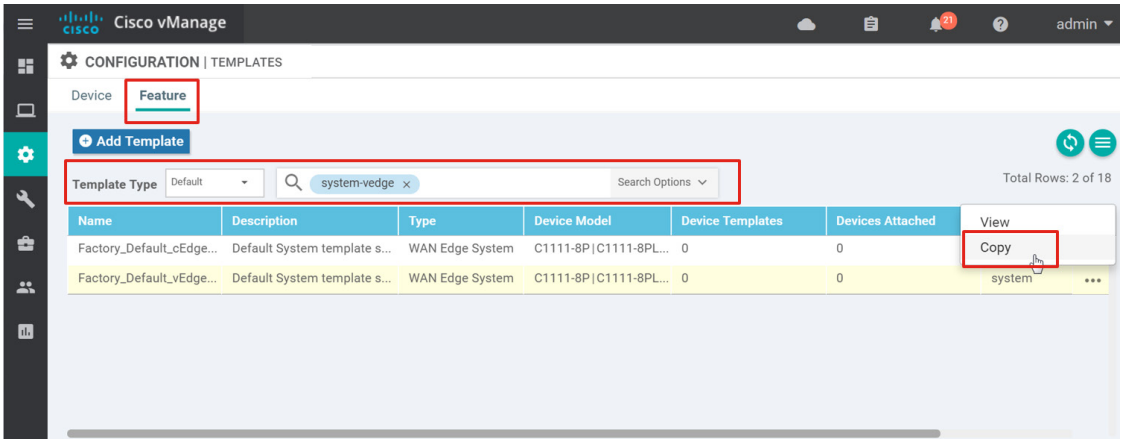
此部分中将配置属于设备模板的基本信息部分的功能模板。这包括系统设置、日志记录、网络时间协议 (NTP)、AAA、OMP、双向转发检测 (BFD) 和安全功能模板。

系统

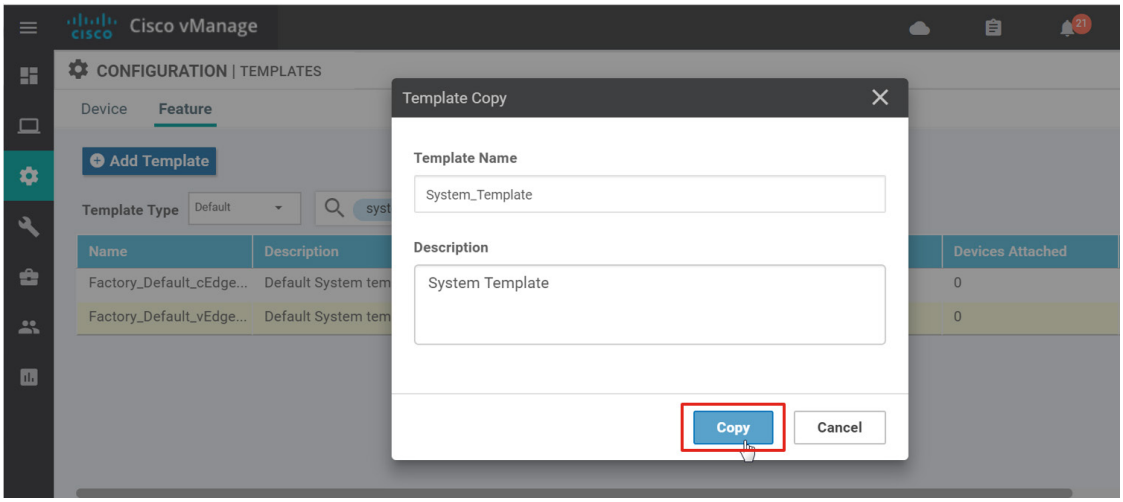
以下步骤显示了通过复制默认系统模板为广域网边缘设备创建系统模板的过程。您需要为经度和纬度等不同的参数创建变量，从而使功能模板可以用于大多数广域网边缘设备。我们可以在 vManage GUI 中依次转到**监控 > 地理位置**，利用经度值和纬度值在 vManage 地图上查看广域网边缘设备的位置。

1. 在**配置 > 模板**页面上，确保选择**功能**选项卡。从**模板类型**旁的下拉列表框中选择**默认**，查看所有默认功能模板的列表。

2. 在搜索框中输入 **system-vedge**，然后按回车键。系统将列出一个模板。选择名为 *Factory_Default_vEdge_System_Template* 的模板旁边的 **...**，然后选择**复制**。

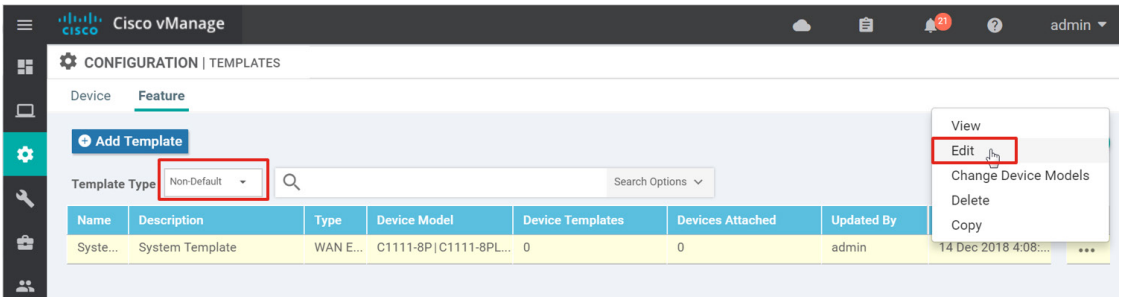


3. 在弹出窗口中，输入模板名称 **System_Template** 和说明**系统模板**，然后选择**复制**。



4. 返回功能模板主屏幕，从**模板类型**下拉列表框中选择**非默认**。文本 **system-vedge** 在文本搜索框中仍然处于启用状态。系统将列出新复制的系统功能模板。

5. 在名为 *System_Template* 的功能模板右侧，选择 **...**，然后选择**编辑**。



系统将显示系统功能模板配置。模板将从其复制的模板中继承**设备类型**字段的值，在此例中设备类型为所有设备类型。默认情况下，已经为**站点 ID**、**系统 IP** 和**主机名**创建以下参数变量：**system_site_id**、**system_system_ip** 和 **system_hostname**。

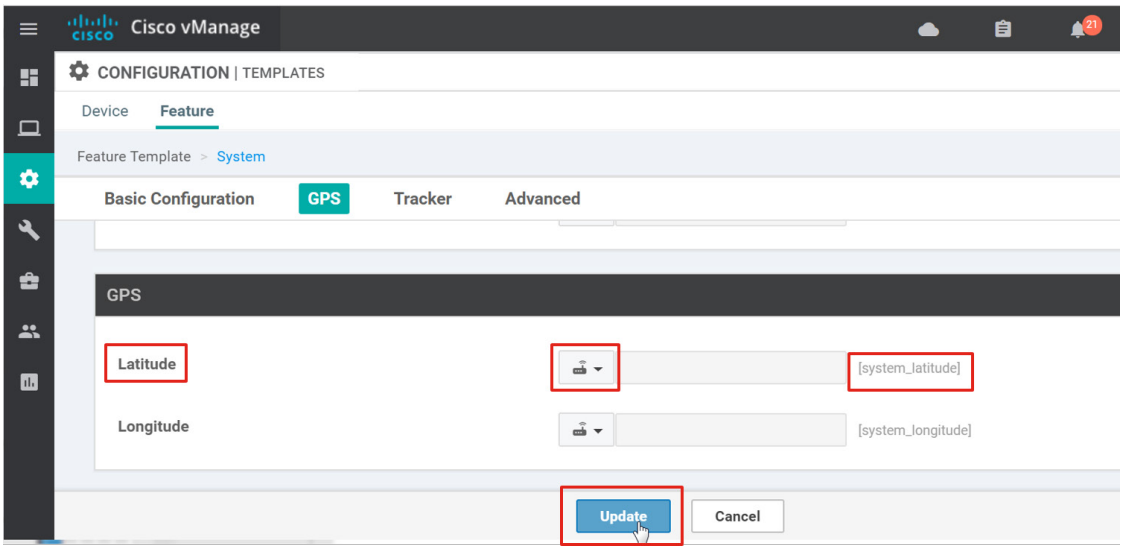
6. 在使用 vManage GUI 进行升级和监控时，设备组有助于对常用广域网边缘路由器进行整理和分组。例如，您可以根据类型或位置组织广域网边缘路由器，在升级过程中将它们放入不同升级组。在**设备组**旁边，从下拉列表框中选择**特定设备专用**。使用变量名称 **system_device_groups**。

7. 在**控制台波特率 (bps)** 旁边，从下拉列表框中选择**特定设备专用**。使用变量名称 **system_console_baud_rate**。IOS XE SD-WAN 路由器 (**9600 bps**) 和 vEdge 路由器 (**115200 bps**) 的默认波特率不同。

8. 在**纬度**旁边，从下拉列表框中选择**特定设备专用**。保留默认变量名称 **system_latitude**（也可以点击文本框并输入一个新的变量名称，从而更改变量名称）。

9. 对 “纬度” (system_longitude)、“端口跳变” (system_port_hop) 和 “端口偏移量” (system_port_offset) 设置重复第 5 步。包括 “时区” (UTC) 在内，所有其他设置均采用默认配置。

10. 选择**更新**。



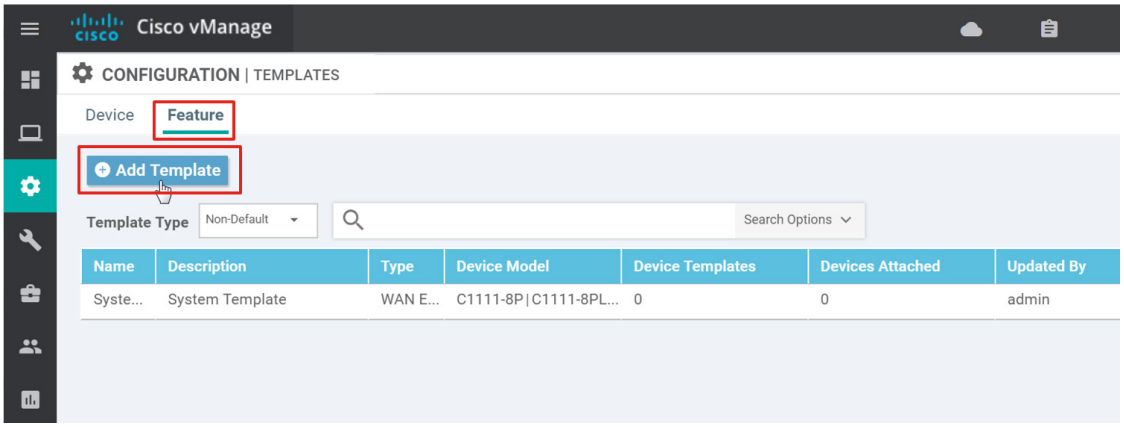
下表总结了系统功能模板中配置的参数:

系统功能模板设置

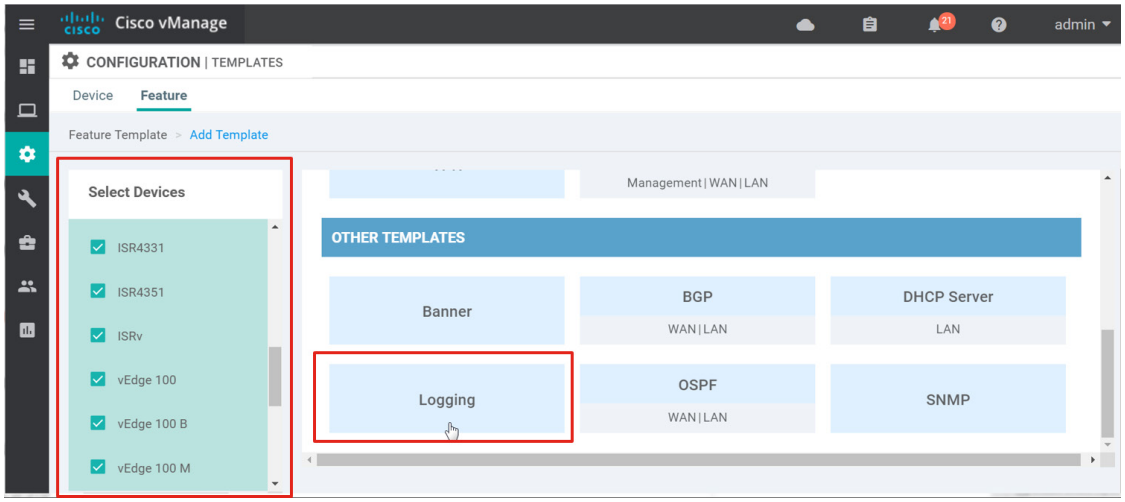
部分	参数	类型	变量/值
基本配置	站点 ID	特定设备专用	system_site_id
	系统 IP	特定设备专用	system_system_ip
	主机名	特定设备专用	system_hostname
	设备组	特定设备专用	system_device_groups
	控制台波特率 (bps)	特定设备专用	system_console_baud_rate
GPS	纬度	特定设备专用	system_latitude
	经度	特定设备专用	system_longitude
高级	端口跳变	特定设备专用	system_port_hop
	端口偏移量	特定设备专用	system_port_offset

日志记录

11. 要创建日志记录功能模板，请依次转到**配置 > 模板**，然后选择**功能**选项卡。选择**添加模板**按钮。



12. 在左侧选择要将此模板应用到的设备。选中除 vManage 和 vSmart 之外的所有设备所对应的复选框。在右侧的**其他模板**类别下，选择**日志记录**模板块。

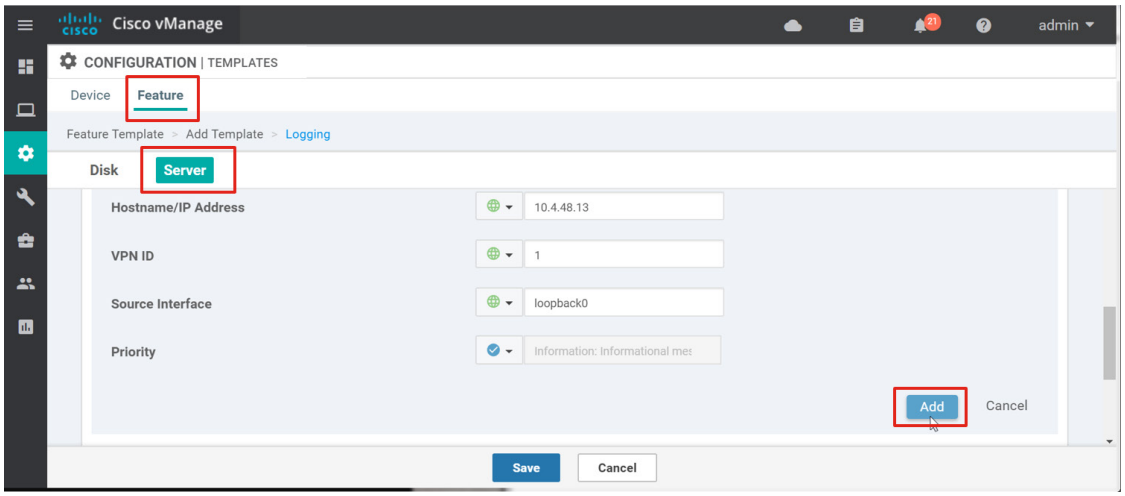


13. 系统显示“日志记录”模板。填写“模板名称”(**Logging_Template**) 和“说明”（**日志记录模板**）

14. 选择**服务器**，以跳转到该模板的日志记录服务器部分。选择**新建服务器**按钮。在**主机名 /IP 地址**框中，输入日志记录服务器主机名或 IP 地址（在本例中是 **10.4.48.13**）。默认情况下，这是一个**全局**值，这意味着值 **10.4.48.13** 将应用于应用此模板的所有设备。或者，也可以将此变量定义为**特定设备专用**变量。

15. 对于 **VPN ID**，从下拉列表框中选择**全局**，然后输入 **1**，引用将要创建的服务端 VPN 编号。日志记录服务器位于数据中心，应该可以从任意站点的本地网络对其进行访问。对于远程站点，流量将穿越隧道到达数据中心。

16. 对于**源接口**，从下拉列表框中选择**全局**，然后在文本框中输入 **loopback0**。我们需要从 loopback0 获取日志记录消息，即设备的系统 IP，以便更好地关联 vManage 上显示的事件。



技术提示：因为 loopback0 在此模板中作为日志记录消息的源接口引用，所以必须在引用的功能模板中的某处定义 loopback0。如果不定义 loopback0，但在日志记录模板中进行引用，则当设备模板部署到设备中时，配置推送将会失败。

17. 默认情况下，事件也将记录到本地磁盘中。其优先级默认设置为信息性消息。选择**添加**按钮，以便将日志记录服务器配置添加到功能模板中。

> **技术提示：**如果您在选择**保存**或**更新**按钮以保存或更新对功能模板的更改之前忘了选择**添加**按钮，您的日志记录服务器配置将会丢失，届时您需要编辑模板并重新进行配置。

18. 选择**保存**按钮以完成模板。

下表总结了日志记录功能模板中配置的参数：

日志记录功能模板设置

部分	参数	类型	变量/值
服务器	主机名/IP 地址	全局	10.4.48.13
	VPN ID	全局	1
	源接口	全局	loopback0

网络时间协议 (NTP)

在 NTP 模板中，设备将使用位于互联网中的 NTP 服务器 **time.nist.gov**，通过传输端 VPN（即 VPN 0）可访问该服务器。保持正确的时间非常重要，因为需要使用证书进行身份验证并连接控制器。需要连接到 vSmart 控制器，然后才能形成 IPSec 隧道并从分支机构恢复与数据中心的连接。为了使 NTP 正常工作，必须在传输端 VPN 中配置一个 DNS 服务器以解析 NTP 主机名。此外，还需要在隧道接口上允许 NTP 协议，否则 NTP 将无法在传输端 VPN 中工作。本指南后面部分中配置的 VPN 接口模板中将配置 DNS 和允许的协议。

19. 假设您仍在“功能模板”页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 NTP 模板：

    选择设备：**除 vManage 和 vSmart 之外的所有设备**

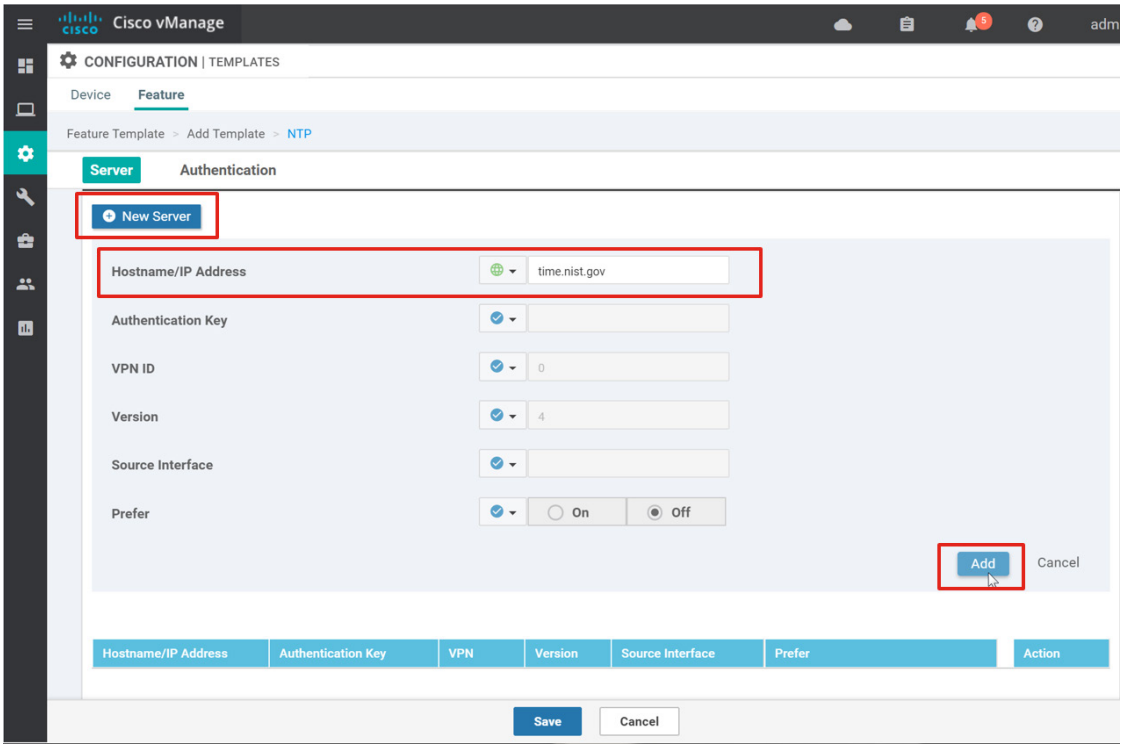
    模板：基本信息/NTP

    模板名称：**NTP_Template**

    说明：NTP 模板

20. 在**服务器**部分，选择**新建服务器**按钮，然后在**主机名 /IP 地址**框中输入 **time.nist.gov**。没有配置身份验证，而且 **VPN ID** 默认情况下为 0。

21. 选择**添加**。按需添加任何其他服务器。



技术提示：如果选择使用身份验证，则需要在配置**服务器**部分之前，配置 NTP 功能模板的**身份验证**部分。如果您尝试先配置**服务器**部分，并且使用身份验证密钥，系统将提示您值无效（因为尚未创建身份验证），无法添加服务器信息，同时仍引用一个尚不存在的身份验证密钥。

22. 选择**保存**以完成模板。

下表总结了 NTP 功能模板中配置的参数。

NTP 功能模板设置

部分	参数	类型	变量/值
服务器	主机名/IP 地址	全局	time.nist.gov

AAA

在 AAA 功能模板中，定义本地身份验证并创建其他用户、具有只读权限的操作员和可以执行所有操作的 netadmin 用户。请注意，这可以在用户使用 SSH 访问设备时控制访问。在 vManage 中，可以对不同组下的不同用户分别进行配置，从而控制对 vMangage GUI 的访问（在**管理 > 管理用户**下）。

23. 假设您仍在“功能模板”页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 AAA 模板：

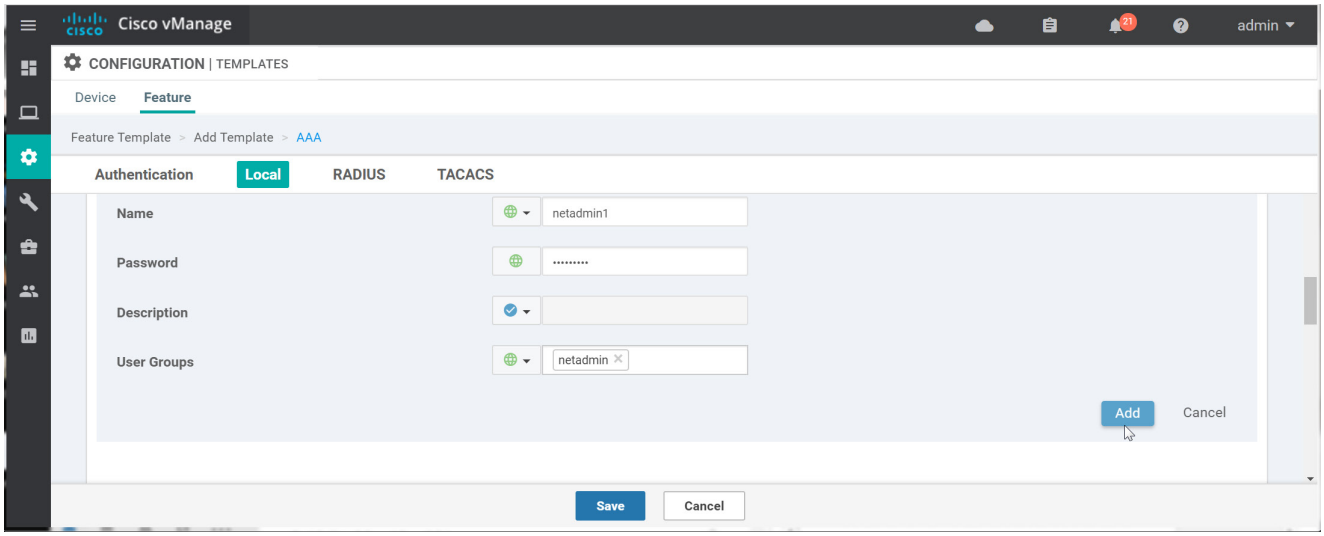
    选择设备：除 vManage 和 vSmart 之外的所有设备

    模板：基本信息/AAA

模板名称：**AAA_Template**

说明：**AAA 模板**

24. 在**身份验证顺序**参数下，从下拉列表框取消选择 **radius** 和 **tacacs**（因此只剩下 **local** 方法）。点击下拉列表框外部位置，从而关闭下拉菜单。
25. 在**本地**身份验证部分下，点击**新建用户**按钮。
26. 在**名称**旁边，输入 **oper1**。在**密码**旁边，输入密码。在**用户组**旁边，从下拉文本框中选择 **operator**。
27. 点击**添加**。
28. 点击**新建用户**按钮添加第二个新用户。
29. 在**名称**旁边，输入 **oper1**。在**密码**旁边，输入密码。在**用户组**旁边，从下拉文本框中选择 **operator**。
30. 在**名称**旁边，输入 **netadmin1**。在**密码**旁边，输入密码。在**用户组**旁边，从下拉文本框中选择 netadmin。
31. 点击**添加**。



32. 选择**保存**以完成模板。

下表总结了 AAA 功能模板中配置的参数。

AAA 功能模板设置

部分	参数	类型	变量/值
身份验证	身份验证顺序	下拉列表	本地
本地/新建用户	名称/密码/用户组	全局	oper1/oper1/operator
	名称/密码/用户组	全局	netadmin1/netadmin1/netadmin

重叠管理协议 (OMP)

在 OMP 功能模板中，**每前缀通告的路径数**和 **ECMP 限制**参数将从默认值 4 改为最大值 16。默认情况下，连接的和静态的路由与 OSPF 将重新分发至 OMP，但外部 OSPF 路由除外。它将在全局级别被禁用，但将在需要的情况下在服务端 VPN 模板中启用。

33. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 OMP 模板：

    选择设备：**除 vManage 和 vSmart 之外的所有设备**

    模板：基本信息/OMP

    模板名称：**OMP_Template**

    说明：OMP 模板

34. 配置以下参数**：**

OMP **功能模板设置**

部分	参数	类型	变量/值
基本配置	每前缀通告的路径数	全局	16
	ECMP 限制	全局	16
通告	互联	全局	关闭
	静态	全局	关闭

35. 选择**保存**以完成模板。

双向转发检测 (BFD)

应用感知路由使用 BFD 来计算 SLA 类的延迟、丢包和抖动。BFD 还在隧道传输链路上用于检测链路故障。BFD 默认处于启用状态且无法禁用。

在 BFD 功能模板中，应用感知路由 BFD 轮询间隔被修改为 120000 毫秒。通过模板中的**颜色**部分，您可以更改传输链路上的默认 BFD 计时器，以检测隧道故障并打开或关闭路径 MTU 发现 (PMTUD)。默认情况下，PMTUD 处于启用状态。

36. 假设您仍在 “功能模板” 页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 BFD 模板：

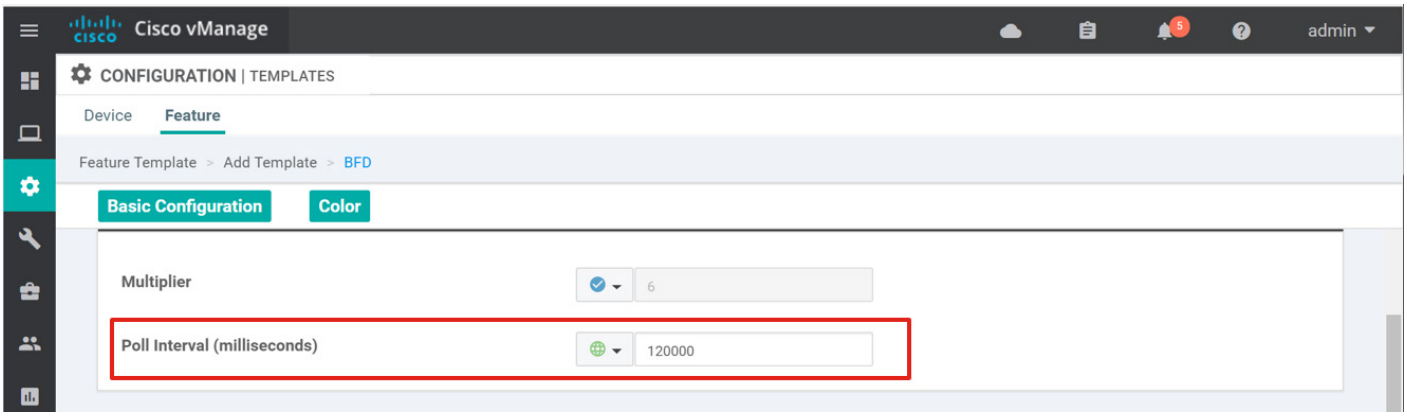
    选择设备：**除 vManage 和 vSmart 之外的所有设备**

    模板：基本信息/BFD

模板名称：**BFD_Template**

说明：**BFD 模板**

37. 在**基本配置**下的**轮询间隔**旁边，选择**全局**并在文本框中输入 **120000**。



38. 选择**保存**以完成模板。

下表总结了 BFD 功能模板中配置的参数。

BFD 功能模板设置

部分	参数	类型	变量/值
基本配置	轮询间隔	全局	120000

安全

在安全功能模板中，反重放窗口配置为建议值（4096 个数据包）。

39. 假设您仍在 “功能模板” 页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建安全模板：

选择设备：**除 vManage 和 vSmart 之外的所有设备**

模板：**基本信息/安全**

模板名称：**Security_Template**

说明：**安全模板**

40. 配置以下参数：

安全功能模板设置

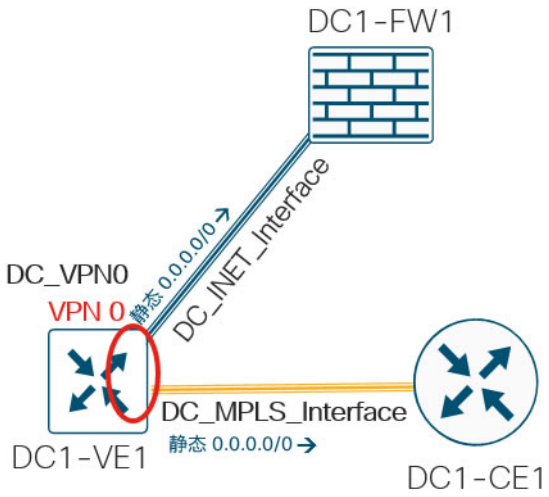
部分	参数	类型	变量/值
基本配置	重放窗口	全局/下拉列表	4096

41. 选择**保存**以完成模板。

程序 6：配置传输端 VPN

对于数据中心，需要创建传输端 VPN 或 VPN 0 功能模板。在 VPN 模板中，您可以配置等价多路径 (ECMP) 键控、DNS 和静态路由。然后为每个传输链路定义物理接口，即 MPLS 接口和互联网接口。在这些模板中，您需要配置接口名称、IP 地址和 IPSec 隧道特征。

图 13　数据中心 vEdge 传输模板

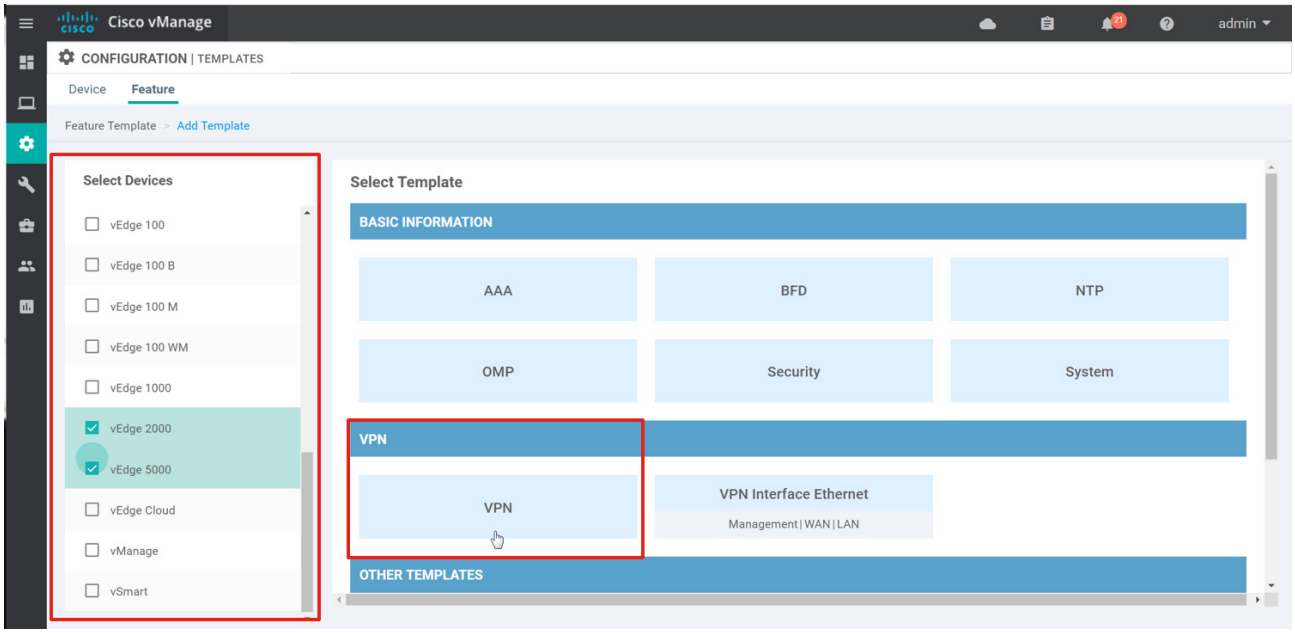


传输端 VPN (VPN 0)

1. 在 vManage GUI 中，依次选择**配置 > 模板**，然后选择**功能**选项卡。
2. 选择**添加模板**按钮。

对于 VPN 特定的配置，数据中心模板与分支机构模板保持独立，因此在分支机构模板配置中所做的更改不会无意中更改数据中心的配置。

3. 在**选择设备**列中，选择 **ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000** 和可能位于数据中心内的任何其他广域网边缘设备类型。在右侧的 VPN 部分下，选择 **VPN** 模板块。



4. 配置 “模板名称” 和 “说明”：

   模板名称：**DC _VPN0**

   说明：**数据中心传输端 VPN 0**

5. 在**基本配置**下的 **VPN** 旁边，将 **VPN ID** 配置为 **0**。

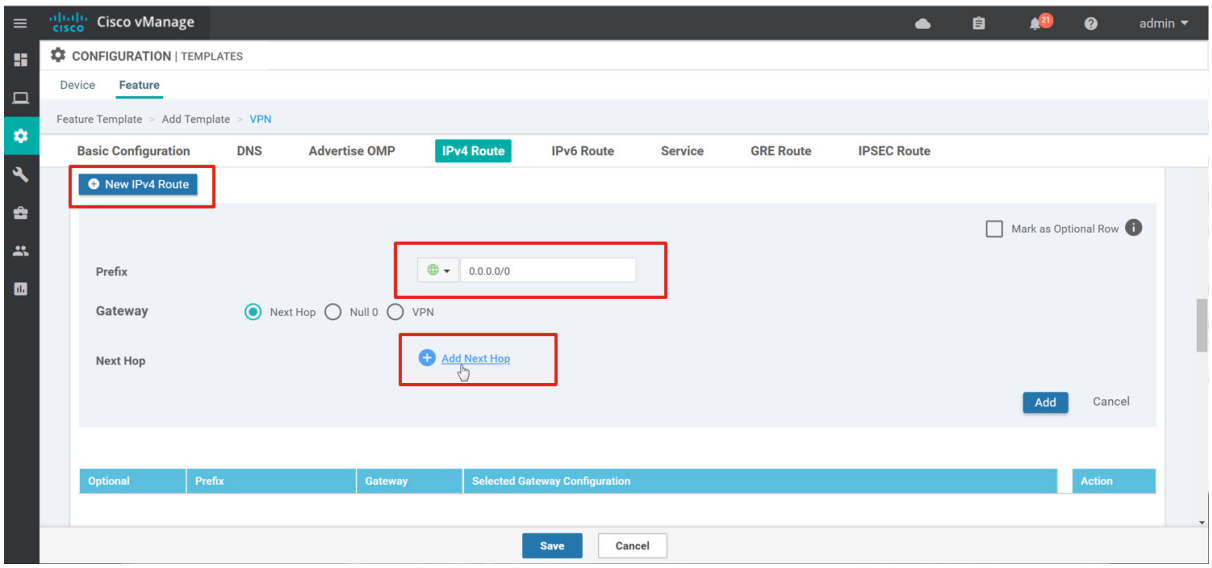
6. 在**名称**旁边，从下拉菜单中选择**全局**，然后输入**传输端 VPN** 作为对 VPN 的说明。

7. 在**增强 ECMP 键控**旁边，从下拉菜单中选择 “全局”，然后选择**开启**。启用此功能会将 ECMP 散列配置为使用第 4 层源和目的端口，以及源和目的 IP 地址、协议和差分服务代码点 (DSCP) 字段作为 ECMP 散列键。VPN 中有等价路由路径时使用 ECMP，并且流量对 IP 报头中的键值字段中使用散列来确定选择哪条路径。

8. 在 **DNS** 下的**主 DNS 地址**旁边，从下拉菜单中选择**全局**，然后输入 **64.100.100.125**。系统将显示**辅助 DNS 地址**框。从下拉菜单中选择**全局**，并在**辅助 DNS 地址**文本框中输入 **64.100.100.126**。

在 **IPv4 路由**模板部分下，为每个接口添加默认路由。请使用这些路由，以便隧道终端可以与相邻站点建立对等关系。由于广域网边缘设备在执行路由决策时使用物理隧道终端源和目的，因此可能会存在多条默认路由。

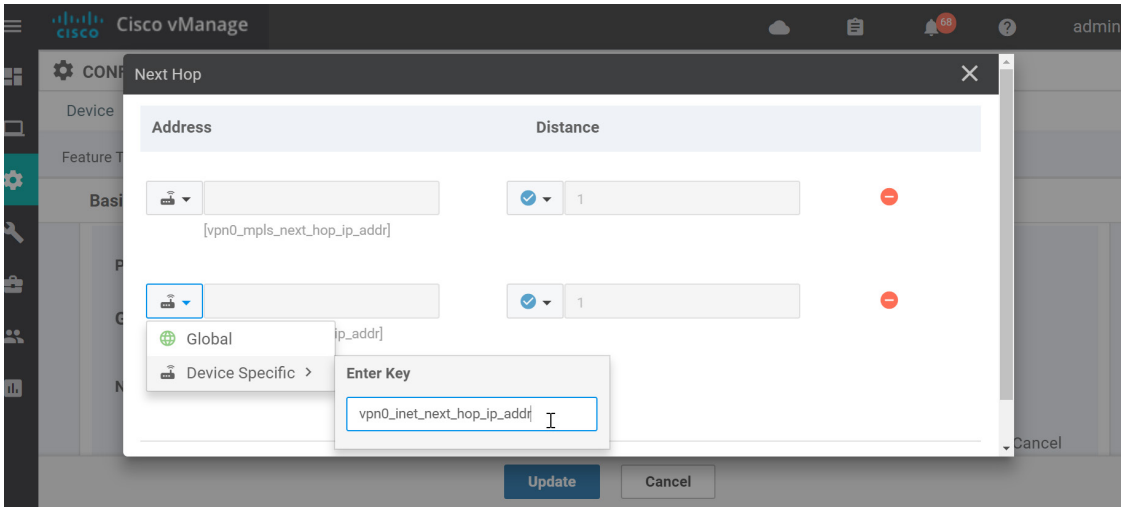
9. 在 **IPv4 路由**部分下，点击**新建 IPv4 路由**按钮。在**前缀**框中添加 **0.0.0.0/0**，然后选择**添加下一跳**。



10. 系统将显示一个弹出窗口，提示您可以添加第一个下一跳。选择**添加下一跳**按钮。

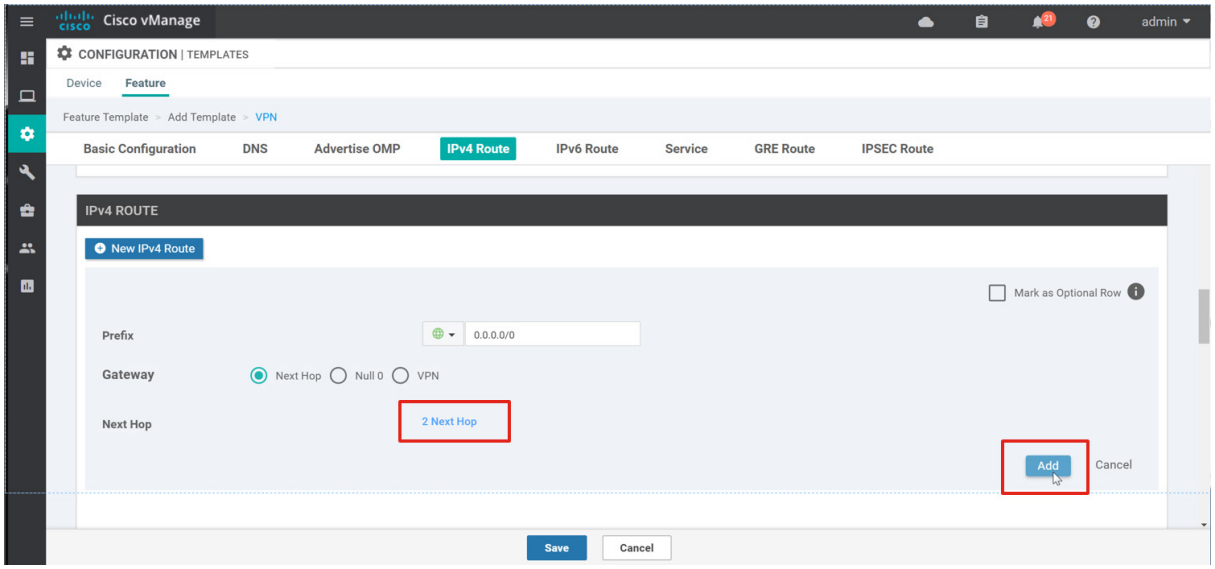
11. 由于此模板将应用于多个广域网边缘设备，因此下一跳参数是变量，而不是全局值。在弹出窗口中，在**地址**下，从下拉菜单中选择**特定设备专用**，并在文本框中输入 MPLS 传输链路的下一跳 IP 地址 (**vpn0_mpls_next_hop_ip_addr**)。点击**添加下一跳**按钮添加第二个下一跳。

12. 在**地址**下的第二个下一跳条目上，从下拉菜单中选择**特定设备专用**，然后在文本框中为互联网传输链路输入下一跳 IP 地址变量 (**vpn0_inet_next_hop_ip_addr**)。



13. 在弹出窗口底部选择**添加**。这将为前缀 **0.0.0.0/0** 存储这两个下一跳。您将返回到 “功能模板” 页面。

14. 现在，**下一跳**字段将显示配置了 **2 个下一跳**条目。按**添加**将前缀 **0.0.0.0/0** 以及该前缀的下一跳信息添加到模板。



15. 选择**保存**以创建模板。

下表总结了 VPN 0 功能模板中配置的参数:

VPN 0 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	0
	名称	全局	传输端 VPN
	增强 ECMP 键控	全局	开启
DNS	主 DNS 地址	全局	64.100.100.125
	辅助 DNS 地址	全局	64.100.100.126
IPv4 路由	前缀	全局	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn0_mpls_next_hop_ip_addr
	下一跳地址	特定设备专用	vpn0_inet_next_hop_ip_addr

接下来，在传输端 VPN 下配置接口。

VPN 接口 (MPLS)

16. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 VPN 接口模板:

    选择设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

    模板：VPN/VPN 接口以太网

    模板名称：**DC_ MPLS_Interface**

    说明：数据中心 MPLS 接口

17. 在**基本配置**部分的**关闭**旁边，选择**特定设备专用**，并输入变量名称 **vpn0_mpls_int_shutdown**。通过将端口状态定义为一个变量，可以出于任何原因打开或关闭端口，只需修改变量值即可，无需修改功能模板。

18. 在**基本配置**部分的**接口名称**旁边，选择**特定设备专用**，并输入变量名称 **vpn0_mpls_int_x|x**。通过将接口名称作定义为一个变量，可以出于任何原因修改接口，只需修改变量值即可，而无需修改功能模板。

19. 在**基本配置**下的**说明**旁边，选择**全局**并输入 **MPLS 接口**作为对此接口的说明。

20. 在**基本配置**部分 “IPv4 配置” 下的 “IPv4 地址” 旁边，选择**特定设备专用**，并输入变量名称 **vpn0_mpls_int_ip_addr|maskbits**。

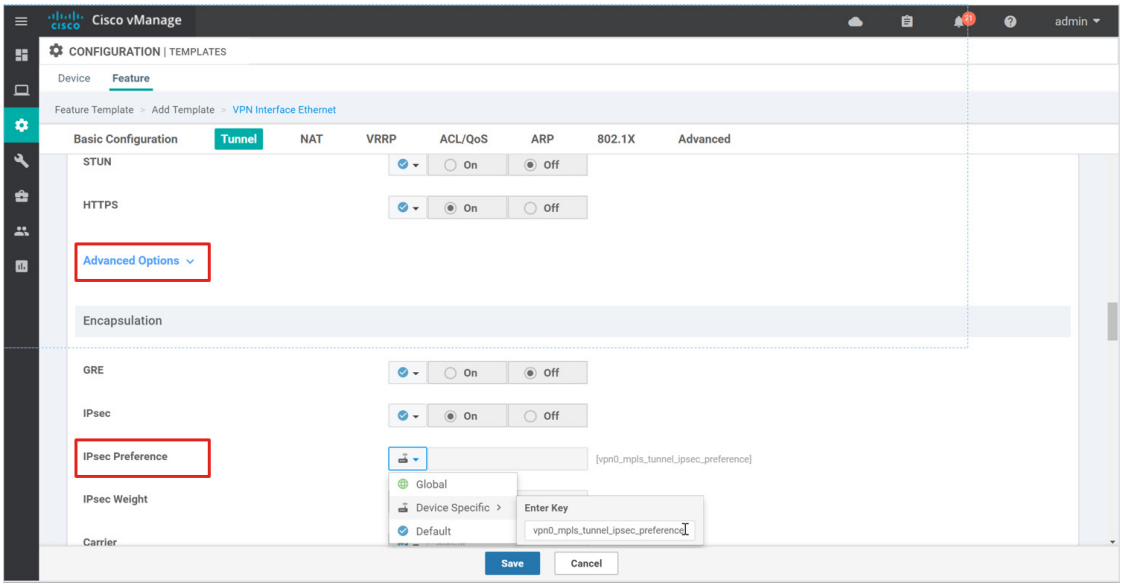
21. 在**基本配置**下的**上行带宽**旁边，选择**特定设备专用**，并输入变量名称 **vpn0_mpls_int_bandwidth_up**。在**下行带宽**旁边，选择**特定设备专用**并输入变量名称 **vpn0_mpls_int_bandwidth_down**。设置这两个变量后，在带宽利用率达到 85% 或高于配置的带宽时，系统将发送 vManage 通知、简单网络管理协议 (SNMP) 陷阱和日志记录消息。

22. 在**隧道**下的**隧道接口**旁边，选择**全局**，然后选择**开启**。选择**开启**之后，系统将为隧道显示更多参数。在**颜色**旁边，选择**全局**，然后从下拉文本框中选择 **mpls**。在**限制**旁边，选择**全局**，然后选择**开启**。这种限制意味着只与相同颜色的其他终端形成隧道。

如果是广域网边缘设备，默认情况下，在启用隧道后，物理接口接受 DTLS/TLS 和 IPSec 流量。此外，还可以启用其他服务并将其加入未加密的物理接口，默认情况下这包括 DNS、DHCP、HTTPS 和互联网控制消息协议 (ICMP)。其他协议包括 SSH、NETCONF、NTP、BGP、OSPF 和 STUN。它是一种最佳安全实践，用于最大限度减少允许通过的协议。在示例网络中，出于初始故障排除目的，ICMP 保持启用并且 DHCP 对 MPLS 接口保持关闭，因为该接口上的 IP 地址是静态的。由于 MPLS 传输链路可以通过数据中心到达互联网，因此允许 NTP 和 DNS 通过。

23. 在**隧道**和**允许服务**部分的 **DHCP** 旁边，选择**全局**，然后选择**关闭**。在 **NTP** 旁边，选择**全局**，然后选择**开启**。

24. 在**允许服务**部分下，选择**高级选项**文本。系统显示**封装**部分。在**首选项**旁边，选择**特定设备专用**，并将变量配置为 **vpn0_mpls_tunnel_ipsec_preference**。利用 IPSec 隧道首选项，您可以根据首选项的值在隧道之间选择优先使用哪个隧道。



25. 在**高级**部分的**清除不分段**旁边，选择**全局**，然后选择**开启**。这会清除 DF 位设置，并允许大于接口最大传输单位 (MTU) 的数据包进行分段。

26. 按**保存**按钮以创建模板。

下表总结了该功能模板中配置的参数：

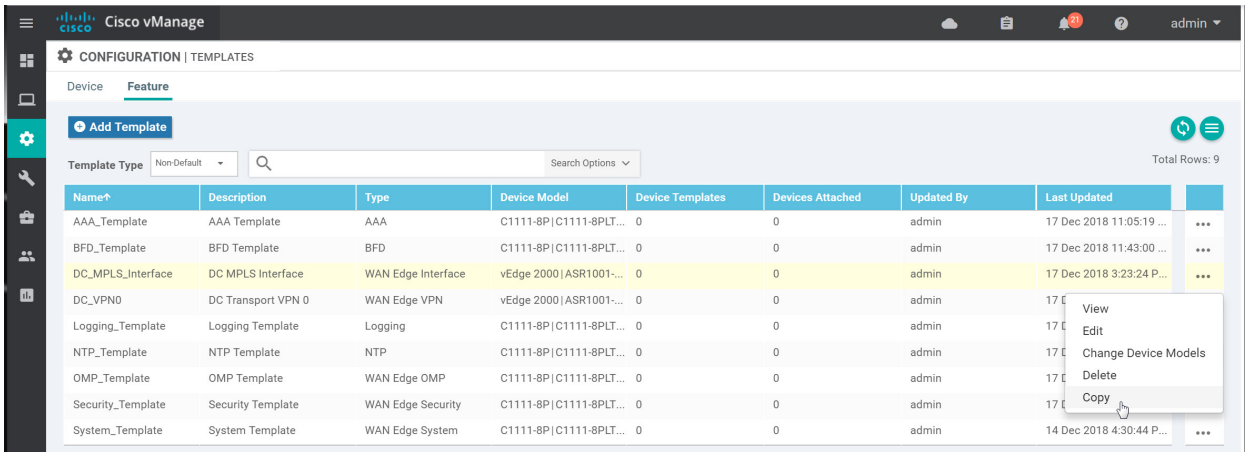
VPN 0 VPN 接口以太网功能模板设置 (MPLS)

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启
	允许服务 > DHCP	全局	关闭
	允许服务 > NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

接下来，在传输端 VPN 下配置互联网接口。该模板应该与 MPLS VPN 接口模板非常相似，但变量名称不同。

VPN 接口（互联网）

27. 假设您仍在**功能模板**页面上，找到刚刚创建的功能模板 (**DC_MPLS_Interface**)，并选择最右侧的 **...**。选择**复制**。

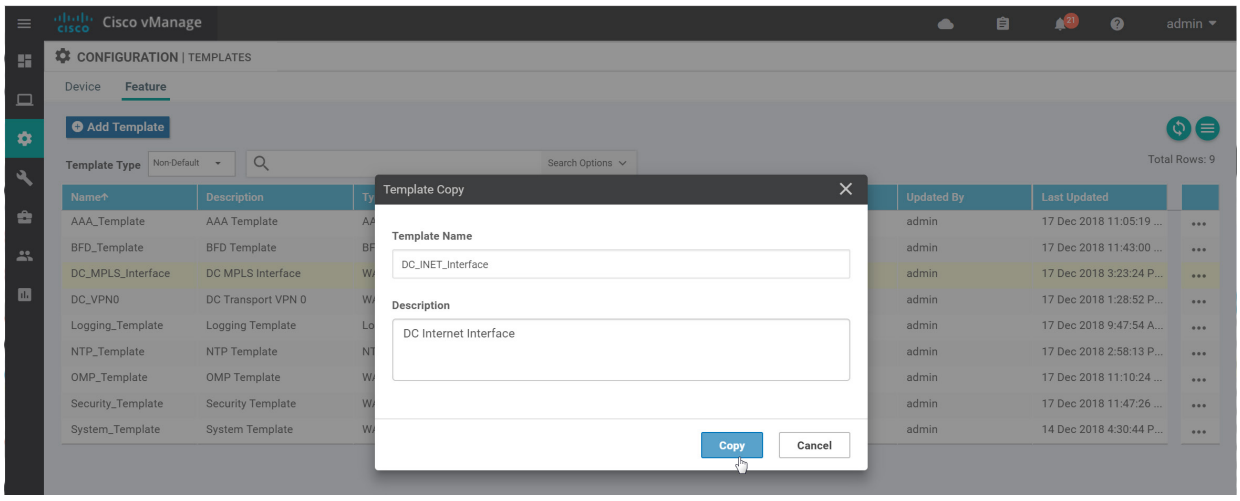


28. 在弹出窗口中，如下定义模板名称和说明：

    模板名称：**DC_INET_Interface**

    说明：**数据中心互联网接口**

29. 选择**复制**按钮。功能模板即已创建，并与已创建的其他功能模板一起显示在列表中。



30. 选择新创建的功能模板 (**DC_INET_Interface**) 右侧的 **...**，然后选择**编辑**以修改模板。

31. 修改接口说明、变量和隧道颜色。

下表总结了该功能模板中的参数。

VPN 0 VPN 接口以太网功能模板设置（互联网）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
基本配置	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
	限制	全局	关闭
	允许服务 > DHCP	全局	关闭
	允许服务 > NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
高级	清除不分段	全局	开启

32. 执行配置更改后，选择**更新**按钮以保存对功能模板的更改。

程序 7：配置管理 VPN（可选）

这将配置带外管理 VPN。此 VPN 始终是 VPN 512，而且此 VPN 不能用于任何其他用途。此模板可应用于任何广域网边缘路由器。

1. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。使用以下设备类型、模板类型、模板名称和说明创建 VPN 512 模板：

   选择设备：除 vManage 和 vSmart 之外的所有设备

   模板：VPN/VPN

   模板名称：VPN512_Template

   说明：VPN 512 带外管理

2. 配置下表中列出的参数。

VPN512 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	512
	名称	全局	管理 VPN
IPv4 路由/新建 IPv4 路由	前缀	全局	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn512_mgt_next_hop_ip_addr

3. 选择**保存**以创建功能模板。

接下来，需要配置管理 VPN 下的接口。

VPN 接口 (VPN512)

4. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。
5. 使用以下设备类型、模板类型、模板名称和说明创建 VPN 512 接口模板：

   选择设备：除 vManage 和 vSmart 之外的所有设备

   模板：VPN/VPN 接口以太网

   模板名称：VPN512_Interface

   说明：VPN 512 管理接口

6. 配置下表中列出的参数。

VPN512 接口功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	全局	否
	接口名称	特定设备专用	vpn512_mgt_int_x|x
	说明	全局	管理接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn512_mgt_int_ip_addr|maskbits

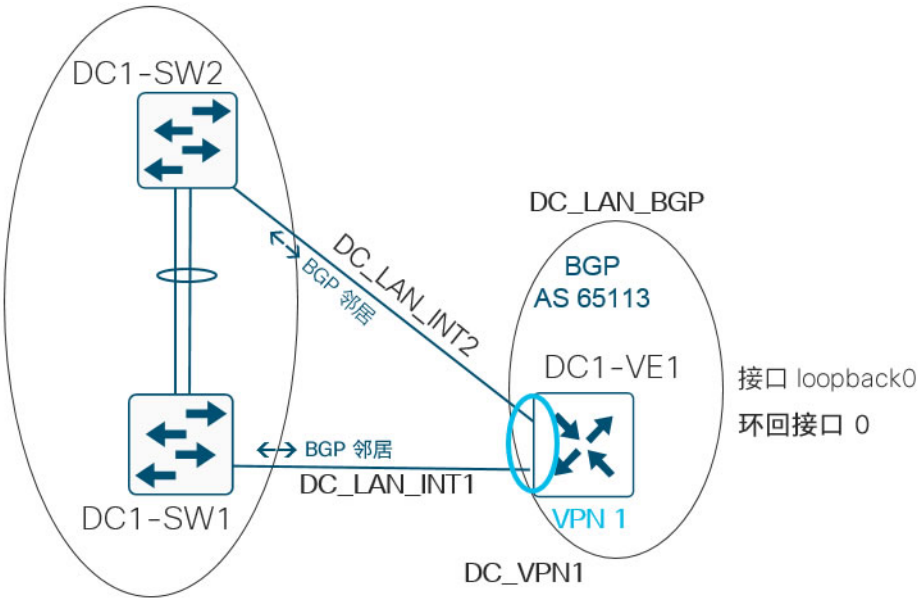
通过将接口名称定义为变量，就只需使用一个模板，并且可以将此模板应用于多种类型的广域网边缘设备，因为不同的型号类型会使用不同的管理端口接口。例如，vEdge 1000、2000 和 5000 路由器都使用内置的 mgmt0，vEdge 100 使用常规以太端口（在本示例网络中为 ge0/1），而 IOS XE SD-WAN 路由器则使用 GigabitEthernet0。

7. 按**保存**按钮以创建模板。

程序 8：配置服务端 VPN

配置本地服务端或面向局域网的网络。此网络将连接到数据中心的广域网分布式交换机/汇聚交换机。此服务 VPN 需要三个 VPN 以太网 VPN 模板，因为您无法在同一个 VPN 中将某个模板重复使用两次，而且局域网接口需要两个模板，使用系统 IP 地址定义的 loopback0 接口需要一个模板。此外还需要一个 BGP 模板与数据中心中已在运行 BGP 的交换机连接。BGP 重新分发到 OMP，从而使远程站点可以访问数据中心。

图 14　数据中心 vEdge 服务模板



服务端 VPN 1

1. 依次选择**配置 > 模板**，然后选择**功能**选项卡。选择**添加模板**按钮。
2. 使用以下设备类型、模板、模板名称和说明创建 VPN 1 模板：

   选择设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

   模板：VPN/VPN

   模板名称：DC_VPN1

   说明：数据中心服务端 VPN 1

3. 配置下表中列出的参数。

数据中心 VPN 1 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	1
	名称	全局	服务端 VPN 1
	增强 ECMP 键控	全局	开启
通告 OMP	BGP	全局	开启

利用**通告 OMP** 配置，BGP 路由将被重新分发到 OMP 中，使远程站点可以访问数据中心和服务端路由。

4. 选择**保存**以创建模板。

VPN 接口以太网 1

5. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。

6. 使用以下设备类型、模板类型、模板名称和说明创建创建第一个 VPN 1 接口模板：

   选择设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

   模板：VPN/VPN 接口以太网

   模板名称：DC_LAN _INT1

   说明：数据中心局域网接口 1

7. 配置下表中列出的参数。

数据中心 VPN 接口功能模板设置（接口 1）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits

8. 选择**保存**以完成模板。

VPN 接口以太网 2

9. 假设您仍在**功能模板**页面上，找到刚刚创建的功能模板 (**DC_LAN_INT1**)，并选择最右侧的 **...**。选择**复制**。

10. 在弹出窗口中，如下定义**模板名称**和**说明**:

    模板名称：DC _LAN_INT2

    说明：数据中心局域网接口 2

11. 选择**复制**按钮。功能模板即已创建，并与已创建的其他功能模板一起显示在列表中。

12. 选择新创建的功能模板 (**DC_LAN_INT2**) 右侧的 **...**，然后选择**编辑**以修改模板。

13. 修改接口变量。

下表总结了该功能模板中的参数。

数据中心 VPN 接口功能模板设置（接口 2）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr|maskbits

14. 执行配置更改后，选择**更新**按钮以保存对功能模板的更改。

VPN 接口以太网 Loopback0

创建具有系统 IP 地址的 loopback0 接口，以便从系统 IP 地址发出日志记录、SNMP 和其他管理流量，简化与 vManage 的关联。此模板可以在所有设备类型之间共享。

15. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。

16. 使用以下设备类型、模板类型、模板名称和说明创建 loopback0 接口模板:

    选择设备：除 vManage 和 vSmart 之外的所有设备

    模板：VPN/VPN 接口以太网

    模板名称：Loopback0

    说明：环回接口 0

17. 配置下表中列出的参数。

VPN 接口以太网功能模板设置（环回接口 0）

部分	参数	类型	变量/值
基本配置	关闭	全局	否
	接口名称	全局	loopback0
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lo0_int_ip_addr|maskbits

18. 选择**保存**以完成模板。

边界网关协议 (BGP)

配置服务端 VPN 中的 BGP。在配置中，OMP 重新分发到 BGP，从而使数据中心可以访问远程站点。启用名为 “传播 AS 路径” 的功能设置，将 BGP AS 路径信息传输到 OMP，而 OMP 可将此信息传递到启用了 BGP 的其他站点，以防出现环路。

技术提示：在 16.11.1 版之前，IOS XE SD-WAN 软件不支持传播 AS 路径功能。

19. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。

20. 使用以下设备类型、模板类型、模板名称和说明创建 BGP 模板：

    选择设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

    模板：其他模板/BGP

    模板名称：DC_LAN_BGP

    说明：数据中心局域网 BGP 模板

21. 在**基本配置**部分下，配置下表中列出的参数。

BGP 功能模板基本配置设置

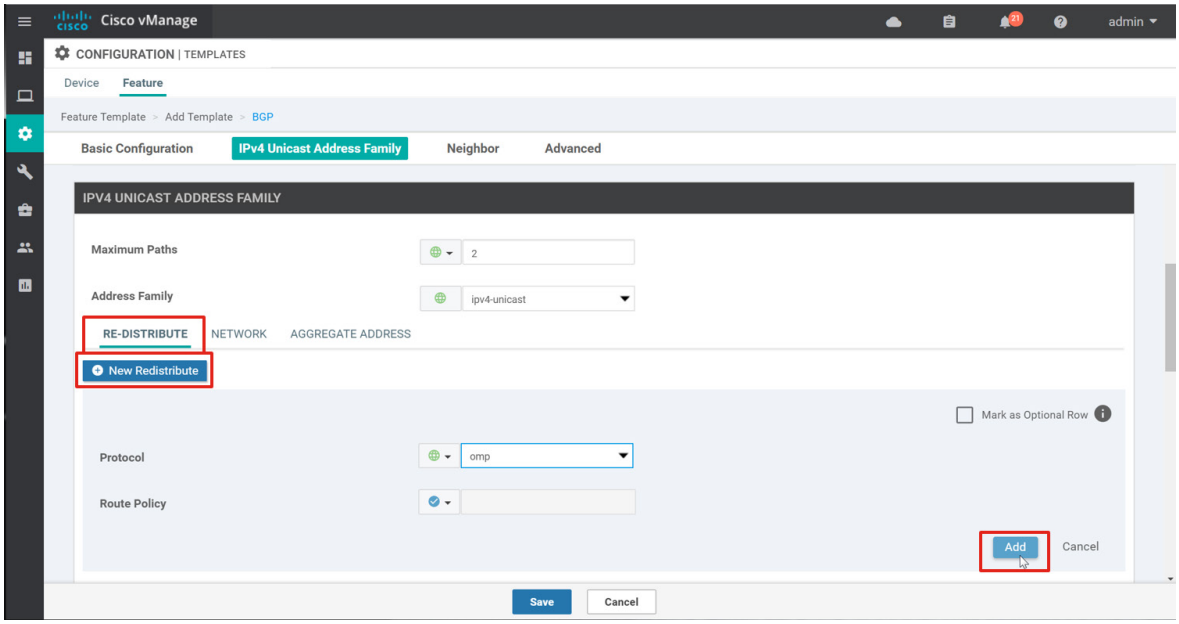
部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_bgp _shutdown
	AS 编号	特定设备专用	lan_bgp_as_num
	路由器 ID	特定设备专用	lan_bgp_as_num
	传播 AS 路径	全局	开启

22. 配置 BGP 模板的 **IPv4 单播地址系列**部分。在**最大路径数**旁边，选择**全局**，然后在文本框中输入 **2**。

23. 在**地址系列**旁边，从下拉列表框中选择 **ipv4 单播**。

24. 在**重新分发**选项卡（默认选项卡）中，点击**新建重新分发**按钮。此配置区域允许将多个协议重新分发到 BGP。在本例中将重新分发 OMP。

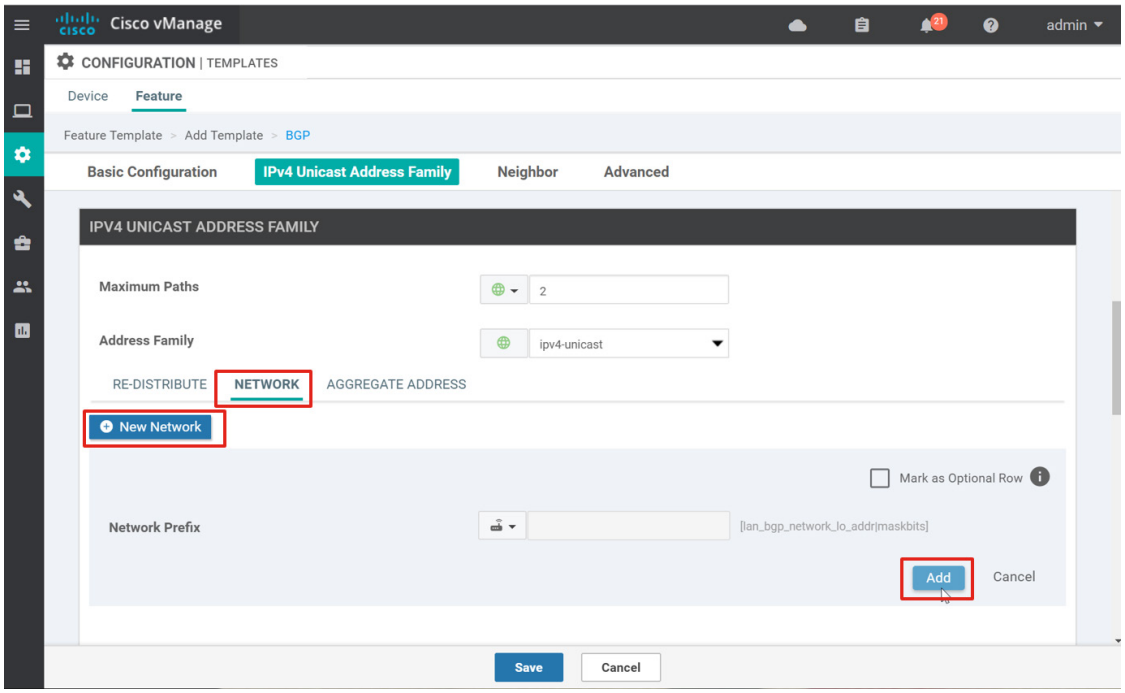
25. 在**协议**旁边，从下拉列表框中选择 **omp**，然后点击**添加**按钮。



26. 此示例中的 loopback0 地址将通过配置 network 语句在 BGP 中进行通告。选择**网络**选项卡，然后点击**新建网络**按钮。

27. 在**网络前缀**旁边，选择**特定设备专用**，然后在文本框中输入变量名称 **lan_bgp_network_lo_addr|maskbits**。

28. 点击**添加**按钮。



BGP 功能模板 IPv4 单播地址系列配置设置

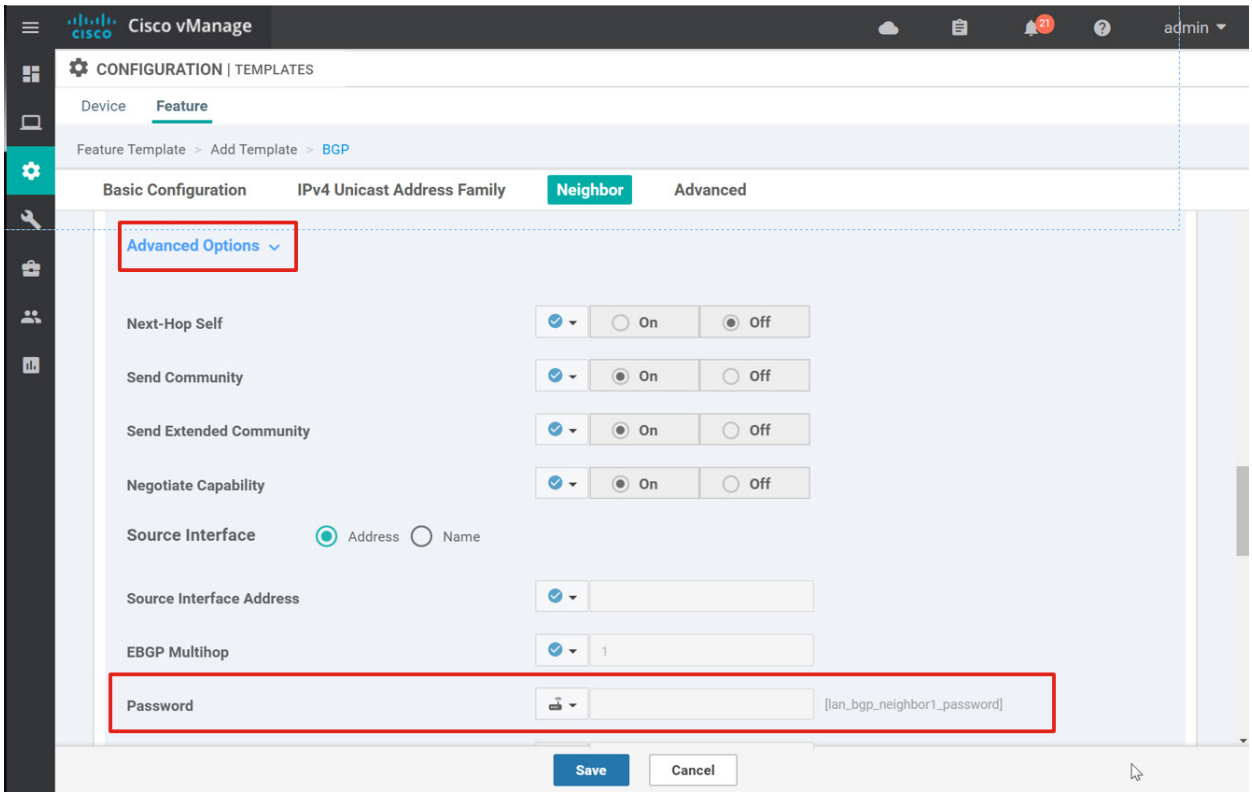
部分	参数	类型	变量/值
IPv4 单播地址系列	最大路径数	全局	2
	地址系列	下拉列表	ipv4 单播
	重新分发/协议	下拉列表	omp
	网络/网络前缀	特定设备专用	bgp_network_lo_addr|maskbits

29. 配置 BGP 模板的**邻居**部分。点击**新建邻居**按钮并配置下表中列出的参数。点击**高级选项**文本以显示高级参数选项。

BGP 功能模板邻居 1 配置设置

部分	参数	类型	变量/值
邻居 (1)	地址	特定设备专用	lan_bgp_neighbor1_addr
	说明	特定设备专用	lan_bgp_neighbor1_description
	远程 AS	特定设备专用	lan_bgp_neighbor1_remote_as
	地址系列	全局	开启
	地址系列	全局	ipv4 单播
	关闭	特定设备专用	lan_bgp_neighbor1_shutdown

部分	参数	类型	变量/值
	高级选项/密码	特定设备专用	lan_bgp_neighbor1_password
	高级选项/保持时间（秒）	全局	3
	高级选项/保持时间（秒）	全局	9



30. 点击**添加**按钮将邻居配置添加到模板中。

31. 重复前两个步骤，添加第二个 BGP 邻居的配置。配置下表中列出的参数。

BGP 功能模板邻居 2 配置设置

部分	参数	类型	变量/值
邻居 (2)	地址	特定设备专用	lan_bgp_neighbor2_addr
	说明	特定设备专用	lan_bgp_neighbor2_description
	远程 AS	特定设备专用	lan_bgp_neighbor2_remote_as
	地址系列	全局	开启
	地址系列	下拉列表	ipv4 单播

部分	参数	类型	变量/值
	关闭	特定设备专用	lan_bgp_neighbor2_shutdown
	高级选项/密码	特定设备专用	lan_bgp_neighbor2_password
	高级选项/保持时间（秒）	全局	3
	高级选项/保持时间（秒）	全局	9

32. 点击**添加**按钮将邻居配置添加到模板中。

33. 选择**保存**以创建模板。

程序 9：配置其他模板（可选）

您可以创建一个横幅和一个 SNMP 功能模板。

横幅

有两种横幅：一种在 CLI 用户名/登录提示之前显示（即登录横幅）；一种在成功登录后显示（即当日消息 [MOTD] 横幅）。配置 MOTD 横幅。

1. 依次选择**配置 > 模板**，然后选择**功能**选项卡。选择**添加模板**按钮。
2. 使用以下设备类型、模板类型、模板名称和说明创建横幅模板：

   选择设备：除 vManage 和 vSmart 之外的所有设备

   模板：其他模板/横幅

   模板名称：Banner_Template

   说明：横幅模板

3. 配置下表中列出的参数。

横幅功能模板设置

部分	参数	类型	变量/值
基本配置	MOTD 横幅	全局	这是专用网络。它仅供在获得授权的情况下使用。

4. 选择**保存**以创建模板。

SNMP

技术提示：目前，IOS-XE SD-WAN 代码不支持 SD-WAN 特定 MIB 和陷阱，只支持 IOS MIB 和陷阱。

5. 假设您仍在**功能模板**页面上，请选择**添加模板**按钮。
6. 使用以下设备类型、模板、模板名称和说明创建 SNMP 模板：

   选择设备：除 vManage 和 vSmart 之外的所有设备

   模板：其他模板/SNMP

   模板名称：SNMP_Template

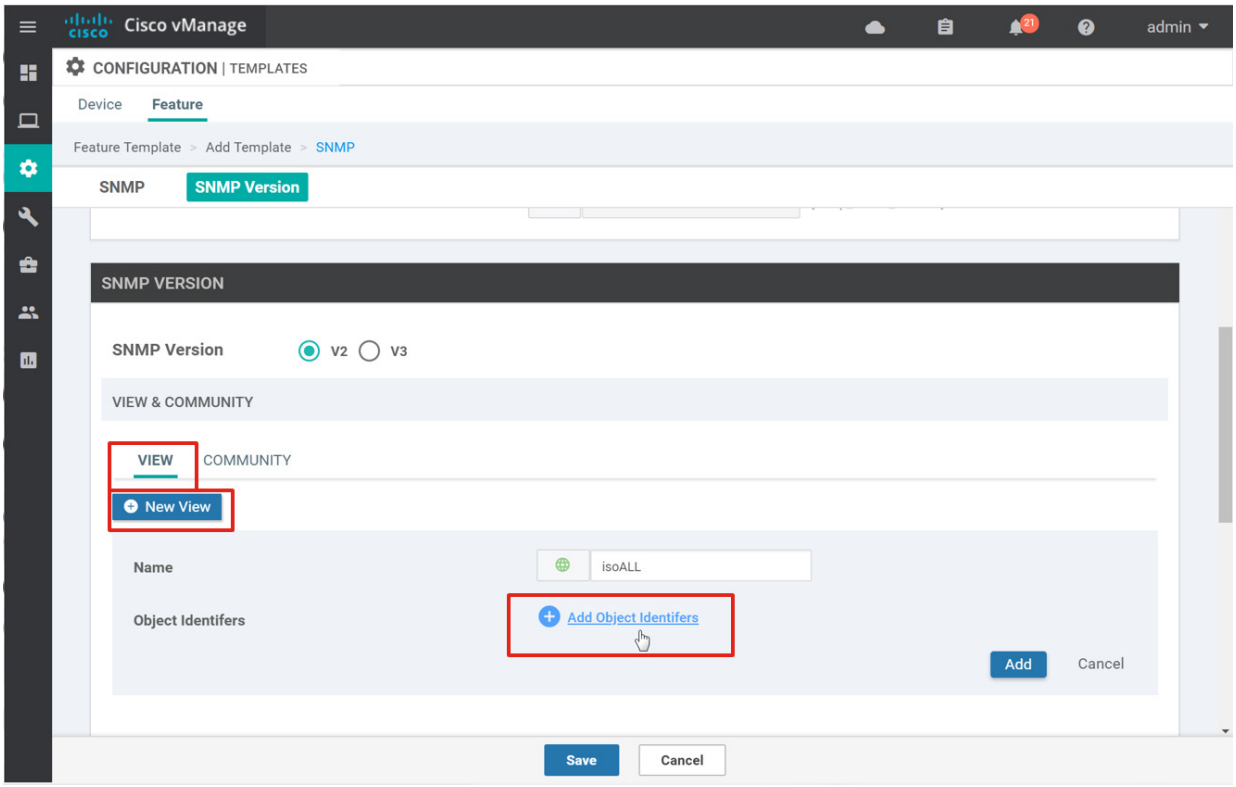
   说明：SNMP 模板

7. 配置下表中列出的基本配置参数。

SNMP **功能模板基本配置设置**

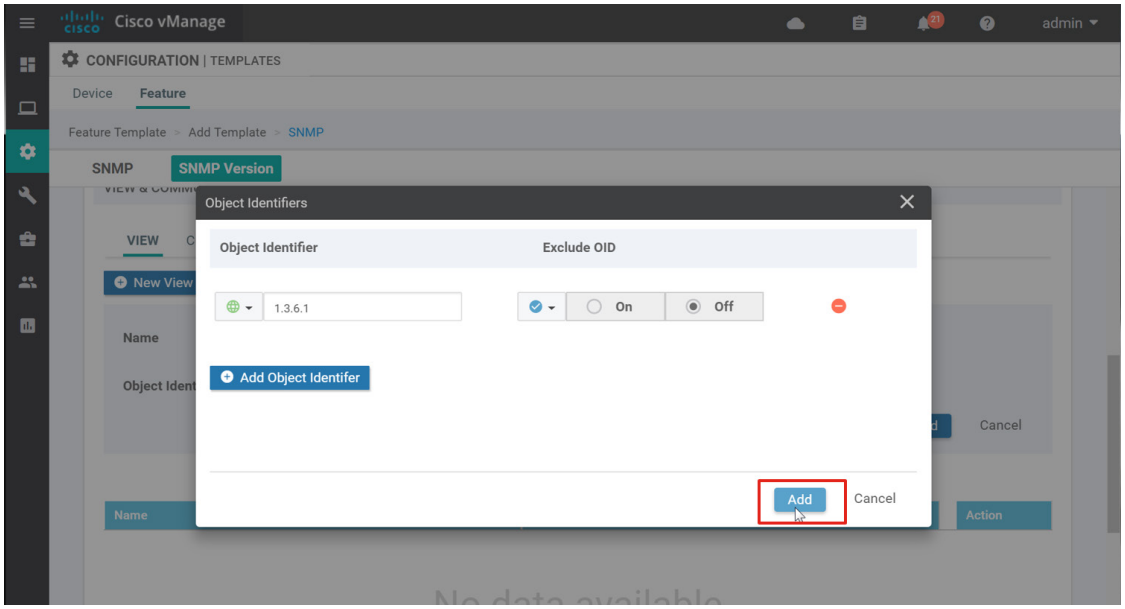
部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	snmp_shutdown
	SNMP 的设备名称	特定设备专用	snmp_device_name
	设备位置	特定设备专用	snmp_device_location

8. 配置模板的 **SNMP 版本**部分。在 **SNMP 版本**旁边，确保选择 **V2**。在**视图**选项卡的**视图和社区**下，点击**新建视图**按钮。
9. 在**名称**旁边的文本框中，输入 **isoALL**。
10. 点击**添加对象标识符**文本。



11. 系统将弹出一个窗口，指示您应添加第一个对象标识符。点击**添加对象标识符**按钮。

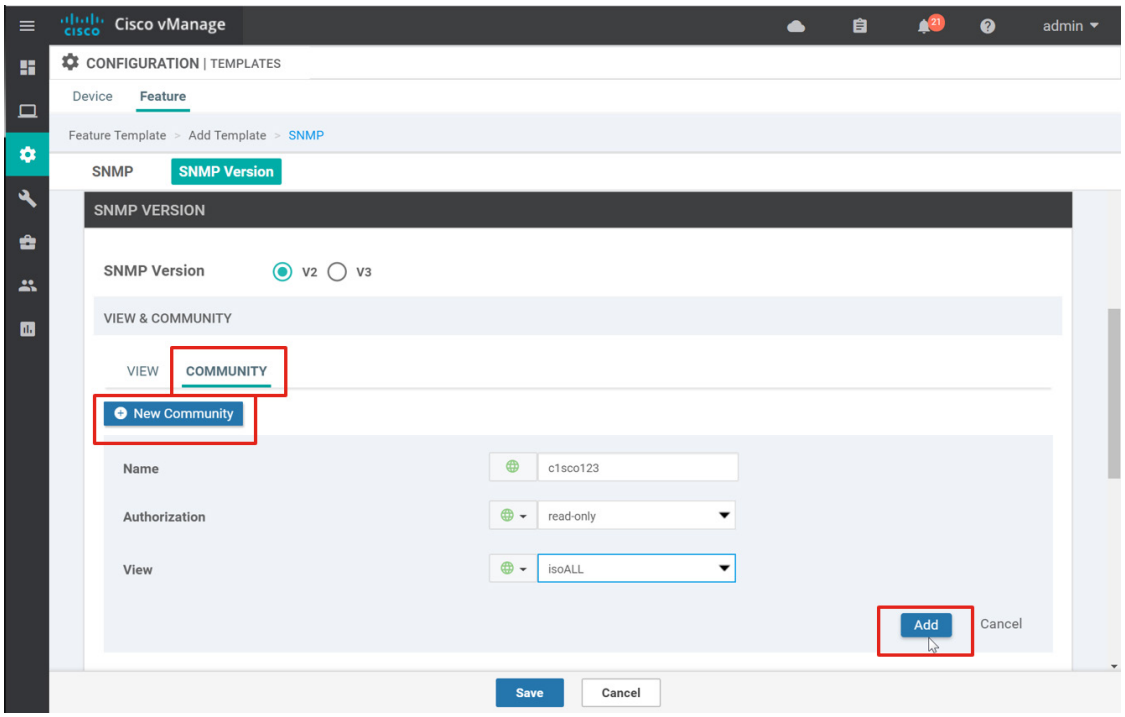
12. 系统将显示**对象标识符**弹出窗口。在文本框中，输入 **1.3.6.1**。然后，点击**添加**按钮。



13. 在主要功能模板页面上，点击**添加**按钮将 **isoALL** 视图保存到模板中。

14. 在**视图和社区**部分下，选择**社区**选项卡，然后点击**新建社区**按钮。输入社区**名称** (**c1sco123**)，选择**授权**（**只读**），然后选择刚刚创建的**视图** (**isoALL**)。

15. 点击**添加**按钮将社区设置保存到模板中。

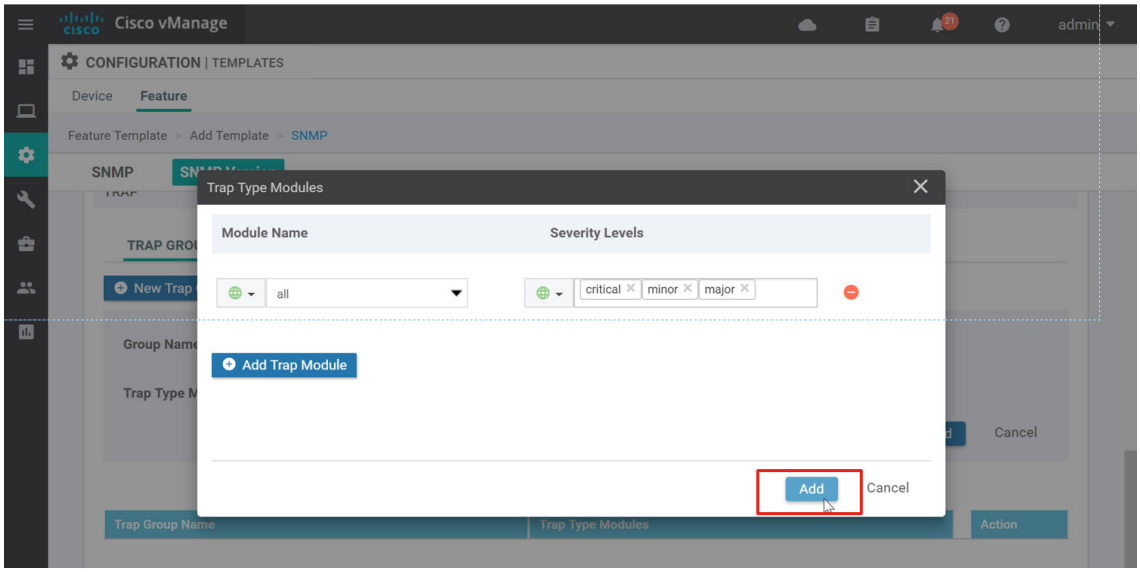


16. 在**陷阱**部分下，选择**陷阱组**选项卡，然后点击**新建陷阱组**按钮。输入**组名称** (**SNMP-GRP**)，然后点击**添加陷阱类型模块**文本。

17. 系统将弹出一个窗口，指示您添加第一个陷阱模块。点击**添加陷阱模块**按钮。

18. 从下拉列表框中选择**模块名称** (**all**) 和**严重性级别**（**严重、重要、次要**）。

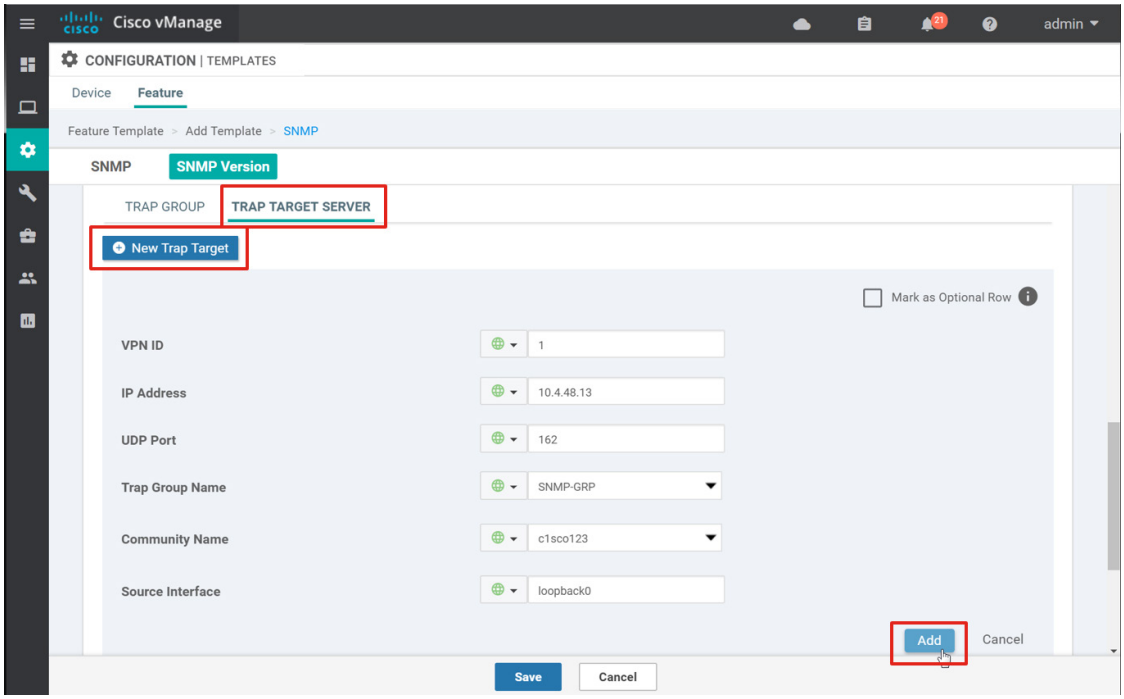
19. 点击**添加**按钮。



20. 转到主要功能模板页面后，点击**添加**按钮以将陷阱组保存到模板中。

21. 在**陷阱**部分下，选择**陷阱目标服务器**选项卡，然后点击**新建陷阱目标**按钮。输入 SNMP 陷阱服务器的 **VPN ID** (1)、**IP 地址** (10.4.48.13) 和 **UDP 端口** (162)、**陷阱组名称** (SNMP-GRP) 和**社区名称** (c1sco123)。在**源接口**旁边，从下拉列表框中选择**全局**，然后输入 loopback0。

22. 点击**添加**按钮。



23. 选择**保存**以创建模板。

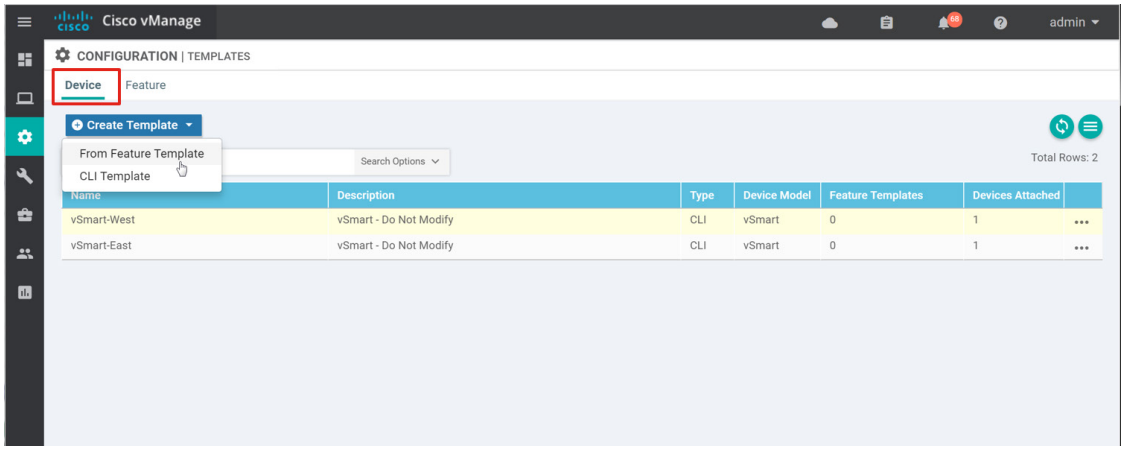
SNMP 功能模板视图、社区和陷阱设置

部分	参数	类型	变量/值
SNMP 版本	SNMP 版本	单选按钮	V2
SNMP 版本/视图和社区	视图/名称	全局	isoALL
	视图/对象标识符	全局	1.3.6.1
	社区/名称	全局	c1sco123
	社区/授权	全局/下拉列表	只读
	社区/视图	全局	isoALL
SNMP 版本/陷阱	陷阱组/组名称	全局	SNMP GRP
	陷阱组/陷阱类型模块/模块名称	全局	all
	陷阱组/陷阱类型模块/严重性级别	全局	严重、重要、次要
	陷阱目标服务器/VPN	全局	1
	陷阱目标服务器/IP 地址	全局	10.4.48.13
	陷阱目标服务器/UDP 端口	全局	162
	陷阱目标服务器/陷阱组名称	全局	SNMP GRP
	陷阱目标服务器/社区名称	全局	c1sco123
	陷阱目标服务器/源接口	全局	loopback0

程序 10：创建设备模板

在此程序中，您需要创建一个引用刚创建的功能模板的设备模板。

1. 在 vManage GUI 中，依次转到**配置 > 模板**，并确保选择**设备**选项卡（默认选项卡）。
2. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。



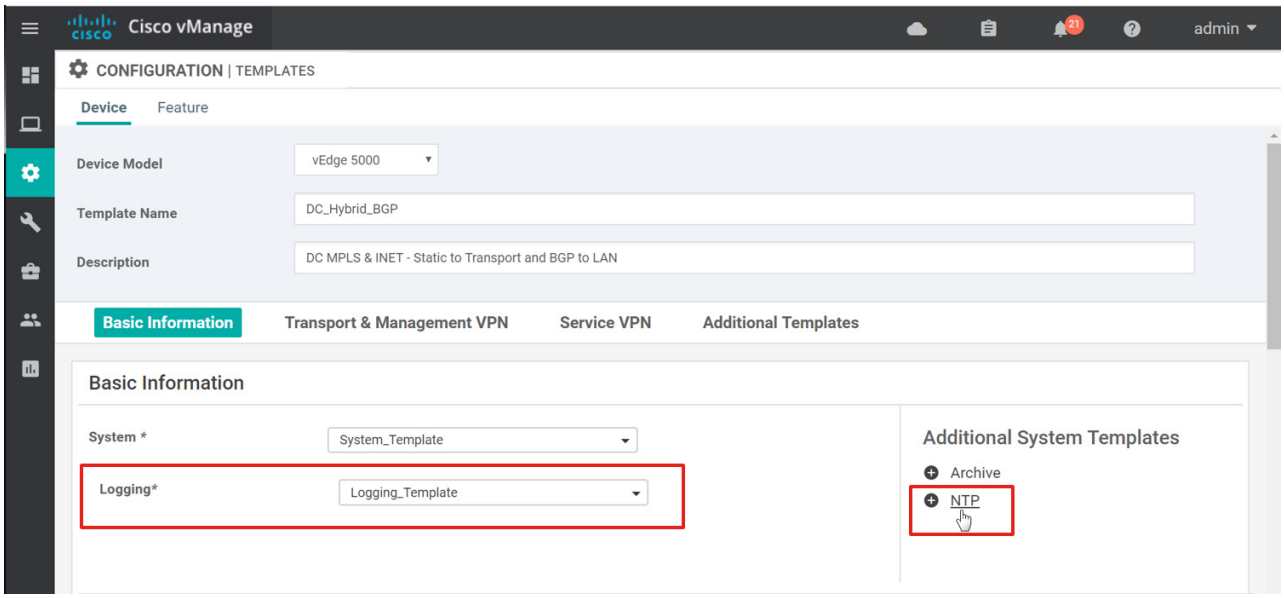
3. 从下拉列表框中选择**设备型号** (vEdge 5000)。

4. 填写**模板名称** (**DC_Hybrid_BGP**)，并在**说明**字段为其提供说明（**数据中心 MPLS 和 INET – 传输静态和局域网 BGP**）。默认情况下，设备模板中需要功能模板的区域都预填了默认模板。

5. 在**基本信息**下的**系统**旁边，从下拉列表框中选择功能模板 **System_Template**。

6. 在**日志记录**旁边，从下拉列表框中选择功能模板 **Logging_Template**。

7. 对于 NTP，首先需要将此功能添加到设备模板中。在**其他系统模板**下，点击 **NTP**，然后从下拉列表框中选择功能模板 **NTP_Template**。



8. 在 AAA 旁边，从下拉列表框中选择功能模板 **AAA_Template**。

9. 对 BFD (BFD_Template)、OMP (OMP_Template) 和安全 (Security_Template) 模板重复最后一步。

设备模板基本信息部分

模板类型	模板名称
系统	System_Template
日志记录	Logging_Template
NTP	NTP_Template
AAA	AAA_Template
OMP	OMP_Template
BFD	BFD_Template
安全	Security_Template

10. 在**传输和管理 VPN** 部分下，选择右侧**其他 VPN 0 模板**下的 **VPN 接口**。此操作会在**传输端 VPN** 下添加第二个 VPN 接口。在 **VPN 0** 下拉列表框下以及 VPN 0 下的每个 **VPN 接口**下拉列表框下，选择新创建的功能模板。

11. 对于 VPN 512，在 **VPN 512** 下拉列表框下以及 **VPN 512** 下的 **VPN 接口**下拉列表框下，选择新创建的功能模板。

设备模板的传输和管理 VPN **部分**

模板类型	模板子类型	模板名称
VPN0		DC_VPN0
	VPN 接口	DC_MPLS_Interface
	VPN 接口	DC_INET_Interface
VPN 512		VPN512_Template
	VPN 接口	VPN512_Interface

12. 在**服务端 VPN** 部分下，将鼠标悬停在 **+ 服务端 VPN** 文本上。系统将显示一个窗口，您可以在其中的文本框中输入您想要创建的服务端 VPN 数量。

13. 选择 **1**，然后按回车键。系统将添加一个 **VPN** 下拉列表框。在右侧**其他 VPN 模板**中，选择 **VPN 接口**三次（用于两个局域网接口和 Loopback0 定义），然后选择 **BGP** 模板。

14. 为添加的每个下拉列表框选择新创建的功能模板。

设备模板的服务端 VPN 部分

模板类型	模板子类型	模板名称
VPN1		DC _VPN1
	BGP	DC_LAN_BGP
	VPN 接口	DC_LAN_INT1
	VPN 接口	DC_LAN_INT2
	VPN 接口	Loopback0

15. 在**其他模板**部分下，为每个下拉列表框（横幅和 SNMP）选择新创建的功能模板。本地化策略尚未创建，因此在**策略**旁边的下拉列表框中尚无任何策略可以引用。此时也没有任何可以引用的**安全策略**。

设备模板的其他模板部分

模板类型	模板名称
横幅	Banner_Template
策略	
安全策略	
SNMP	SNMP_Template

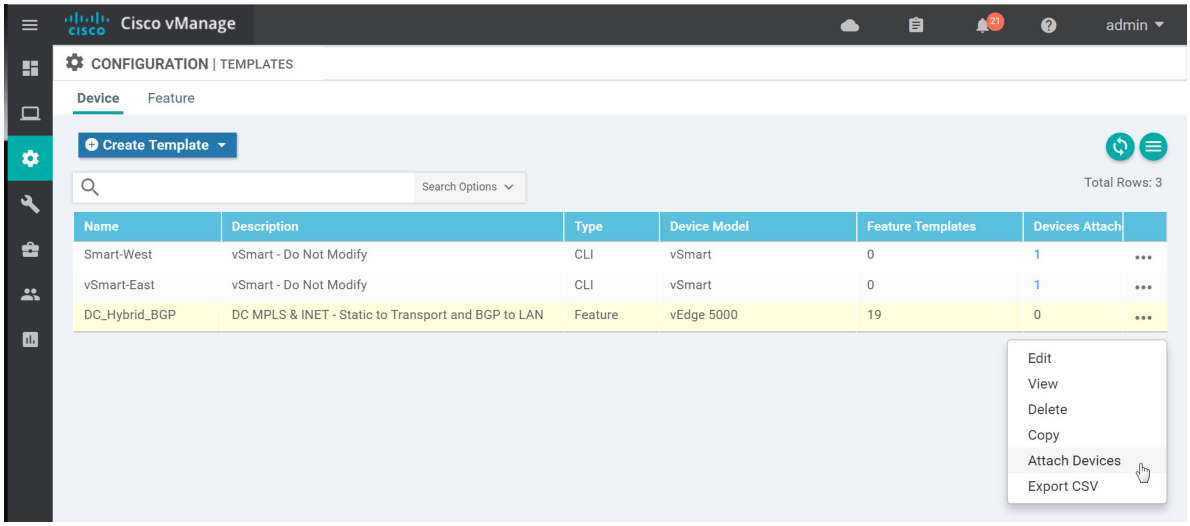
16. 选择**创建**以创建并保存设备模板。

程序 11：将设备模板部署到广域网边缘路由器中

为了将所创建的设备模板部署到广域网边缘路由器中，vManage 根据功能模板构建完整配置，然后将其推送至指定的广域网边缘路由器。在可以构建并推送完整配置之前，需要先定义与设备模板所关联的功能模板相关联的所有变量。可以通过以下两种方式执行此操作：在 GUI 中手动输入变量的值；上传一份包含变量及变量值列表的 .csv 文件。

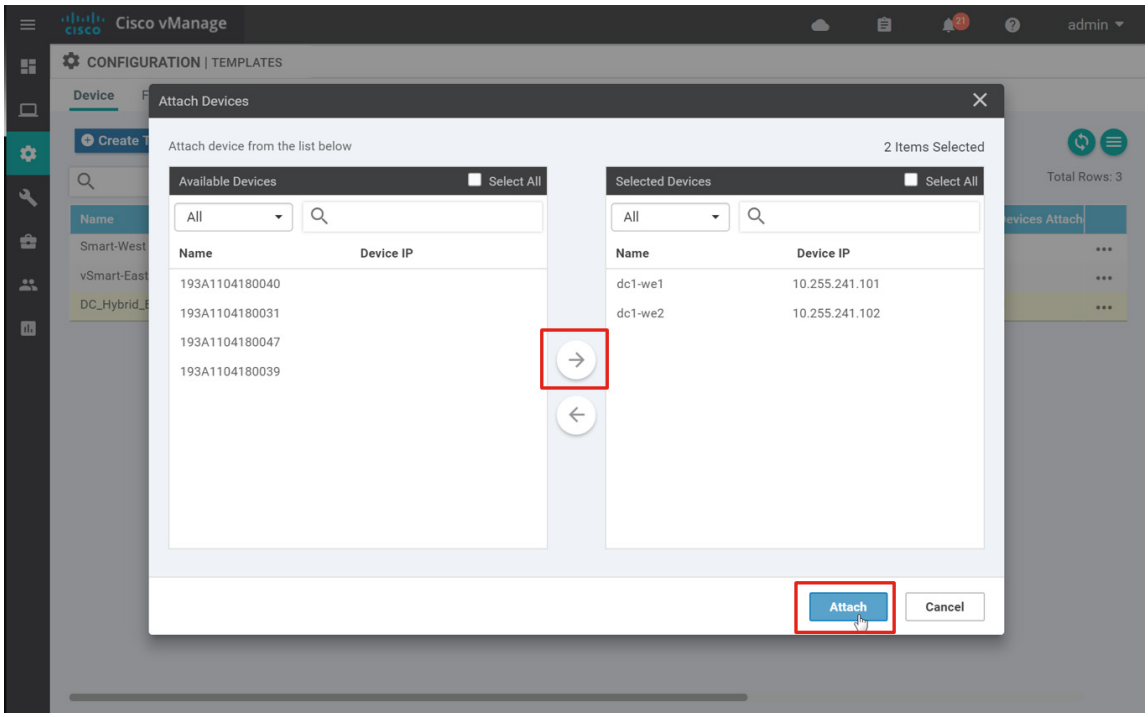
手动输入

1. 依次转到**配置 > 模板**，然后选择**设备**选项卡。找到所需的设备模板 (**DC_Hybrid_BGP**)。选择模板右侧的 **...**，然后选择**关联设备**。

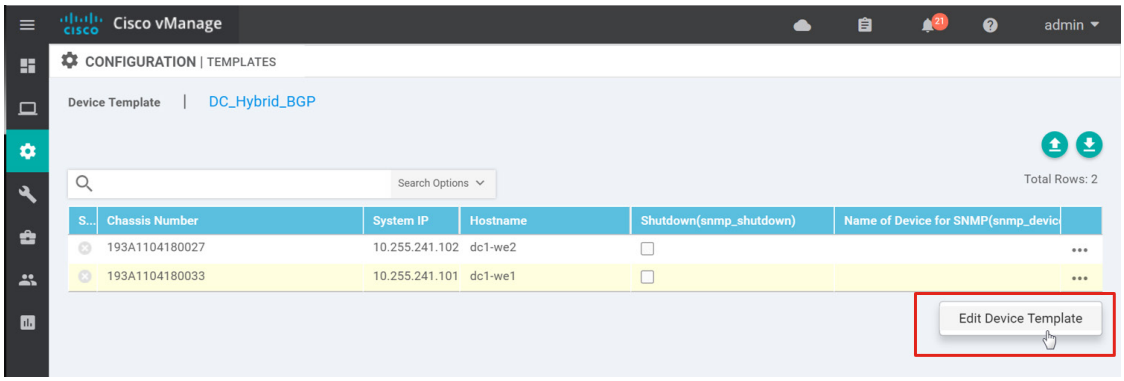


2. 系统将弹出一个窗口，列出可与此配置相关联的设备。如果可以通过 vManage 获知，此可用设备列表中将包含设备主机名和 IP 地址，否则如果设备尚未进入网络并被 vManage 获知，则将包含设备的机箱序列号。在任何情况下，此列表都只包含已在创建模板时定义的设备型号（在本例中为 vEdge 5000）。

3. 选择要应用配置模板的设备，然后选择箭头以将设备从**可用设备**框移到**选定设备**框。一次可以选择多个设备，只需分别点击所需的设备即可。选择**关联**。



4. 系统将显示一个页面，列出您已选择的设备。找到 dc1-we1，然后选择其最右侧的 ...。选择**编辑设备模板**。



5. 系统将弹出一个屏幕，显示一份变量和空文本框的列表。可能还会有变量带有复选框，可以通过选中或取消选中这些复选框来选择值 “开启” 和 “关闭”。在文本框中填入变量的值。由于我们未选择数据中心模板中的任何可选配置，因此必须填写所有文本框，但是可以不选中复选框。对于这些复选框，选中意味着打开，取消选中意味着关闭。如果将文本框字段留空，则在您尝试进入下一页时文本框将突出显示。填写下表中列出的变量。

数据中心广域网边缘设备 1 设备模板变量值

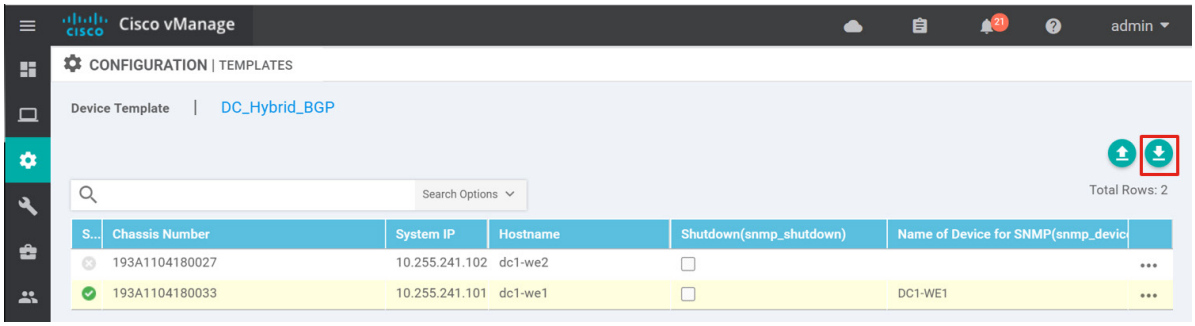
变量	值
Hostname(system_host_name)	dc1-we1
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG3,Primary
System IP(system_system_ip)	10.255.241.101
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
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)	☐

变量	值
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

变量	值
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. 选择**更新**。

7. 变量填写完成后，请选择右上角的下载箭头符号下载 .csv 文件，然后再继续其他操作。



该 .csv file 文件中将填入您到目前为止已填写的值。如果在部署配置时出于任何原因导致某个输入变量出现错误而使配置部署失败，则当您返回此页面时，您先前输入的所有值都将不可用，您需要重新输入这些值。如果您下载了已填写的 .csv 文件，只需选择向上箭头进行上传。然后，您可以选择所需设备右侧的 **...**，并选择**编辑设备模板**，所有最新输入的值将填入文本框中。修改任何输入值，并尝试重新部署。

通过 .csv 文件上传值

8. 在页面右上角，选择下载箭头符号。这将下载 .csv 文件，该文件将按照设备模板命名为 *DC_Hybrid_BGP.csv*。.csv 文件将列出已与模板关联的两台设备，并在每一列中列出必要的变量。由于 dc1-we1 设备已手动填写，因此那些值已填入该电子表格中。

9. 填写 dc1-we2 的变量值，然后保存该 .csv 文件。保存时，请保留 .csv 格式。填写下表中列出的变量值。

数据中心广域网边缘设备 2 设备模板变量值

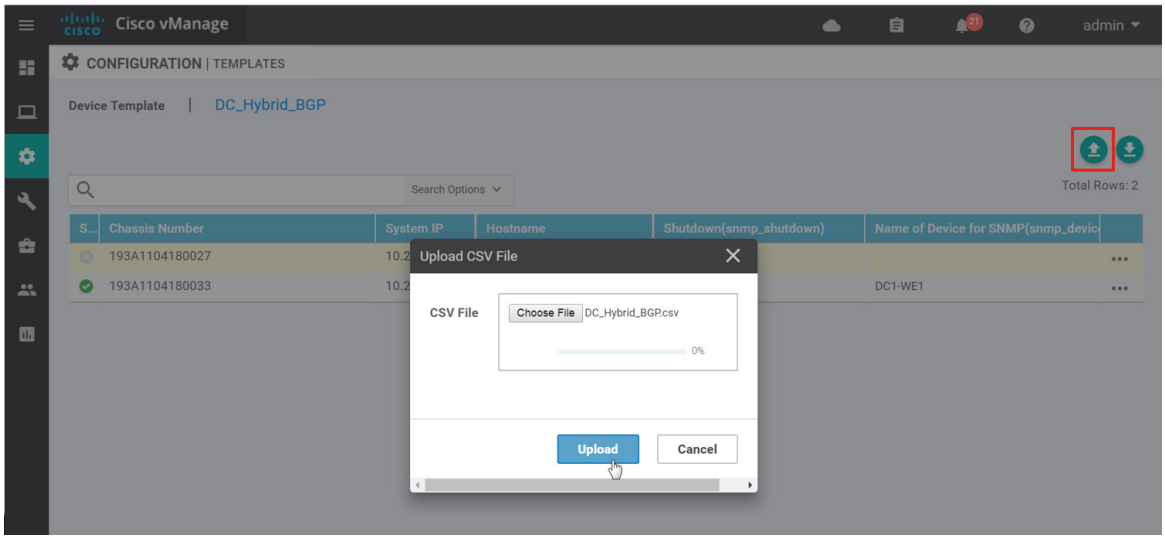
变量	值
Hostname(system_host_name)	dc1-we2
Latitude(system_latitude)	37.409284
Longitude(system_longitude)	-121.928528
Device Groups(system_device_groups)	DC,v5000,US,West,UG2,Secondary
System IP(system_system_ip)	10.255.241.102
Site ID(system_site_id)	110001
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☐
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)	☐

变量	值
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. 选择屏幕右上角的上传箭头以上传 .csv 文件。

11. 系统将弹出一个窗口。选择**选择文件**按钮，然后选择已完成的 .csv 文件以及已保存的变量值。

12. 选择**上传**按钮。屏幕顶部应以绿色显示**文件已成功上传**。



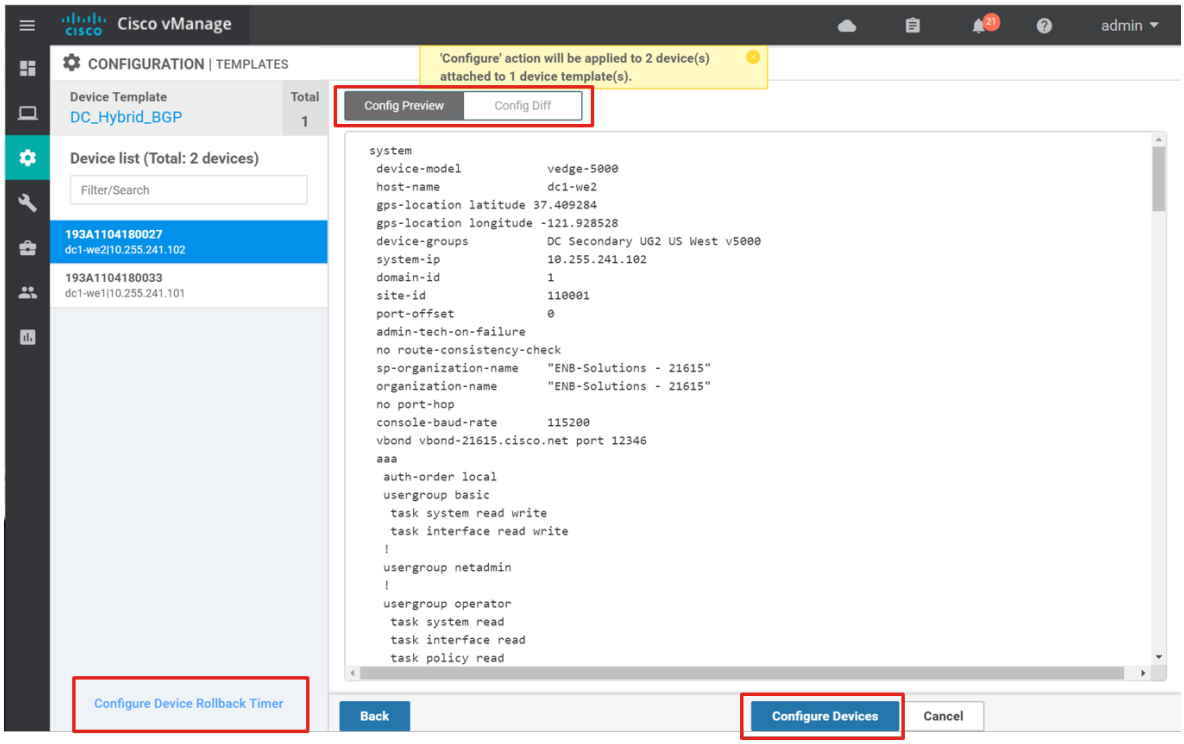
13. 您可以向右滚动并查看或修改已用于输入的变量值。您也可以选择每个设备右侧的 **...**，然后选择**编辑设备模板**以查看所有输入变量并查看或修改变量的值。或者，您还可以上传经过修改的 .csv 文件来修改变量值。

14. 准备好部署后，选择**下一步**按钮。如果您忘记为设备添加值，则会出现错误，在错误得到纠正之前您将无法继续操作。

15. 下一个屏幕会指出，配置操作将应用于关联到一个设备模板的两台设备。选择左侧的设备会显示将要推送到广域网边缘路由器的配置（**配置预览**选项卡）。选择屏幕顶部的**配置差异**选项卡，查看当前本地配置与即将推送的新配置之间的差异。

16. 或者，您也可以选择左下角的**配置设备回滚计时器**文本，查看或更改回滚计时器。默认情况下，此计时器设置为五分钟，这意味着，如果推送配置的操作导致与 vManage 断开连接，则广域网边缘路由器将在五分钟内回滚到先前的配置。您可以更改此计时器并将其设置为介于 6 到 15 分钟之间，或完全禁用它（不推荐）。

17. 回到**配置预览**页面，选择**配置设备**。

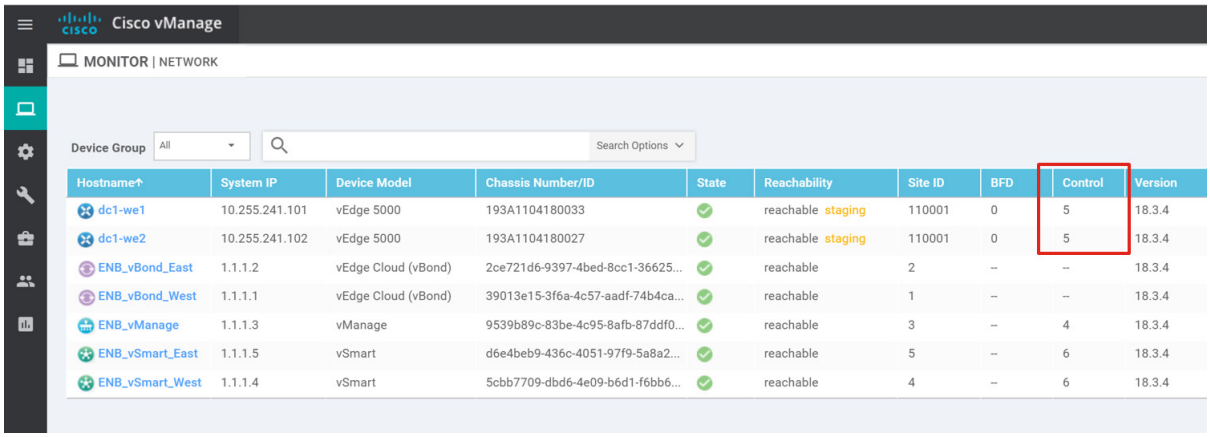


18. 系统会弹出一个窗口并显示以下消息：提交这些更改会影响 2 台设备上的配置。是否确定要继续？选中复选框，确认两个设备上的配置更改。选择确定。

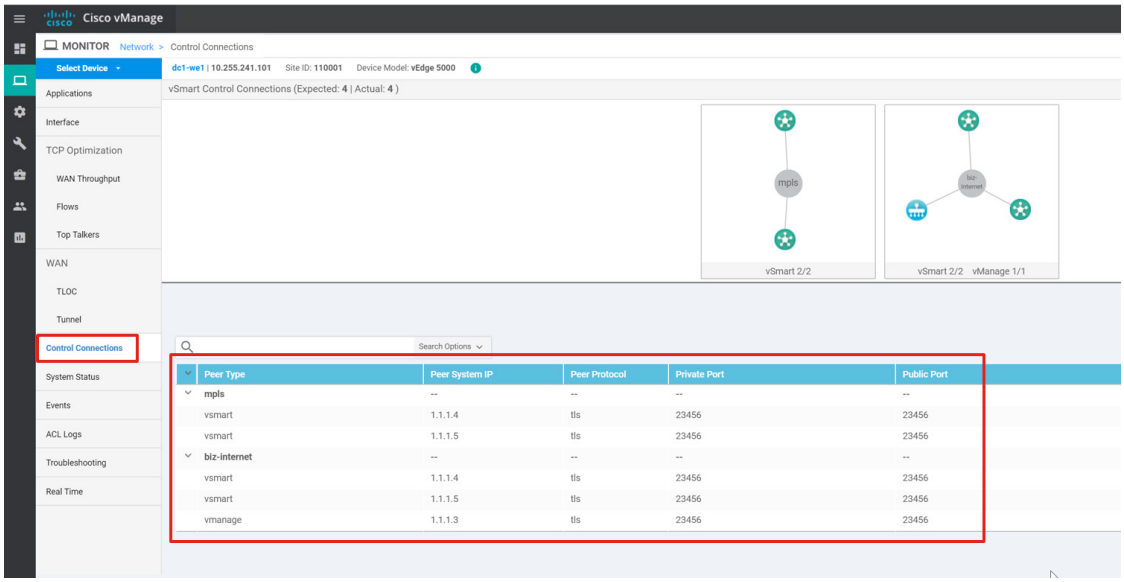
然后系统会将配置推送到这两个设备。完成后，vManage 应指示操作成功。

由于广域网边缘路由器处于试运行模式，因此无法从 vManage 控制面板中看到广域网边缘设备的状态。

19. 依次转到**监控 > 网络**。从表中可以看出，dc1-we1 和 dc1-we2 均可访问，各有总计五个控制连接。



20. 点击 **dc1-we1**。在左侧进行选择，您可以看到已通过每条传输链路建立的控制连接。



程序 12：创建本地化策略

本地化策略直接在广域网边缘路由器上调配。本地化控制策略示例包括路由策略，该策略可以影响本地站点网络上的 BGP 和 OSPF 路由行为，还可以影响进出该特定站点的路由。本地化数据策略可控制进出广域网边缘路由器上的接口和接口队列的数据流量。示例包括访问列表，访问列表用于对流量进行分类并将流量映射到不同的类，或流量镜像、策略管制和 QoS。

在示例网络的数据中心，CE 路由器标记所有具有 101:101 社区的 MPLS 路由（传输和非 SD-WAN 站点路由）。在广域网边缘设备上创建示例本地化策略，该策略将：

- 为 BGP 定义路由策略，以过滤局域网端 MPLS 传输链路（192.168.0.0/16 le 32、10.101.1.0/30、10.104.1.0/30、10.105.1.0/30）和通往 CE 路由器的链路（10.4.1.0/30 和 10.4.2.0/30）的任何传入前缀。
- 在 BGP 的路由策略中，匹配并接受具有 101:101 社区 (Non-SD-WAN-Sites) 的路由前缀。
- 在 BGP 的路由策略中，匹配并接受指示本地路由的其他路由，其中 AS-PATH 设置源自 65112，并将这些路由的社区设置为 1:100。
- 打开 netflow/cflowd，以便广域网边缘路由器可以进行流量监控并将信息发送到 vManage。
- 打开深度数据包检测 (DPI) 或应用可视性。通过 DPI，广域网边缘路由器可以发现、监控和跟踪局域网中运行的应用。这样可以增加 vManage GUI 中显示的应用信息。

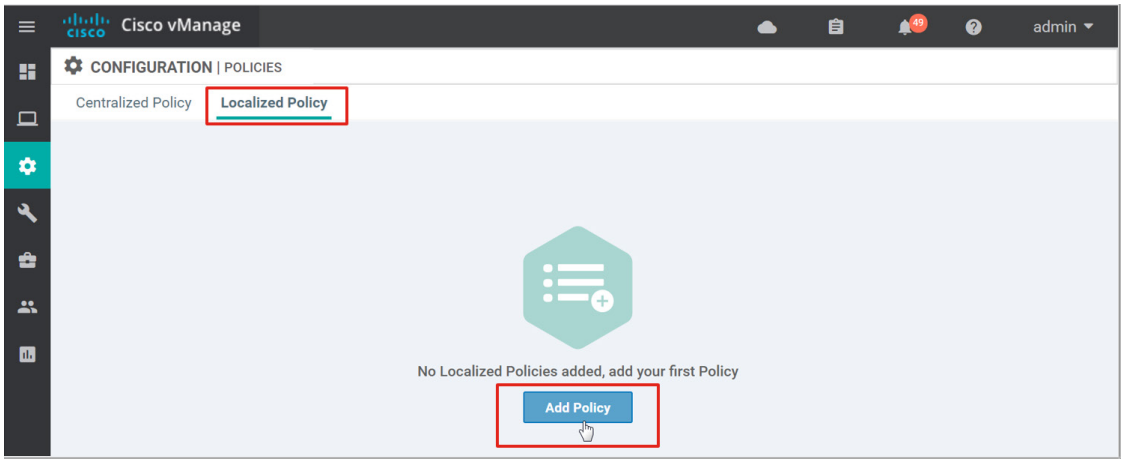
您将创建一个路由策略，应用于此示例的数据中心局域网中的 BGP 邻居。先定义列表，然后定义路由策略。对于每个路由策略，均定义序列，每个序列具有一个匹配/操作对。按照自上而下从低到高的顺序对每个路由策略进行评估。一旦完成匹配，路由就会被接受或拒绝/过滤。如果路由被接受，则可以使用 set 命令执行进一步的操作。一旦完成匹配并执行操作，处理就会停止。未引用列表的匹配项会匹配所有流量。对于与策略中的任何条件都不匹配的任何流量，每个路由策略结束时会执行默认操作（接受或拒绝）。

请注意，每个设备只能应用一个本地化策略，但可以在多个设备之间共享一个策略。如果在关联到设备的本地化策略中定义了变量，则无论设备是否引用该部分策略，都需要在应用策略时定义变量的值。因此，您可能希望根据类似的设备类型创建多个本地化策略和组，以避免必须输入不必要的变量值。

在**策略**旁边的**其他模板**部分中，将本地化策略与设备模板关联。关联到模板并部署到设备后，可以在关联到设备模板的任何功能模板中引用策略中的路由策略、访问列表及其他组件。如果不将策略关联到包含策略元素的设备模板，您将无法在设备模板中配置功能模板。如果设备模板已与设备关联，并且您尝试使用策略元素更新其某一个功能模板但尚未关联策略，则配置更新将失败。

按照以下步骤创建本地化策略。

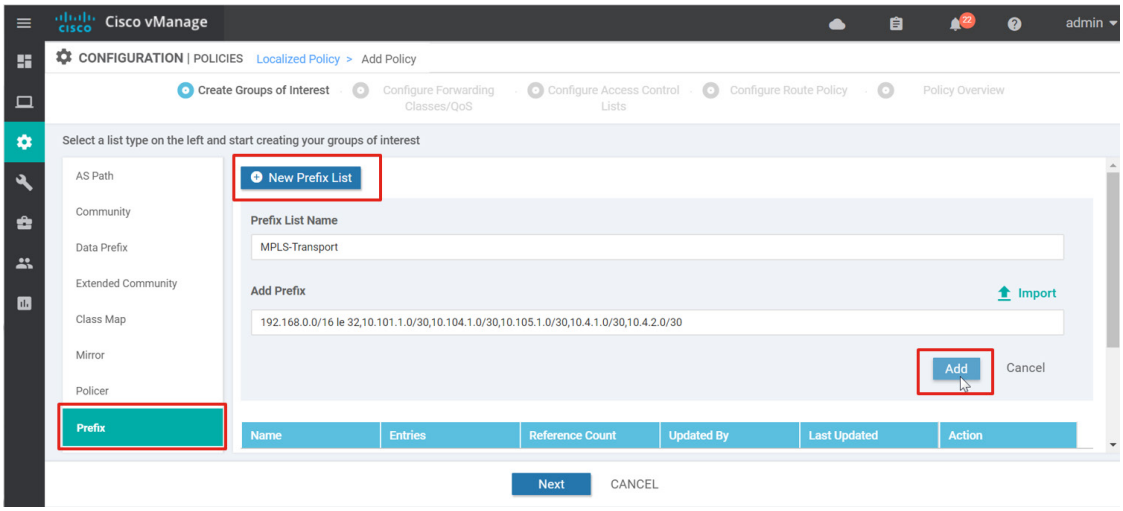
1. 在 vManage GUI 中，依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。
2. 选择**添加策略**按钮。



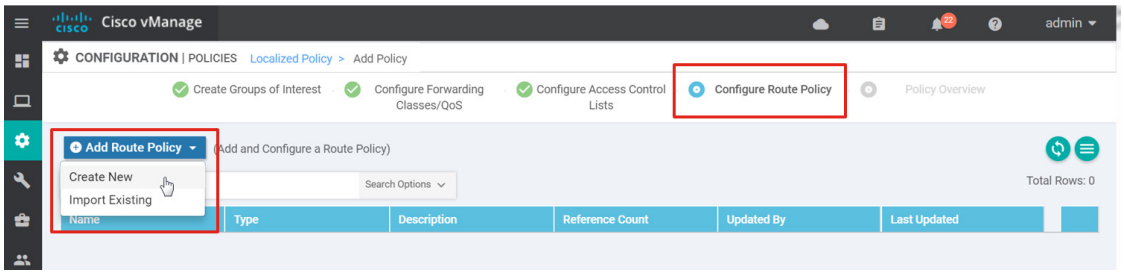
技术提示：请注意，在 vManage 18.2 代码版本之前，本地化策略仅基于 CLI。您仍可通过 CLI 如下配置策略：点击右上角的**自定义选项**下拉列表框，然后选择 **CLI 策略**。

创建本地化策略的第一步是创建关注的组。在示例要求中，定义一个前缀列表、一个社区列表和一个 AS 路径列表。

3. 选择左侧的**前缀**，然后点击**新建前缀列表**按钮。
4. 在**前缀列表名称**下的文本框中，输入 **MPLS-Transport**。
5. 在 “添加前缀” 下的文本框中，输入 **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**。
6. 点击**添加**按钮。

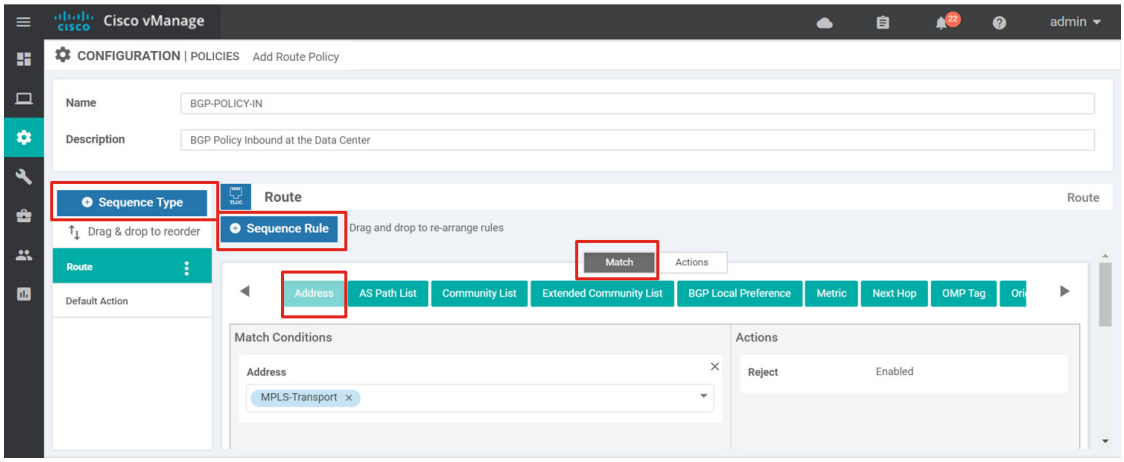


7. 在左侧选择**社区**，然后点击**新建社区列表**按钮。
8. 在**社区列表名称**下的文本框中，输入 **Non-SD-WAN-Sites**。
9. 在**添加社区**下的文本框中，输入 **101:101**。
10. 点击**添加**按钮。
11. 在左侧选择 **AS 路径**，然后点击**新建 AS 路径列表**按钮。
12. 在 **AS 路径列表名称**下的文本框中，输入 **Local-Routes**。
13. 在**添加 AS 路径**下的文本框中，输入 **^65112$**。
14. 点击**添加**按钮。
15. 点击**下一步**按钮三次，直至转到**配置路由策略**页面。
16. 点击**添加路由策略**按钮，然后选择**新建**。



17. 在**名称**旁边输入路由策略的名称 (**BGP-POLICY-IN**)，然后在**说明**旁边输入说明（**数据中心的入站 BGP 策略**）。
18. 选择左侧的**序列类型**，然后点击**序列规则**。

19. 确保选择**匹配**框，然后选择**地址**。在**匹配条件**下，从下拉文本框中选择 **MPLS-Transport**。



20. 保持此匹配条件的默认操作（拒绝）不变。点击**保存匹配项和操作**按钮。

21. 点击**序列规则**添加下一对匹配项/操作。

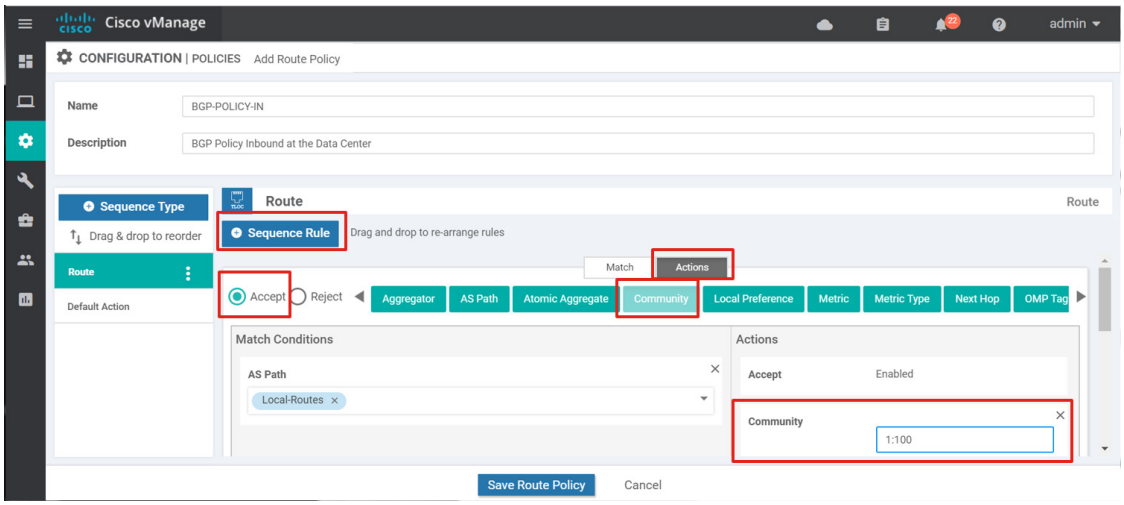
22. 确保选择**匹配**框，然后选择**社区列表**。在**匹配条件**下，从下拉文本框中选择 **Non-SD-WAN-Sites**。

23. 选择**操作**框，然后选择**接受**单选按钮。点击**保存匹配项和操作**按钮。

24. 点击**序列规则**添加下一对匹配项/操作。

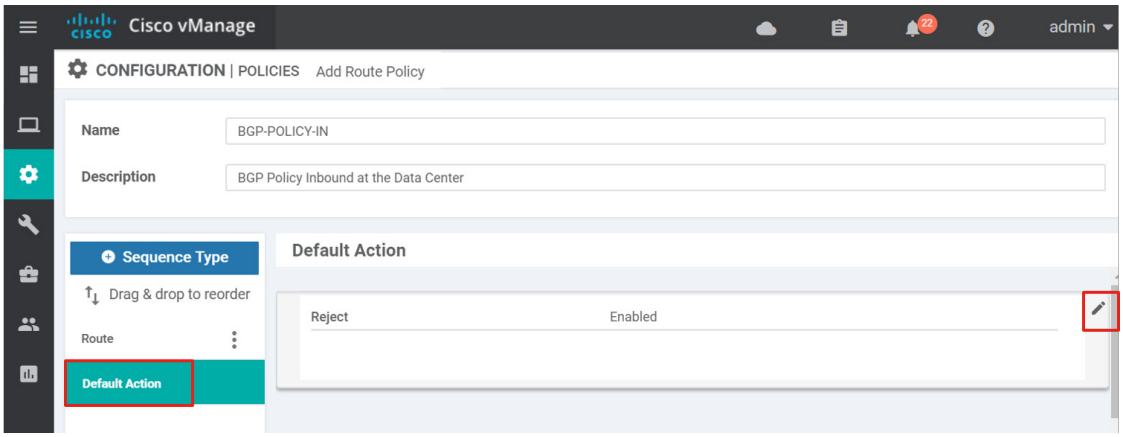
25. 确保选择**匹配**框，然后选择 **AS 路径列表**。在**匹配条件**下，从下拉文本框中选择 **Local-Routes**。

26. 选择**操作**框，然后选择**接受**单选按钮。选择**社区**框，然后在文本框中输入 **1:100**。此社区将在满足操作条件时设置。



27. 点击**保存匹配项和操作**按钮。

28. 选择左侧的**默认操作**。保留默认设置，即，如果没有匹配项则拒绝。要进行更改，请选择最右侧的铅笔图标，选择**接受**或**拒绝**，然后点击**保存匹配项和操作**。

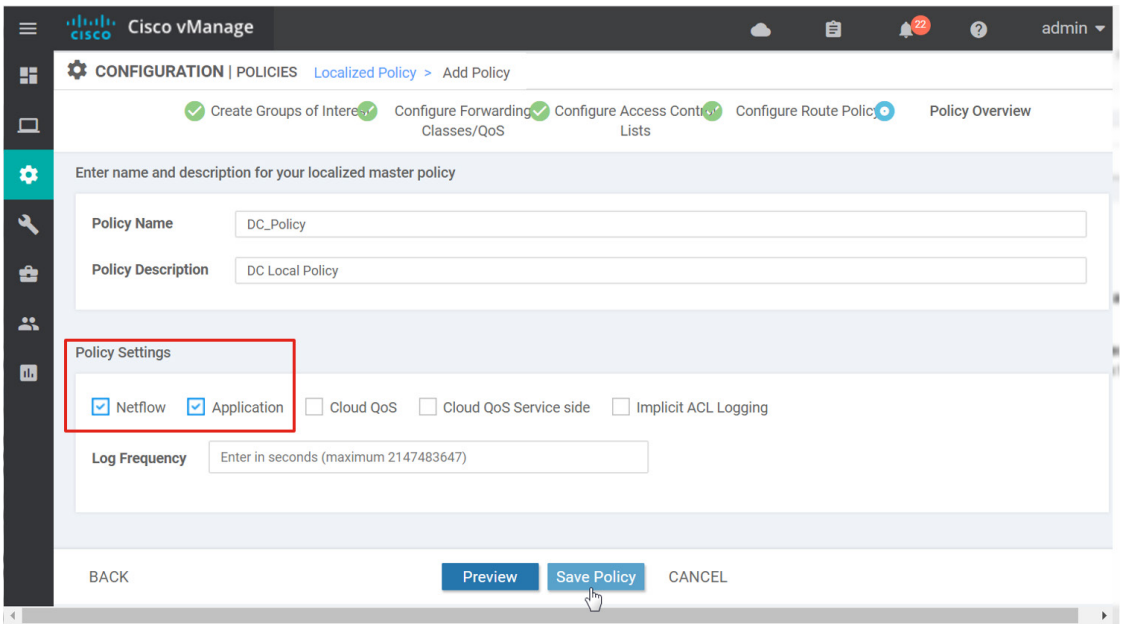


29. 点击**保存路由策略**按钮。

30. 点击**下一步**。

31. 输入策略名称 (**DC_Policy**) 和策略说明（**数据中心本地策略**）。

32. 在**策略设置**部分下，选中 **Netflow** 复选框启用 Netflow 或 Cflowd，然后选中**应用**复选框开启应用可视性。



33. 或者，点击**预览**按钮查看将要推送到广域网边缘路由器的策略。

34. 点击**保存策略**。

技术提示：要修改刚刚创建的 DC_Policy，可以依次转到**配置 > 本地化策略**，选择策略右侧的“...”，然后从下拉列表中选择**编辑**。您可以添加 QoS 配置、访问控制列表和其他路由策略。如果需要创建其他列表，或者想要创建独立的 QoS 配置、访问控制列表和路由策略（稍后可将其导入本地化策略中），请选择主要策略页面右上角的**自定义选项**按钮。

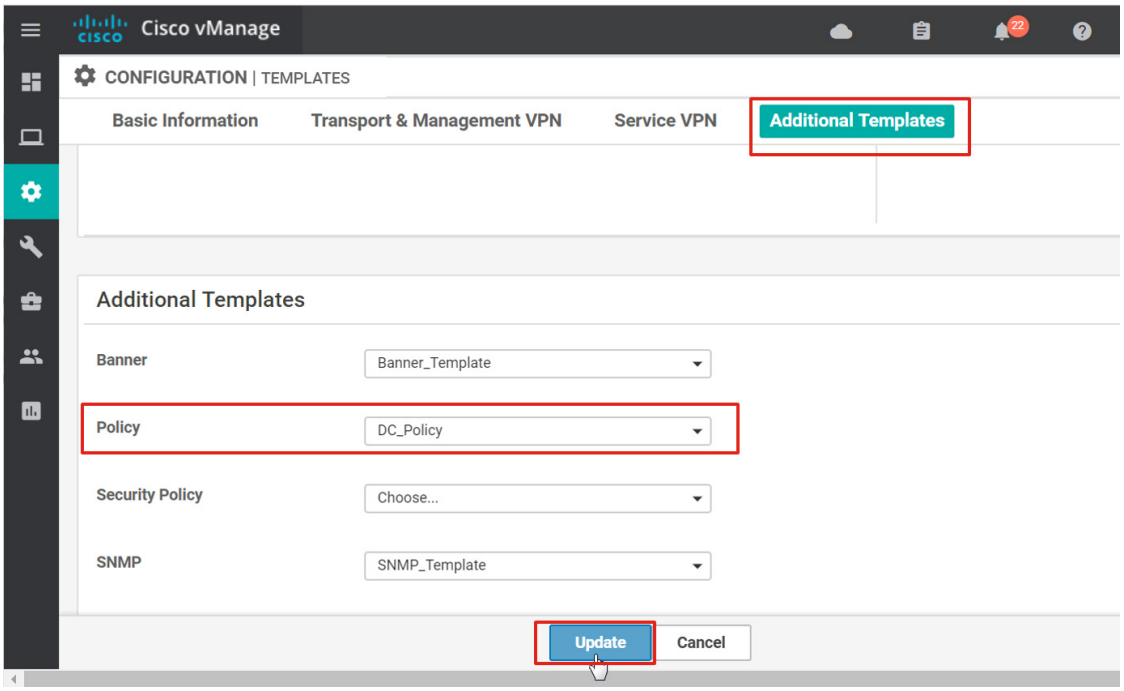
程序 13：将本地化策略与设备模板关联

现在已经创建了本地化策略，需要设备模板引用该策略。这会将策略配置下载到广域网边缘路由器。

1. 依次转到**配置 > 模板**，并确保选择**设备**选项卡。在模板 **DC_Hybrid_ BGP** 的旁边，选择右侧的“...”，然后选择**编辑**。

2. 滚动到**其他模板**部分，或选择**其他模板**以跳转到相应的设备模板部分。

3. 在**策略**的旁边，选择新创建的本地化策略 **DC_Policy**，然后选择**更新**。



4. 没有要定义的变量，因此选择**下一步**，然后选择**配置设备**。

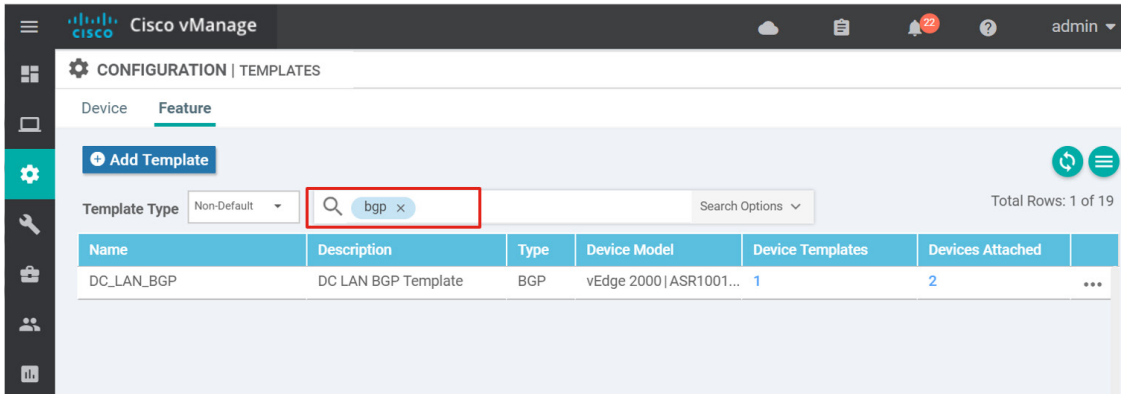
5. 选中相应复选框确认两台设备上的更改，然后选择**确定**。

6. 系统会将策略推送到广域网边缘路由器，并且状态应指示成功。

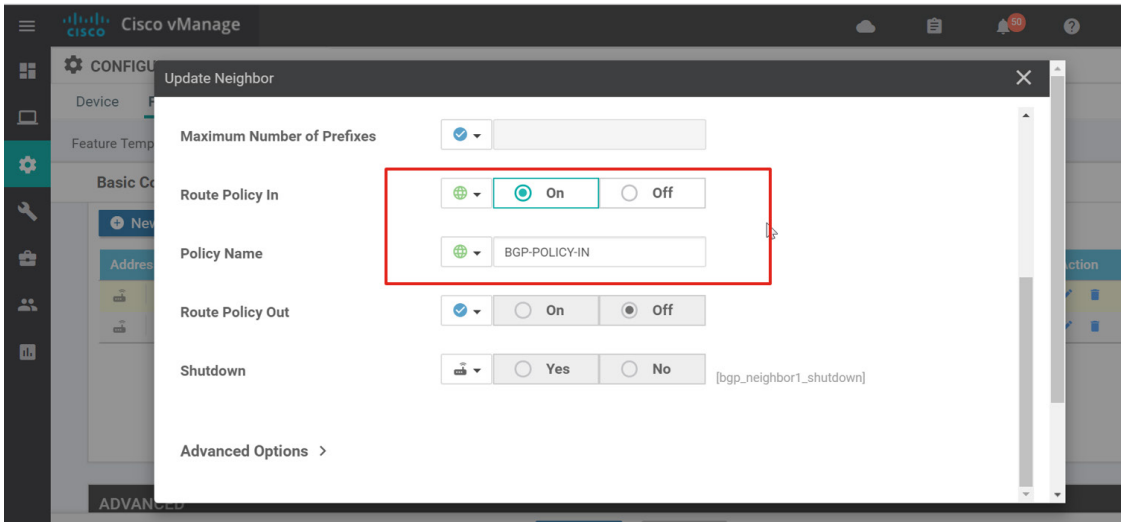
程序 14：在功能模板中添加本地化策略引用

现在本地化策略已与设备模板关联并下载到广域网边缘设备，请在 BGP 功能模板中配置路由策略。

1. 依次转到**模板 > 配置**，然后选择**功能**选项卡。
2. 在搜索文本框中，输入 **bgp** 并按回车键。系统将使用该关键字在**名称**、**说明**、**类型**和**型号**列中过滤模板。
3. 选择模板 **DC_LAN_BGP** 右侧的 “...”，然后选择**编辑**。



4. 在**邻居**下，选择所定义的第一个邻居的**操作**列下的编辑符号。
5. 对于**路由策略范围**，从下拉列表框中选择**全局**，然后选择**开启**。在**策略名称**旁边输入 **BGP-POLICY-IN**。



6. 选择 **Save Changes（保存更改）**。
7. 对所定义的第二个邻居重复第 4 至 6 步。

8. 选择**更新**以保存功能模板。由于修改过的功能模板与设备关联，因此 vManage 会在进行任何功能模板更改后尝试推送修改后的配置。vManage 会将新更改合并到其完整本地配置中，并将完整配置推送到广域网边缘路由器。

9. 无需输入新变量值，因此选择**下一步**。如果需要，请检查配置。否则，请选择**配置设备**。

10. 在弹出窗口中确认两台设备上的配置更改，然后选择**确定**。

程序 15：将 vEdge 设备退出试运行模式

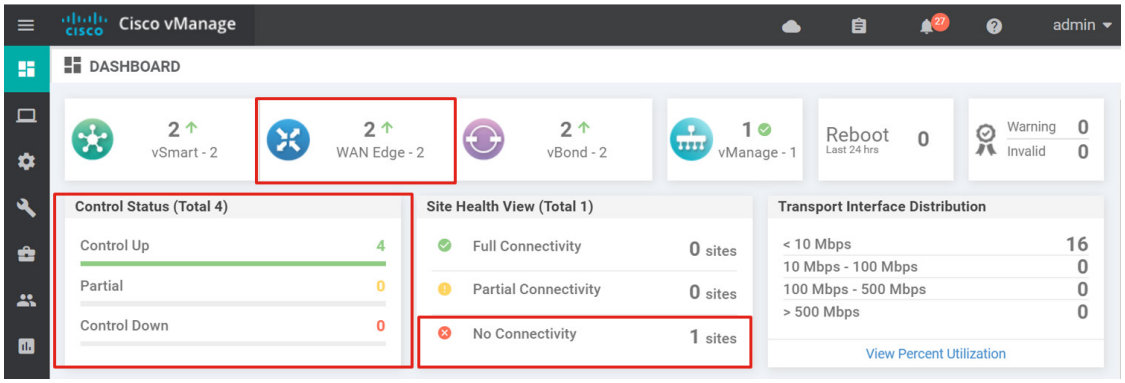
如果广域网边缘路由器最初被置于试运行模式，则可以让它们上线并开始运行。可以随时进行这项操作。

1. 依次转到**配置 > 证书**，找到刚配置的广域网边缘路由器（**dc1-we1** 和 **dc1-we2**），然后为每台路由器选择**有效**。

2. 对于每台设备，系统都会弹出消息，询问您是否确定要验证设备。选择**确定**。

3. 两台设备都有效后，选择**发送至控制器**按钮，为控制器提供最新的授权设备列表。广域网边缘路由器最初可能会在控制面板上显示不可访问且不可控制状态，但在一分钟内应该就会显示可访问且可控制状态。

您会在 vManage 控制面板的**站点运行状况视图**中看到此第一个站点没有连接。这是因为这些广域网边缘路由器上的所有 BFD 会话均处于关闭状态。这是因为其他站点均尚未上线，并且两台数据中心广域网边缘设备之间由于它们均配置为相同的站点 ID 而不会形成 BFD 会话。



部署远程站点

有五个分支机构代表了常见的新环境部署。这五个分支机构运行着许多部署中常见的各种功能。

在此部署中，将首先配置本地化策略和功能模板，然后配置设备模板。接下来，将设备模板与广域网边缘路由器关联，然后利用 ZTP（适用于 vEdge）或 PnP（适用于 IOS XE SD-WAN）流程使广域网边缘路由器上线。通过自动调配过程升级路由器，然后使用完整配置使路由器上线。

程序 1：为分支机构创建本地化策略

为分支机构创建本地化策略。您可以创建一个适用于所有分支机构的较大策略，也可以创建较小的策略并将不同的策略应用到不同的分支机构类型。

示例策略应包括:

- 流可视性
- 应用可视性或深度数据包检测 (DPI)
- 双广域网边缘路由器站点上的 BGP 路由策略。一个策略应仅通告 TLOC 扩展链路子网，以便使用 MPLS 传输链路的路由器可以利用 TLOC 扩展链路连接到广域网边缘路由器以进行 MPLS 传输。另一个策略应过滤进入传输端 VPN 的所有 BGP 路由，因为指向 MPLS 传输链路下一跳的静态默认路由将用于将控制流量和 IPSec 隧道终端流量路由出传输端 VPN。
- 包含默认路由的前缀列表，以便 VRRP 跟踪它。如果 OMP 前缀路由消失，广域网边缘路由器会放弃 VRRP 主状态。

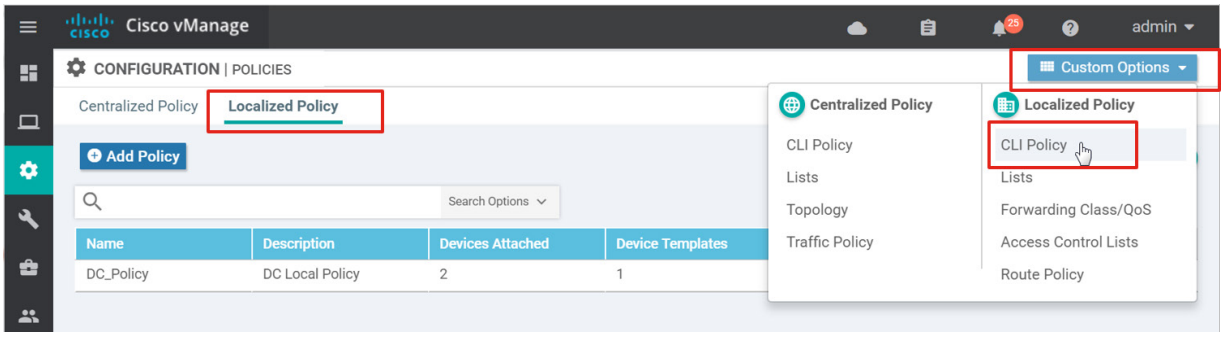
> **技术提示：**在 vManage 18.3 版中，对于使用本地策略向导有一些限制。首先，您必须包含对 QoS 策略、ACL 或路由策略的引用，才能创建有效的本地策略；不能只是开启应用可视性或流可视性，或者只包括路由进程要使用的前缀列表。其次，您无法在策略中使用变量将同一路由策略应用到不同的广域网边缘设备（每台设备都使用站点特定信息）。请注意，在策略向导 GUI 中，您仍然可以创建多个路由策略，根据需要使用模板中的特定设备专用变量引用路由策略，将不同的路由策略应用到不同的广域网边缘设备。如果不使用本地策略向导，可以改而使用本地化 CLI 策略，点击本地化策略主页右上角的**自定义选项**按钮可对其进行配置。您甚至可以使用策略向导来构建本地策略，还可以选择预览该策略。预览 CLI，使用它创建 CLI 策略，并在其中进行修改。

首先，创建两个分支机构策略：**Branch_Policy** 和 **Branch_BGP_OSPF_Policy**。**Branch_BGP_OSPF_Policy** 将包含为 BGP 配置的广域网边缘路由器（用于通告 TLOC 扩展子网）或为 OSPF 配置的广域网边缘路由器所需的任何路由策略。**Branch_Policy** 在非 OSPF 和非 BGP 广域网边缘路由器上用于流可视性和应用可视性以及 VRRP 的默认路由跟踪。由于显示的策略向导用于数据中心本地策略，因此 CLI 本地策略将用于分支机构。

请注意，将本地化策略应用到某个应用于多台广域网边缘路由器的设备模板时，必须为该本地化策略中的所有变量定义值，无论该设备是否在其功能模板中使用这些策略组件均是如此。（可选）创建任何其他策略，这样在应用策略时就不用定义不必要的变量。

按照以下步骤为分支机构创建本地化策略:

1. 在 vManage GUI 中，依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。
2. 点击 GUI 右上角的**自定义选项**按钮，然后从下拉菜单中选择 **CLI 策略**。



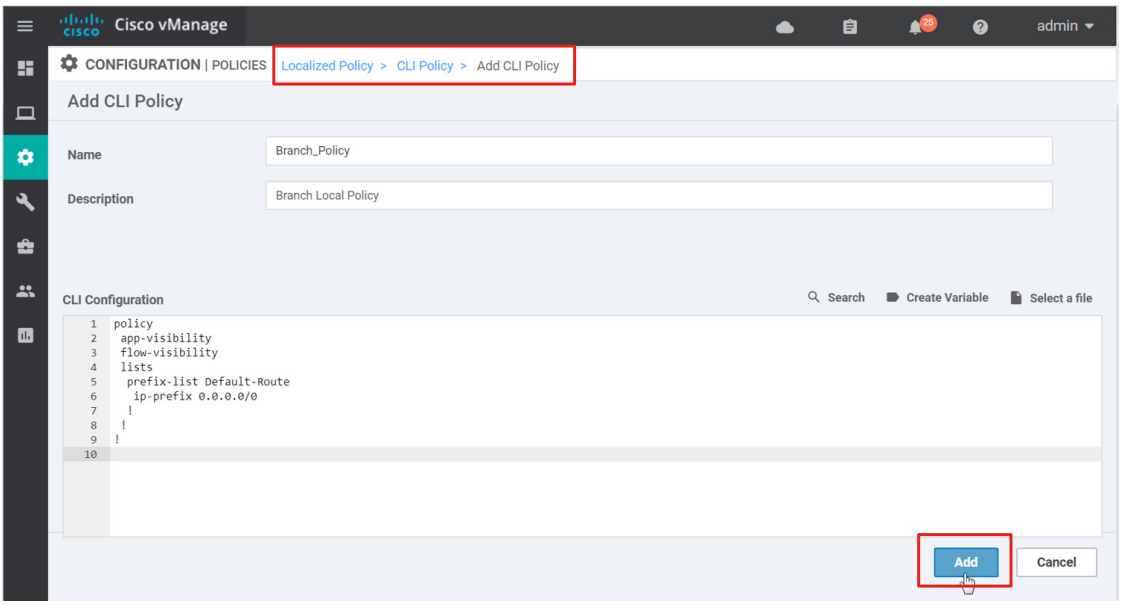
3. 点击**添加策略**按钮。

4. 输入**名称** (Branch_Policy) 和**说明**（分支机构本地策略）。

5. 在 CLI 中输入或粘贴以下命令:

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

6. 选择**添加**以完成并保存本地化策略。



7. 添加第二个分支机构本地策略。选择**添加策略**按钮。
8. 输入**名称** (**Branch_BGP_OSPF_Policy**) 和**说明**（**分支机构 BGP 和 OSPF 本地策略**）。
9. 在 CLI 中输入或粘贴以下命令:

```
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. 选择**添加**以完成并保存本地化策略。

程序 2：配置传输端功能模板

在示例网络的传输端，应创建几个不同的功能模板。

子接口用于分支机构 4，因为两台广域网边缘路由器之间的单条链路负责支持广域网传输和 TLOC 扩展子接口。很多时候，通过将接口名称指定为变量，可以将子接口和物理接口组合到一个功能模板中。根据设计，子接口不支持 QoS。但是，QoS 策略可以应用到模板，该模板通过为接口名称创建变量来组合以配置物理接口和子接口，但在将策略应用到子接口时将以静默方式丢弃该策略。

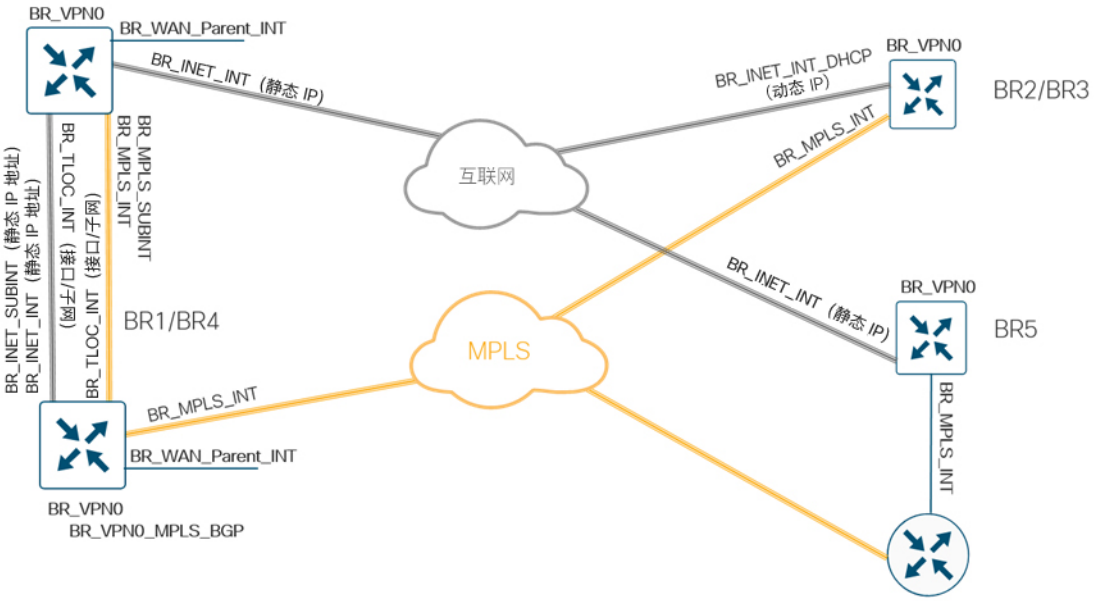
如果服务提供商支持使用较少的 DSCP 类，则重写策略允许您在隧道头中重写 DSCP 值。如果您需要重写策略，vManage 将不允许您将其应用到子接口，因此在这种情况下最好创建单独的接口和子接口模板。

子接口要求在 VPN 0 中定义物理父接口，并且由于 802.1q 标记，还要求子接口 MTU 比物理接口少四个字节。建议为 1504 字节的 MTU 配置父物理接口以满足此要求。

以下是分支机构传输端所需的功能模板：

- VPN 0 模板 - 可以为所有分支机构构建一个功能模板（所有分支机构均为 BR_VPN0）
- VPN 接口以太网模板 - VPN 0 下需要几个不同的接口模板：
  - MPLS 传输链路的物理接口（所有分支机构均需要 BR_MPLS_INT）
  - 使用 -TLOC 扩展的 MPLS 传输链路的子接口（分支机构 4 需要 BR_MPLS_SUBINT）
  - 使用静态 IP 寻址的互联网传输链路的物理接口（分支机构 1、4 和 5 需要 BR_INET_INT）
  - 使用 DHCP IP 寻址的互联网传输链路的物理接口（分支机构 2 和 3 需要 BR_INET_INT_DHCP）
  - 使用静态 IP 寻址的互联网传输链路的子接口（分支机构 4 需要 BR_INET_SUBINT）
  - TLOC 扩展接口或子接口，可以组合成一个模板（分支机构 1 和 4 需要 BR_TLOC_EXT_INT）
  - 子接口的广域网父物理接口（分支机构 4 需要 BR_WAN_Parent_INT）
- BGP - 需要 BGP 功能模板，以便 MPLS 连接的广域网边缘路由器的传输端将 TLOC 扩展链路子网传递给 MPLS 传输链路（分支机构 1 和 4 需要 BR_VPN0_MPLS_BGP）。

图 15　分支机构广域网边缘设备传输端模板



分支机构 VPN 0 模板

一个 VPN 0 模板将用于所有分支机构广域网边缘设备。在互联网接口上使用 DHCP 时，从技术上说，只需要一个静态下一跳（用于 MPLS 接口的默认路由前缀），因为互联网接口的默认路由通常是动态获取的。在使用 DHCP 获取互联网 IP 地址的情况下，不需要创建单独的 VPN 0 模板，两种情况可以使用同一模板，因为对接口进行 DHCP 配置后，动态 IP 网关就会覆盖静态定义的网关。

1. 依次转到**配置 > 模板**，然后选择**功能**选项卡。选择**添加模板**按钮，然后使用以下参数配置 VPN 0 功能模板：

选择设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN

模板名称：BR_VPN0

说明：分支机构传输端 VPN 0

分支机构 VPN 0 功能模板

部分	参数	类型	变量/值
基本配置	VPN	全局	0
	名称	全局	传输端 VPN
	增强 ECMP 键控	全局	开启
DNS	主 DNS 地址	全局	64.100.100.125
	辅助 DNS 地址	全局	64.100.100.126
IPv4 路由	前缀	全局	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn0_mpls_next_hop_ip_addr
	下一跳地址	特定设备专用	vpn0_inet_next_hop_ip_addr

2. 选择**保存**以完成模板。

分支机构 MPLS 接口模板

3. 使用以下参数添加新功能模板：

选择设备：**除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备**

模板：**VPN/VPN 接口以太网**

模板名称：BR_MPLS_INT

说明：具有静态 IP 的分支机构 MPLS 接口

分支机构 VPN 0 MPLS 接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启
隧道 > 允许服务	BGP	全局	开启
	DHCP	全局	关闭
	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

4. 选择**保存**以创建模板。

分支机构 MPLS 子接口模板

5. 使用以下参数添加新功能模板或复制之前的功能模板。唯一的变化是**接口名称**的变量，它变为 **vpn0_mpls_int_x|x.VLAN**。

选择设备：**除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备**

模板：**VPN/VPN 接口以太网**

模板名称：**BR_MPLS_SUBINT**

说明：**具有静态 IP 的分支机构 MPLS 子接口**

分支机构 VPN 0 MPLS 子接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x.VLAN
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启
允许服务	BGP	全局	开启
	DHCP	全局	关闭
	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

6. 选择**保存**或**更新**以保存模板。

分支机构互联网接口模板

7. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_INET_INT

说明：具有静态 IP 的分支机构互联网接口

分支机构 VPN 0 互联网接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
允许服务	DHCP	全局	关闭
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

8. 选择**保存**以创建模板。

分支机构互联网 DHCP 接口模板

9. 复制最后创建的模板 (**BR_INET_INT**)。通过将参数 IPv4 单选按钮从静态更改为动态来进行编辑。此外，请务必将**允许服务**下的 **DHCP** 设置更改为**开启**。如果不做此更改，互联网接口就无法获取动态 IP 地址，并且接口上与控制器的连接也可能会断开。

模板名称：BR_INET_INT_DHCP

说明：具有 DHCP IP 的分支机构互联网接口

分支机构 VPN 0 互联网接口动态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_gex|x
	说明	全局	互联网接口

部分	参数	类型	变量/值
IPv4 配置	IPv4 地址	单选按钮	动态
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
允许服务	DHCP	全局	开启
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

10. 选择**更新**以保存模板。

分支机构互联网子接口模板

11. 复制创建的互联网模板静态模板 (**BR_INET_INT**)。通过将接口名称变量更改为 **vpn0_inet_int_x|x.VLAN** 来进行编辑。

模板名称：BR_INET_SUBINT

说明：具有静态 IP 的分支机构互联网子接口

分支机构 VPN 0 互联网子接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x.VLAN
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启

部分	参数	类型	变量/值
	颜色	全局	企业互联网
允许服务	DHCP	全局	关闭
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

12. 选择**更新**以保存模板。

分支机构 TLOC 扩展接口模板

13. 添加新功能模板或复制现有功能模板。使用以下参数:

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_TLOC_EXT_INT

说明：分支机构 TLOC 扩展接口/子接口

分支机构 VPN 0 TLOC **接口/子接口功能模板**

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_tloc_ext_int_shutdown
	接口名称	特定设备专用	vpn0_tloc_ext_int_x|x_or_x|x.VLAN
	说明	全局	TLOC 扩展接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_tloc_ext_int_ip_addr|maskbits
高级	TLOC 扩展	特定设备专用	vpn0_tloc_ext_wan_int_x|x

14. 选择**保存**以创建模板。

分支机构 WAN 父接口模板

15. 添加新功能模板。使用以下参数:

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_WAN_Parent_INT

说明：分支机构 WAN 父接口

分支机构 VPN 0 WAN 父接口功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_wan_parent_int_shutdown
	接口名称	特定设备专用	vpn0_wan_parent_int_x|x
	说明	全局	WAN 父接口
高级	IP MTU	全局	1504

16. 选择**保存**以完成模板。

分支机构 VPN 0 MPLS BGP 模板

17. 添加新功能模板。使用以下参数:

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/BGP

模板名称：BR_VPN0_MPLS_BGP

说明：与提供商相连的分支机构 VPN 0 MPLS BGP

分支机构 VPN 0 MPLS BGP 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_bgp _shutdown
	AS 编号	特定设备专用	vpn0_bgp_as_num
	路由器 ID	特定设备专用	vpn0_bgp_router_id
IPv4 单播地址系列	最大路径数	全局	2
	地址系列	下拉列表	ipv4 单播
	网络/网络前缀	特定设备专用	bgp_tloc_ext_prefix_to_advertise

部分	参数	类型	变量/值
邻居	地址	特定设备专用	vpn0_bgp_neighbor_addr
	说明	特定设备专用	vpn0_bgp_neighbor_description
	远程 AS	特定设备专用	vpn0_bgp_neighbor_remote_as
	地址系列	全局	开启
	地址系列	下拉列表	ipv4 单播
	入站路由策略	全局	开启
	策略名称	全局	DENY-ALL
	关闭	特定设备专用	vpn0_bgp_neighbor_shutdown

18. 选择**保存**以完成模板。

程序 3：配置服务端功能模板

在示例网络的服务端，应创建几个不同的功能模板。

从 18.2 版代码开始，可以将某些模板参数标记为可选。这样，您就可以在过去必须定义多个模板的情况下组合使用模板。

分支机构 5 的服务端 VPN 模板包含静态路由而其他分支机构的服务端 VPN 不包含，因此，通过在模板中将静态路由标记为可选配置，现在所有分支机构可以共享一个通用的服务端 VPN 模板。

> **技术提示：**虽然您也可以在 VPN 以太网接口模板中将 VRRP 配置标记为可选，但当您在经过测试的版本中尝试部署模板时，VRRP 会被视同必需的配置，因此您在提供与 VRRP 配置关联的变量之前无法部署该模板。作为此问题的解决办法，可以创建两个不同的 VPN 以太网接口模板，一个配置 VRRP，一个不配置。

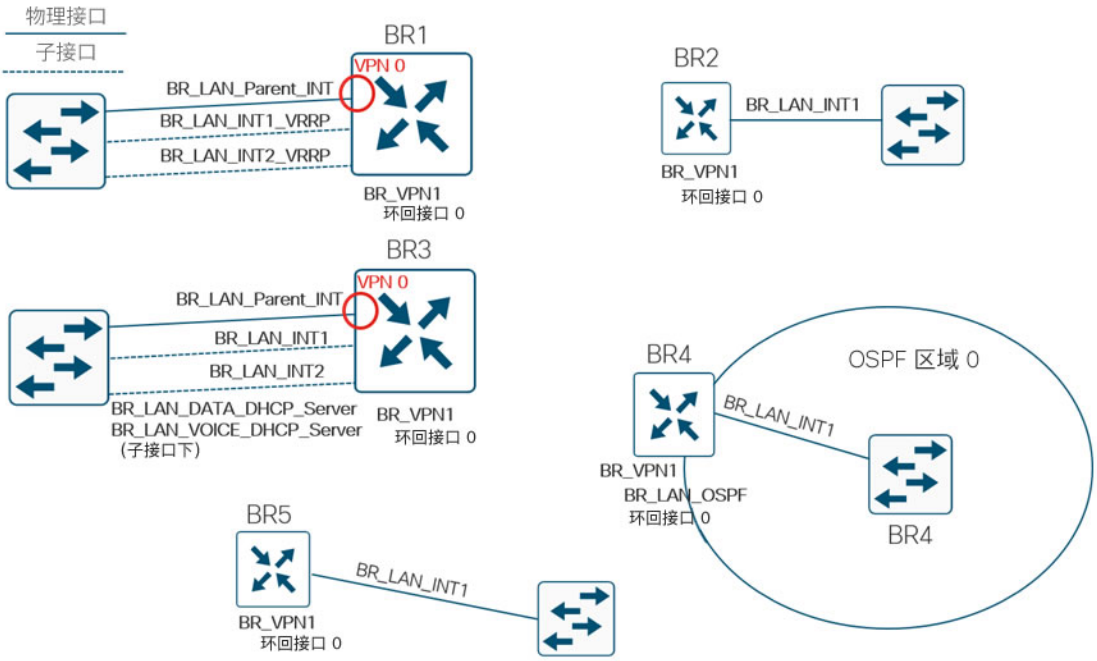
与 VPN 1 相关联的 LAN 接口可以是物理接口或子接口。一个 VPN 以太网接口模板代表物理接口和子接口。大多数站点使用 DHCP 中继到数据中心，因此配置了 IP DHCP 帮助程序地址，但是有一个站点的广域网边缘路由器用作 LAN 网段的 DHCP 服务器。如果同一 VPN 中的一台广域网边缘路由器上有两个 LAN 接口，则需要两个不同的功能模板；不能多次在单个 VPN 下使用相同的功能模板。

以下是分支机构服务端所需的功能模板：

- VPN 1 模板 - 一个基础服务端 VPN 功能模板即可满足分支机构要求（分支机构 1-5 需要 BR_VPN1）。对于分支机构 5，将静态路由添加到模板中并标记为可选。
- VPN 接口以太网模板 - VPN 1 下需要几个不同的接口模板：

  - 一个无 VRRP 的 LAN 接口的物理接口/子接口（分支机构 2-5 需要 BR_LAN_INT1）。
  - 第二个无 VRRP 的 LAN 接口的物理接口/子接口（分支机构 2-3 需要 BR_LAN_INT2）。
  - 为 VRRP 配置的一个 LAN 接口的物理接口/子接口（分支机构 1 需要 BR_LAN_INT1_VRRP）。
  - 为 VRRP 配置的第二个 LAN 接口的物理接口/子接口（分支机构 1 需要 BR_LAN_INT2_VRRP）。
- 子接口的 LAN 父物理接口。此功能模板实际上属于 VPN 0（分支机构 1 和 3 需要 BR_LAN_Parent_INT）。
- DHCP 服务器池 - 接口模板下需要 DHCP 服务器池模板。您需要创建两个模板，一个用于数据，一个用于语音。语音 DHCP 服务器模板将包含在数据 DHCP 服务器模板下未使用的简单文件传输协议 (TFTP) 服务器参数（分支机构 3 需要 BR_LAN_DATA_DHCP_Server 和 BR_LAN_VOICE_DHCP_Server）。
- OSPF - VPN 1 下需要 OSPF 功能模板（分支机构 4 需要 BR_LAN_OSPF）。
- Loopback0 - VPN 1（分支机构 1-5）下需要环回接口 0 的 VPN 以太网接口功能模板（已配置）

图 16　分支机构广域网边缘设备服务端模板



BR_VPN1

系统会将远程站点的一个汇聚前缀通告到 OMP 而不是多个站点路由。请注意，即使您可以将此前缀标记为可选配置，但在开启汇聚后，您至少需要定义一个汇聚前缀。开启已连接路由的重新分发以通告环回接口，以实现与数据中心之间的可访问性，可以进行管理。

配置静态路由并将其标记为可选，以便在分支机构 5 上使用此路由访问位于第 3 层交换机后的 LAN 网段。该站点不是将静态路由重新分发到 OMP，而是通告汇聚前缀。

1. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN

模板名称：BR_VPN1

说明：分支机构 VPN1

分支机构 VPN 1 基础功能模板

部分	参数	类型	变量/值
基本配置	VPN	全局	1
	名称	全局	服务端 VPN
	增强 ECMP 键控	全局	开启
通告 OMP	互联	全局	开启
	集合	全局	开启
	汇聚/前缀	特定设备专用	vpn1_omp_aggregate_prefix
	汇聚/仅汇聚	全局	开启
IPv4 路由 [标记为可选行]	前缀	特定设备专用	vpn1_lan_static_route_prefix|mask bits
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn1_lan_next_hop_ip_addr

2. 选择**保存**以创建模板。

分支机构 LAN 接口 1 模板

3. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT1

说明：分支机构 LAN 接口 1

分支机构 VPN 1 接口 1 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10

4. 选择**保存**以创建模板。

分支机构 LAN 接口 2 模板

5. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT2

说明：分支机构 LAN 接口 2

分支机构 VPN 1 接口 2 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10

6. 选择**保存**以完成模板。

BR_LAN_INT1_VRRP

7. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT1_VRRP

说明：分支机构 LAN 接口 1 VRRP

分支机构 VPN 1 接口 1 VRRP 功能模板设置

部分	参数	类型	变量/值
	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10
VRRP	组 ID	全局	1
	优先级	特定设备专用	lan_int1_vrrp_priority
	跟踪 OMP	全局	关闭
	跟踪前缀列表	全局	Default-Route
	IP 地址	特定设备专用	lan_int1_vrrp_ip_addr

8. 选择**保存**以创建模板。

BR_LAN_INT2_VRRP

9. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT2_VRRP

说明：分支机构 LAN 接口 2 VRRP

分支机构 VPN 1 接口 2 VRRP 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr/maskbits
高级	DHCP 帮助程序	全局	10.4.48.10
VRRP	组 ID	全局	2
	优先级	特定设备专用	lan_int2_vrrp_priority
	跟踪 OMP	全局	关闭
	跟踪前缀列表	全局	Default-Route
	IP 地址	特定设备专用	lan_int2_vrrp_ip_addr

10. 选择**保存**以创建模板。

分支机构 LAN 父接口模板

11. 使用以下参数添加新功能模板:

设备: 除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板: VPN/VPN 接口以太网

模板名称: BR_LAN_Parent_INT

说明: 分支机构 LAN 父接口

分支机构 VPN 1 LAN 父接口模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_parent_int_shutdown
	接口名称	特定设备专用	lan_parent_int_x|x
	说明	全局	LAN 父接口
高级	IP MTU	全局	1504

12. 选择**保存**以完成模板。

分支机构 LAN 数据 VLAN DHCP 服务器模板

13. 使用以下参数添加新功能模板:

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/DHCP 服务器

模板名称：BR_LAN_DATA_DHCP_Server

说明：用于数据 VLAN 的分支机构 LAN DHCP 服务器

用于数据 VLAN 的分支机构 VPN 1 LAN DHCP 服务器功能模板

部分	参数	类型	变量/值
基本配置	地址池	特定设备专用	data_dhcp_addr_pool|maskbits
	排除地址	特定设备专用	data_dhcp_addr_exclude_range
高级	域名	全局	cisco.local
	默认网关	特定设备专用	data_dhcp_default_gateway
	DNS 服务器	全局	10.4.48.10

14. 选择**保存**以完成模板。

分支机构 LAN 语音 VLAN DHCP 服务器模板

15. 复制和编辑之前的模板，并更改变量名称。还要将 TFTP 服务器的变量添加到模板，因为第二个 DHCP 服务器池用于语音 VLAN，而且电话需要向 Call Manager 注册。使用以下参数:

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/DHCP 服务器

模板名称：BR_LAN_VOICE_DHCP_Server

说明：用于语音 VLAN 的分支机构 LAN DHCP 服务器

用于语音 VLAN 的分支机构 VPN 1 LAN DHCP 服务器功能模板

部分	参数	类型	变量/值
基本配置	地址池	特定设备专用	voice_dhcp_addr_pool|maskbits
	排除地址	特定设备专用	voice_dhcp_addr_exclude_range
高级	域名	全局	cisco.local
	默认网关	特定设备专用	voice_dhcp_default_gateway

部分	参数	类型	变量/值
	DNS 服务器	全局	10.4.48.10
	TFTP 服务器	全局	10.4.48.19

16. 选择**更新**以保存模板。

分支机构 LAN OSPF

17. 使用以下参数添加新功能模板：

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/OSPF

模板名称：BR_LAN_OSPF

说明：分支机构 LAN OSPF

分支机构 LAN OSPF **功能模板**

部分	参数	类型	变量/值
基本配置	路由器 ID	特定设备专用	lan_ospf_router_id
重新分发	协议	全局	omp
区域	区域号	全局	0
	接口/接口名称	特定设备专用	lan_ospf_int_x|x
	接口/接口成本	特定设备专用	lan_ospf_int_cost
	接口/高级/OSPF 网络类型	全局下拉列表	点对点
	接口/身份验证/身份验证类型	全局下拉列表	message-digest
	接口/消息摘要/消息摘要密钥 ID	全局	22
	接口/消息摘要/消息摘要密钥	特定设备专用	lan_ospf_message_digest_key
区域范围	地址	特定设备专用	lan_ospf_area_range_addr_0
高级	参考带宽 (Mbps)	全局	100000
	来源	全局	开启

18. 选择**保存**以完成模板。

程序 4：创建分支机构设备模板

创建功能模板后，即可创建设备模板。此示例网络中有四种常规类型的分支机构。

- A 类分支机构：双广域网边缘路由器站点，混合配置（MPLS 和互联网），TLOC 扩展接口，第 2 层交换机堆叠，VRRP
- B 类分支机构：单广域网边缘路由器站点，混合配置（MPLS 和互联网），单第 2 层 LAN 交换机
- C 类分支机构：双广域网边缘路由器站点，混合配置（MPLS 和互联网），TLOC 扩展接口，第 3 层交换机，OSPF
- D 类分支机构：单广域网边缘路由器站点，混合配置（MPLS 和互联网），CE 路由器，第 3 层交换机

对于分支机构 1 和 4，互联网连接的广域网边缘路由器和 MPLS 连接的广域网边缘路由器各自具有不同的广域网边缘设备模板，因为必须将 BGP 功能模板添加到 MPLS 连接的广域网边缘路由器的设备模板中。

配置以下设备模板:

- Branch_A_MPLS_BGP_TLOCEXT_VRRP（分支机构 1，广域网边缘设备 1）
- Branch_A_INET_TLOCEXT_VRRP（分支机构 1，广域网边缘设备 2）
- Branch_B_MPLS_INET(DHCP)（分支机构 2）
- Branch_B_MPLS_INET(DHCP)_LAN(DHCP)（分支机构 3）
- Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF（分支机构 4，广域网边缘设备 1）
- Branch_C_INET_TLOCEXT_SubInt_OSPF（分支机构 4，广域网边缘设备 2）
- Branch_D_MPLS_CE_INET_LAN-Static-Routing（分支机构 5）

Branch_A_MPLS_BGP_TLOCEXT_VRRP

1. 在 vManage GUI 中，依次转到**配置 > 模板**，并确保选择**设备**选项卡。
2. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。
3. 填写 “设备型号”、“模板名称” 和 “说明”。

设备型号：ISR 4351

模板名称：Branch_A_MPLS_BGP_TLOCEXT_VRRP

说明：分支机构双广域网边缘设备混合 TLOC 扩展，具有 MPLS BGP 以及 LAN 端中继和 VRRP

4. 使用以下功能模板进行配置:

Branch_A_MPLS_BGP_TLOCEXT_VRRP **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
	VPN 接口	BR_TLOC_EXT_INT
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN _INT1_VRRP
	VPN 接口	BR_LAN _INT2_VRRP
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

5. 选择**创建**以创建并保存模板。

Branch_A_INET_TLOCEXT_VRRP

6. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

7. 使用以下参数配置设备模板：

设备型号：ISR 4351

模板名称：Branch_A_INET_TLOCEXT_VRRP

说明：分支机构双广域网边缘设备混合 TLOC 扩展，具有 INET 以及 LAN 端中继和 VRRP

Branch_A_INET_TLOCEXT_VRRP **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
	VPN 接口	BR_TLOC_EXT_INT
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN _INT1_VRRP
	VPN 接口	BR_LAN _INT2_VRRP
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

8. 选择**创建**以创建并保存模板。

Branch_B_MPLS_INET(DHCP)

9. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

10. 使用以下参数配置设备模板：

设备型号：ISR 4331

模板名称：Branch_B_MPLS_INET(DHCP)

说明：分支机构单广域网边缘设备混合互联网 DHCP 地址，具有 LAN 中继

Branch_B_MPLS_INET(DHCP) **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT_DHCP
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

11. 选择**创建**以创建并保存模板。

Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

12. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

13. 使用以下参数配置设备模板：

设备型号：vEdge 100 B

模板名称：Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

说明：分支机构单广域网边缘设备混合互联网 DHCP 地址，具有 LAN 中继和 DHCP 服务器

Branch_B_MPLS_INET(DHCP)_LAN(DHCP) **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT_DHCP
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口 > DHCP 服务器	BR_LAN_DATA_DHCP_Server
	VPN 接口	BR_LAN_INT2
	VPN 接口 > DHCP 服务器	BR_LAN_VOICE_DHCP_Server
	VPN 接口	Loopback0
横幅		Banner_Template

模板类型	模板子类型	模板名称
策略		Branch_Policy
SNMP		SNMP_Template

14. 选择**创建**

Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

15. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

16. 使用以下参数配置设备模板:

设备型号：ISR 4351

模板名称：Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

说明：分支机构双广域网边缘设备混合 TLOC 扩展 SubInt，具有 MPLS BGP 以及 LAN 端 OSPF

Branch_C_MPLS_BGP_TLOCEXT_Subint_OSPF **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_SUBINT
	VPN 接口	BR_TLOC_EXT_INT
	VPN 接口	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface

模板类型	模板子类型	模板名称
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

17. 选择**创建**

Branch_C_INET_TLOCEXT_SubInt_OSPF

18. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

19. 使用以下参数配置设备模板：

设备型号：vEdge 1000

模板名称：Branch_C_INET_TLOCEXT_SubInt_OSPF

说明：分支机构双广域网边缘设备混合 TLOC 扩展 SubInt，具有 INET 以及 LAN 端 OSPF

Branch_C_INET_TLOCEXT_Subint_OSPF **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_SUBINT
	VPN 接口	BR_INET_INT

模板类型	模板子类型	模板名称
	VPN 接口	BR_TLOC_EXT_INT
	VPN 接口	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

20. 选择**创建**以创建并保存模板。

Branch_D_MPLS_CE_INET_LAN-Static-Routing

21. 选择**创建模板**，然后从下拉列表框中选择**从功能模板**。

22. 使用以下参数配置设备模板:

设备型号: vEdge 100 B

模板名称: Branch_D_MPLS_CE_INET_LAN-Static-Routingg

说明: 分支机构单广域网边缘设备混合，具有适用于 LAN 的 MPLS CE 和静态路由

Branch_D_MPLS_CE_INET_LAN-Static-Routing **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template

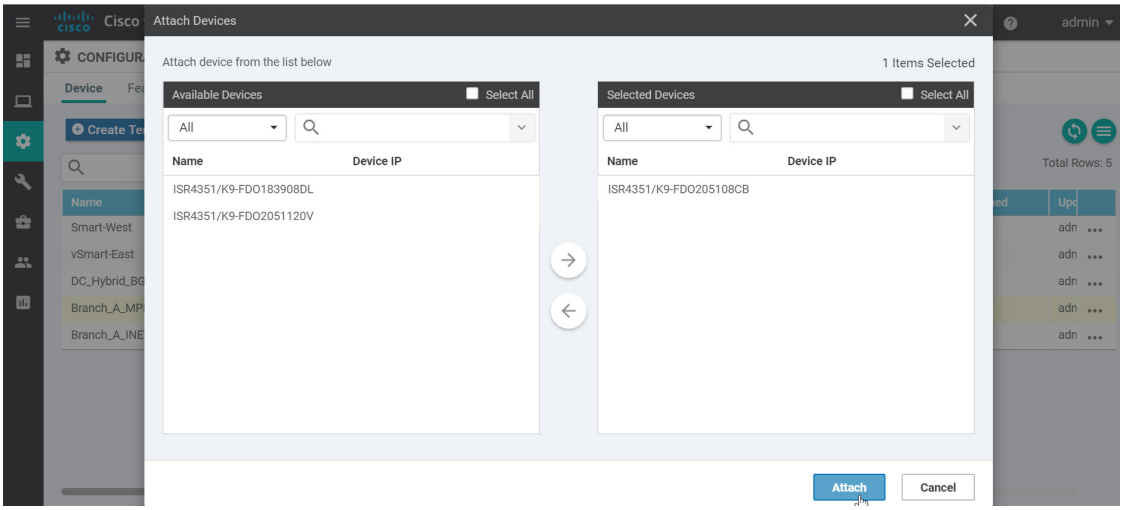
模板类型	模板子类型	模板名称
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

23. 选择**创建**以创建并保存模板。

程序 5：关联设备模板

在此程序中，您要将设备模板与广域网边缘分支机构路由器关联。当这些路由器变为活动状态并在网络中建立控制器连接时，vManage 会将完整配置推送给它们。

1. 依次转到**配置 > 模板**。确保选择**设备**选项卡。
2. 在所需模板 (**Branch_A_MPLS_BGP_TLOCEXT_VRRP**) 的旁边，选择 **...**，然后选择**关联设备**。
3. 选择连接到 MPLS 传输链路的分支机构 1 广域网边缘设备 1，即 br1-we1。您需要找到与此设备 (ISR 4351) 关联的序列号，因为此设备尚不在网络中。您可以在机箱外部找到序列号。或者，在 IOS XE 路由器上，可以从控制台执行 **show license udi** 命令查看序列号。对于 vEdge 路由器，可以从控制台执行 **show hardware inventory** 命令。授权序列号列表中所有 ISR 4351 路由器的序列号均应显示于弹出窗口中，因为这是所选设备模板的设备类型。选择序列号，然后选择箭头，以将设备从**可用设备**行移到**选定设备**行。选择**关联**。



4. 与数据中心设备模板部署类似，您必须填写设备模板的变量值。选择设备右侧的 **...**，然后选择**编辑设备模板**。

5. 填写以下变量（通过 .csv 电子表格或手动填写）。

分支机构 1 广域网边缘设备 1 设备模板变量值

变量	值
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

变量	值
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

变量	值
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. 选择**更新**。在选择下一步之前，您可能需要下载 .csv 文件以保存变量值以便重复使用，然后再继续操作。
7. 选择**下一步**，然后选择**配置**。由于设备处于脱机状态，因此系统将在设备联机时关联配置。
8. 使用以下模板重复第 1 至 8 步。有关变量值，请参见附录 G。

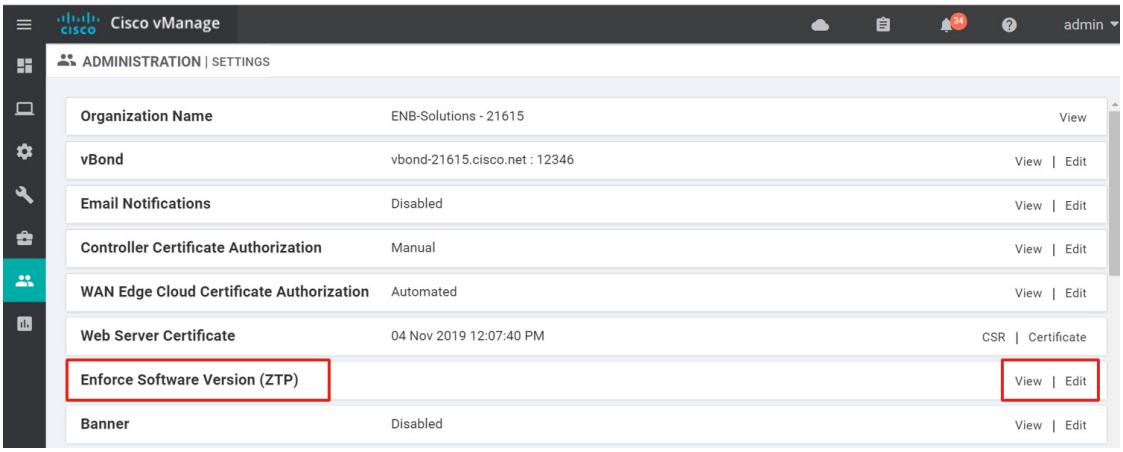
- BR1-WE2：Branch_A_INET_TLOCEXT_VRRP
- BR2-WE1：Branch_B_MPLS_INET(DHCP)
- BR3-WE1：Branch_B_MPLS_INET(DHCP)_LAN(DHCP)
- BR4-WE1：Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF
- BR4-WE2：Branch_C_INET_TLOCEXT_SubInt_OSPF
- BR5-WE1：Branch_D_MPLS_CE_INET_LAN-Static-Routing

程序 6：通过 ZTP 让远程 vEdge 路由器上线

在此程序中，将使用 ZTP 让分支机构 4 中的 vEdge（即 br4-we2）上线。还将通过 ZTP 流程执行软件升级。

vEdge 1000 路由器上的 ge0/0 接口配置为使用出厂默认设置的 DHCP。vEdge 路由器获得 IP 地址后，便会尝试解析 ztp.viptela.com 以查找其 vBond IP 地址并开始控制器的身份验证过程。

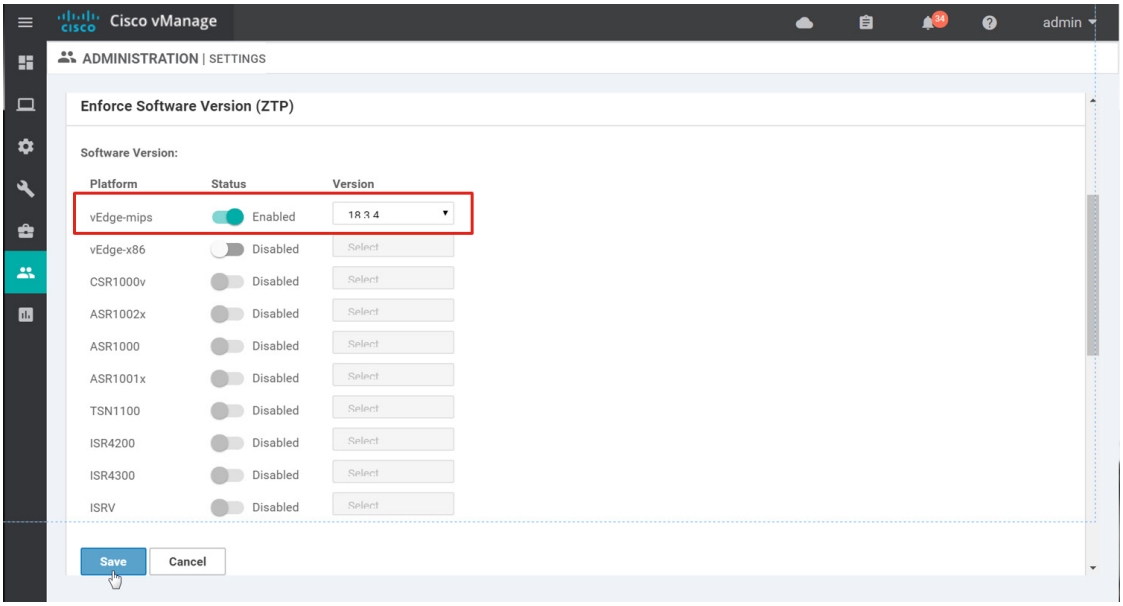
1. 要查看通过 ZTP 上线的 vEdge 路由器的代码版本，请在 vManage GUI 中依次转到**管理 > 设置**。找到**实施软件版本 (ZTP)** 配置。选择最右侧的**编辑**。



2. 在展开的部分下，找到所需平台 (**vEdge-mips**)，然后在**状态**下将滑块向右滑动，将状态更改为**启用**。在**版本**列下，选择要升级的软件版本 (18.3.4)。如果所需版本未作为可选择的选项列出，请依次转到**维护 > 软件存储库**添加所需版本。请注意，**vEdge-mips** 选项是指思科 vEdge 100、1000 和 2000 型号，而 **vEdge-x86** 选项是指思科 vEdge Cloud 和 vEdge 5000 型号。

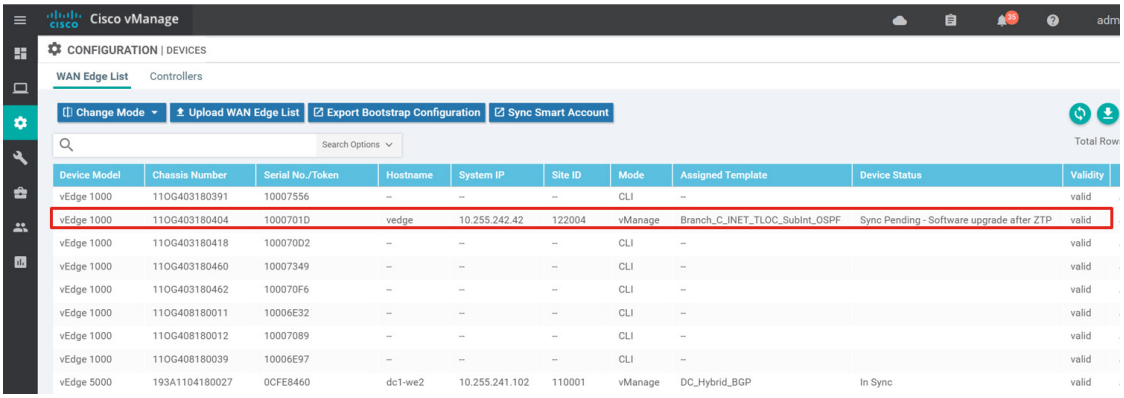
3. 选择**保存**。

技术提示：vManage 代码版本 18.3 不支持在 PnP 流程中进行 IOS XE SD-WAN 代码升级。

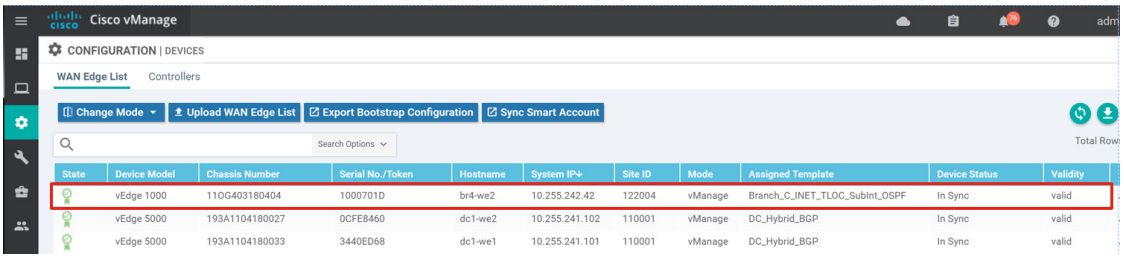


Br4-we2 已安装到网络中。它是 vEdge 1000，它的 ZTP 端口 ge0/0 插入在互联网传输链路中。假设 br4-we2 采用出厂默认设置，目前运行的是 17.2.7 版软件。

4. 接通 vEdge 路由器电源。vEdge 连接到 ZTP 服务器，然后对 vBond 及其他控制器进行身份验证。然后升级代码。



5. 推送完整配置，vEdge 路由器开始与 vManage 保持同步。



6. 通过 ZTP 或手动引导过程启动其他 vEdge 设备。请参阅**部署数据中心广域网边缘路由器**部分，查看手动引导过程的示例。

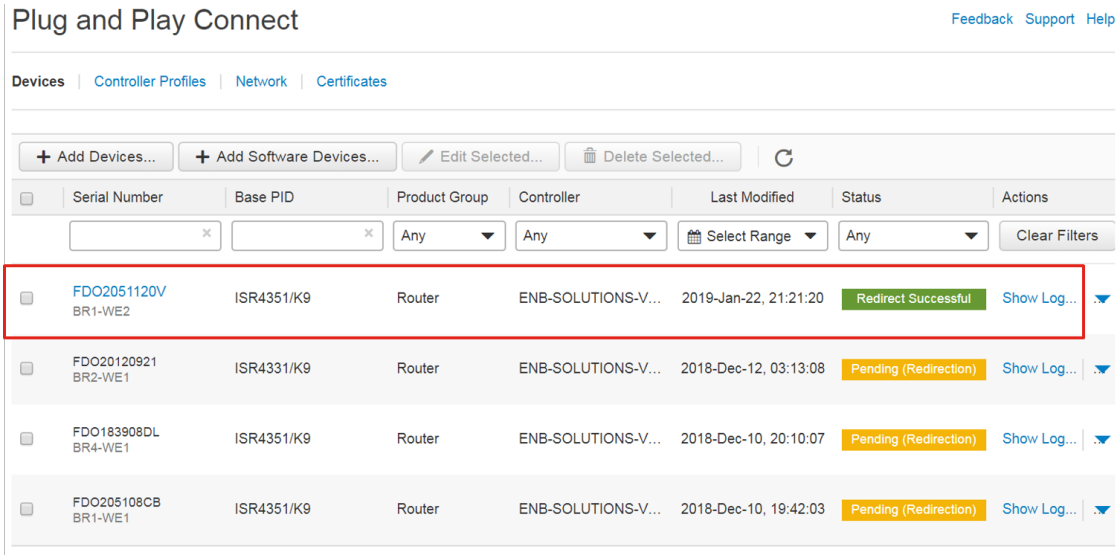
程序 7：通过 PnP 使远程 IOS XE SD-WAN 路由器上线

在此程序中，使用 PnP 使分支机构 1 中的 IOS XE SD-WAN 路由器（即 br1-we2）上线。在经过测试的此 vManage 版本中，PnP 不支持软件升级。PnP 流程在物理接口上使用 DHCP 来检索 IP 地址。IOS XE SD-WAN 路由器获得 IP 地址后，便会尝试解析 **devicehelper.cisco.com** 并联系 PnP 服务器，以便查找其 vBond IP 地址并开始向控制器进行身份验证的过程。

1. 确保将 SD-WAN 设备信息输入 PnP 门户中。有关详细信息，请参阅附录 C。

2. Br1-we2 已安装到网络中。思科 ISR 4351 路由器上的 GigabitEthernet0/0/0 接口连接到互联网运营商。假设路由器已转换为 SD-WAN 映像（请参阅附录 B 中的流程）。

接通 IOS XE SD-WAN 路由器电源。获得 IP 地址后，路由器会与 PnP 服务器联系，然后 PnP 门户会将广域网边缘路由器重定向至 vBond。接下来，广域网边缘路由器会先向 vBond 随后向其余控制器进行身份验证。通过 PnP 将广域网边缘路由器重定向至 vBond 时，PnP 门户将指示**重定向成功**状态。



3. 通过 PnP 流程使任何其他 IOS XE SD-WAN 设备上线。有关手动引导方法，请参阅下一部分。

4. 根据需要使用 vManage 升级路由器。

程序 8：通过手动引导方法使远程 IOS XE SD-WAN 路由器上线

在此程序中，使用手动引导方法使分支机构 2 中的 IOS XE SD-WAN 路由器（即 br2-we2）上线。此方法使用最小配置来实现对 vBond 控制器的访问，并开始向其余控制器进行身份验证的过程。

1. 确保将 SD-WAN 设备信息输入 PnP 门户中。有关详细信息，请参阅附录 C。

2. Br2-we2 已安装到网络中并接通电源。思科 ISR 4351 路由器上的 GigabitEthernet0/0/0 接口连接到互联网运营商。假设路由器已转换为 SD-WAN 映像（请参阅附录 B 中的流程）。

3. 将控制台连接至路由器，并从路由器控制台输入以下命令：

```
config-transaction
```

或

```
config-t
```

4. 等待几秒钟，直至看到以下文本：**admin connected from 127.0.0.1 using console on Router**。输入以下命令与 vBond 建立基本连接：

```
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. 测试与 vBond 控制器的连接

```
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. 输入以下信息，以便路由器建立控制器连接

```
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. 验证与控制器的连接

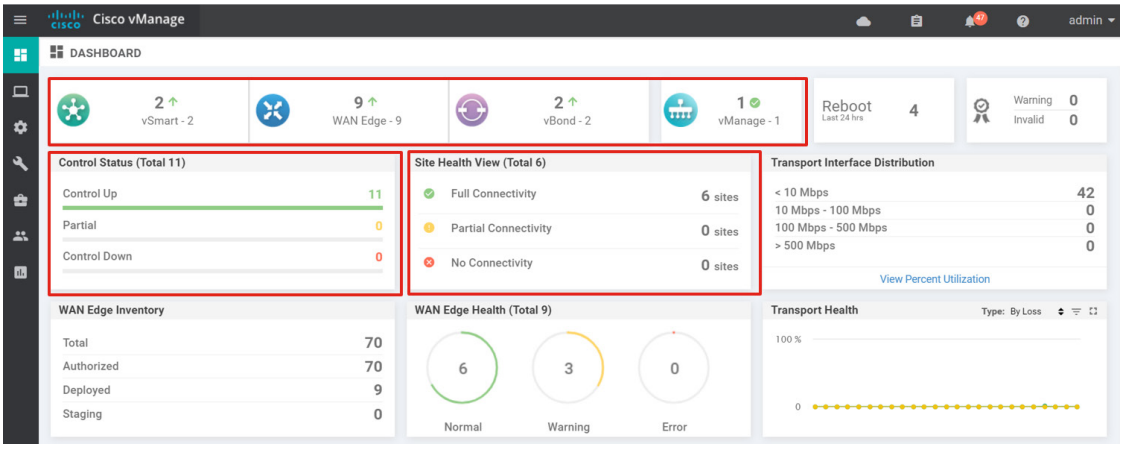
```
Router#show sdwan control summary
control summary 0
 vbond_counts    0
 vmanage_counts 1
 vsmart_counts   2
```

8. 启动任何其他 IOS XE SD-WAN 远程设备。

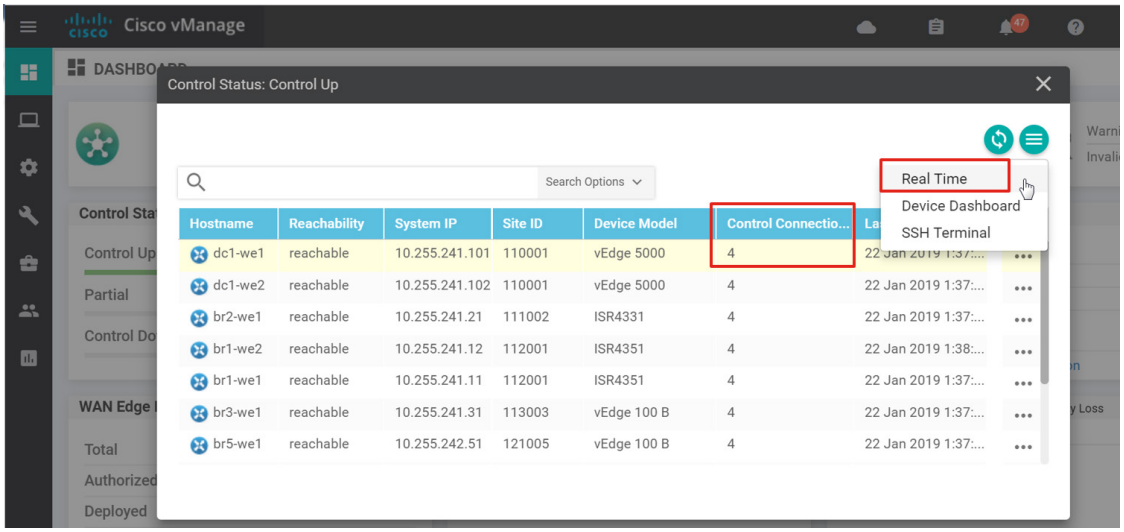
9. 根据需要使用 vManage 升级路由器。

程序 9：验证网络状态

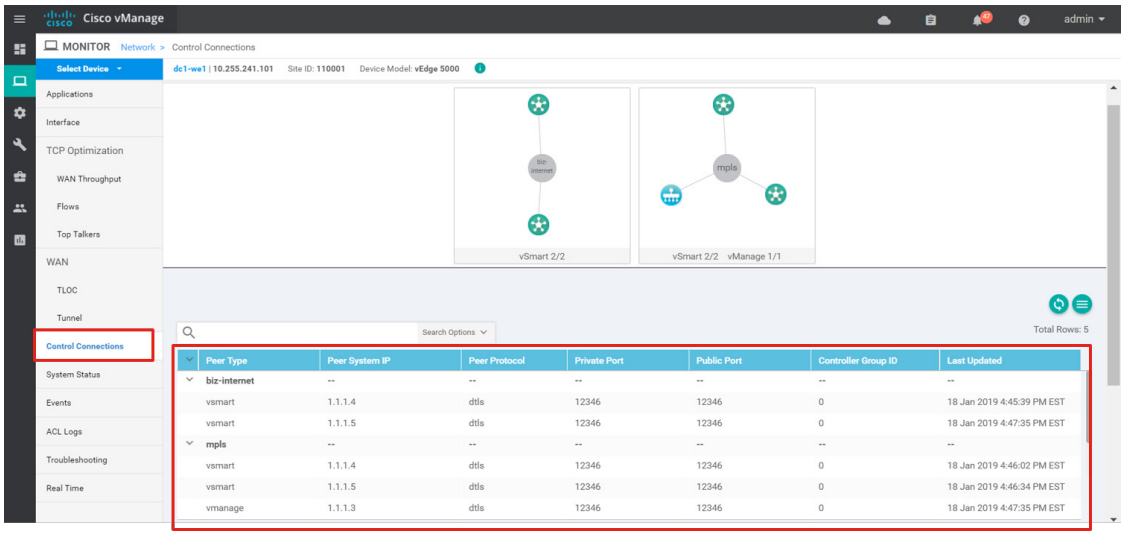
1. 验证网络的状态。vManage 应在控制面板顶部显示所有设备均可访问。**控制状态**应显示九台广域网边缘路由器和两个 vSmart 控制器的所有控制连接均已建立，并且**站点运行状况视图**应显示**完全连接**到六个站点（数据中心和五个分支机构）。这意味着每台广域网边缘设备都能通过每条传输链路连接到所有其他广域网边缘设备。请注意，因为配置了限制关键字，所以只有 MPLS 连接的广域网边缘路由器才能连接到其他 MPLS 连接的广域网边缘路由器。



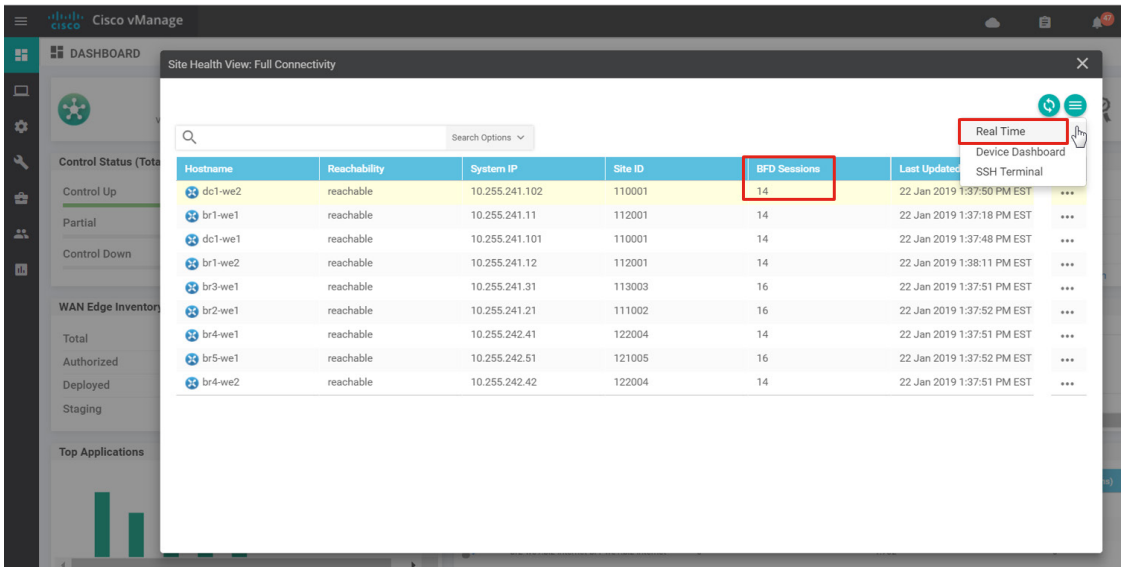
2. 如果在**控制状态**框中选择**控制开启、部分**或**控制关闭**，则系统会弹出一个窗口，其中汇总了每台广域网边缘设备所具有的控制连接数。这仅计算 vSmart 连接数。要获取更多信息，请选择所需设备右侧的 **...**，然后选择**实时**或**设备控制面板**。



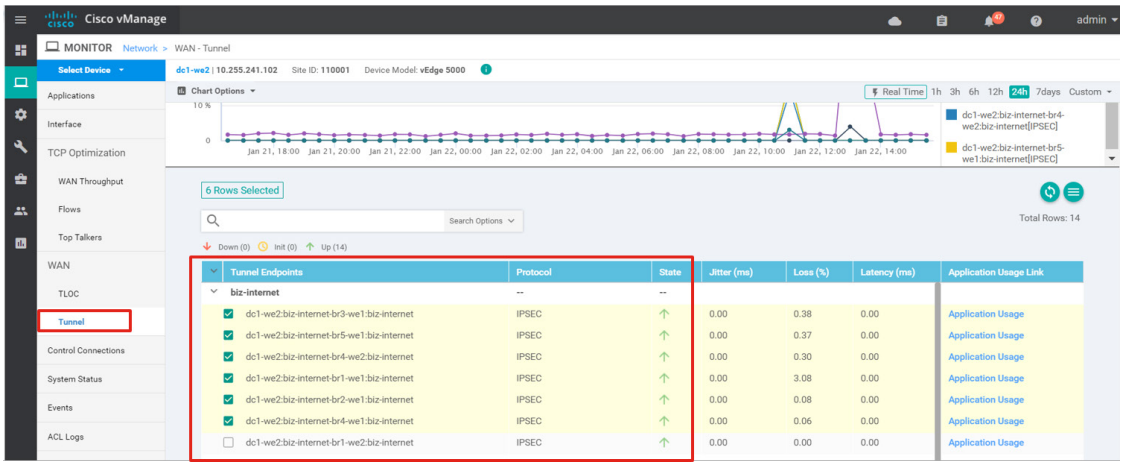
3. 要查看所有控制连接的状态，请选择左列中的**控制连接**。



4. 如果在控制面板的**站点运行状况视图**框中选择**完全连接、部分连接**或**无连接**，则系统会弹出一个窗口，其中汇总了每台广域网边缘设备所具有的 BFD 连接数。要获取更多信息，请在所需设备的右侧转到 **...**，然后选择**实时**或**设备控制面板**。



5. 要查看所有 IPSec 隧道或数据平面连接的状态，请在左列中的 WAN 类别下选择**隧道**。



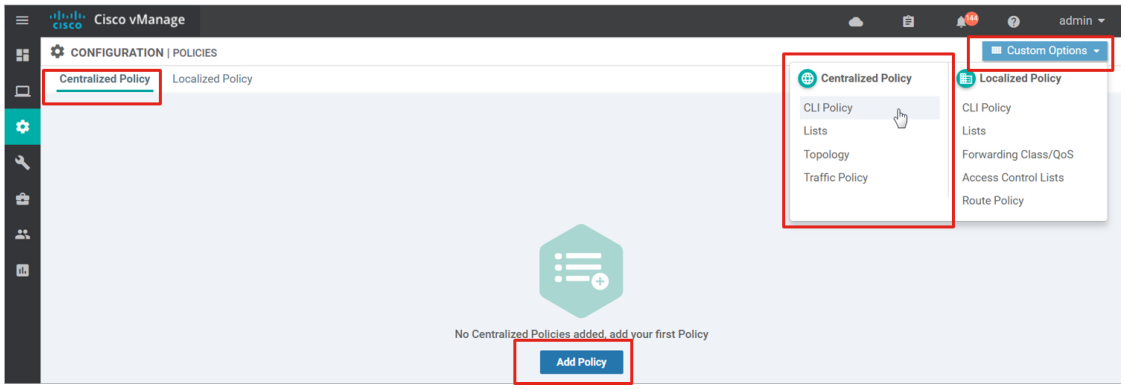
配置集中策略

在 vManage GUI 中，在**集中策略**选项卡下的**配置 > 策略**下配置集中策略。此页面将帮助您创建要下载到 vSmart 控制器的集中策略。

您可以选择**自定义选项**框以创建 CLI 策略，或定义列表，或在集中策略之外创建不同的策略定义。您可以单独创建策略定义，然后随时将其导入或关联到集中策略。一旦关联到集中策略，您就无法通过集中策略对策略定义进行任何编辑；您必须依次转到**配置 > 策略（集中策略**选项卡）页面上的**自定义选项**框，选择“拓扑”（用于控制策略）或“流量策略”（用于数据策略），显示策略定义列表以进行编辑。

当您在此主页上选择**添加策略**按钮时，实际上您正在开始定义集中策略，并且一次只能将一个集中策略下载到 vSmart 控制器。然后，您可以开始在集中策略中创建一系列控制或数据策略定义，然后将它们应用到站点和 VPN 列表。保存完成后，集中策略将下载到 vSmart 控制器。

图 17　vManage 集中策略部分



在创建集中策略时，有四个主要步骤：

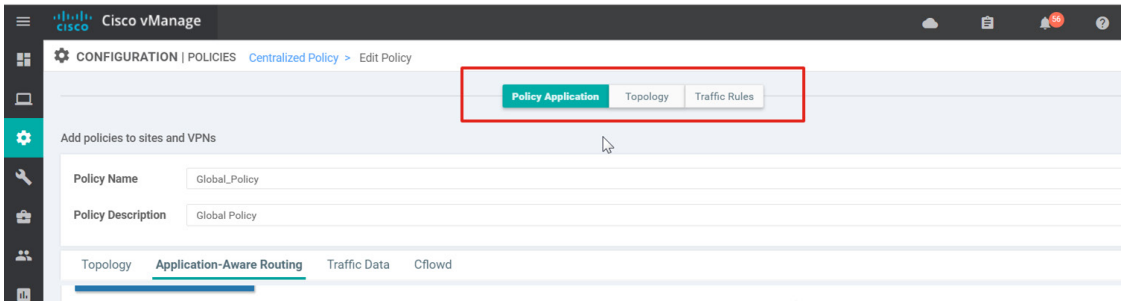
1. 创建兴趣组。在此部分中，您将创建将在策略中使用的列表，例如应用、颜色、数据前缀、策略器、前缀、站点、SLA 类、TLOC 和 VPN 列表。您至少需要创建站点 ID 列表才能应用各个策略定义。出于应用策略定义的目的创建站点 ID 时，不同列表中的站点 ID 不能存在重叠。您可能还需要可能应用策略的服务端 VPN 列表，以及策略序列中匹配和操作语句的列表。

2. 配置拓扑和 VPN 成员身份（控制策略）。在“拓扑和 VPN 成员身份”页面下，可以选择“拓扑”或“VPN 成员身份”选项卡。在“拓扑”选项卡下，您将能够配置控制策略。您可以从全网状或中心辐射型预定义策略中进行选择，也可以选择配置自己的自定义路由和 TLOC 策略定义。还可以将现有控制策略导入到集中策略中。在“VPN 成员身份”选项卡下，您可以创建允许或限制各个站点的 VPN 的策略定义。

3. 配置流量规则（数据策略）。在“流量规则”页面下，可以创建应用感知路由、流量数据或 Cflowd 策略。也可以导入已在集中策略之外创建的现有数据策略定义。

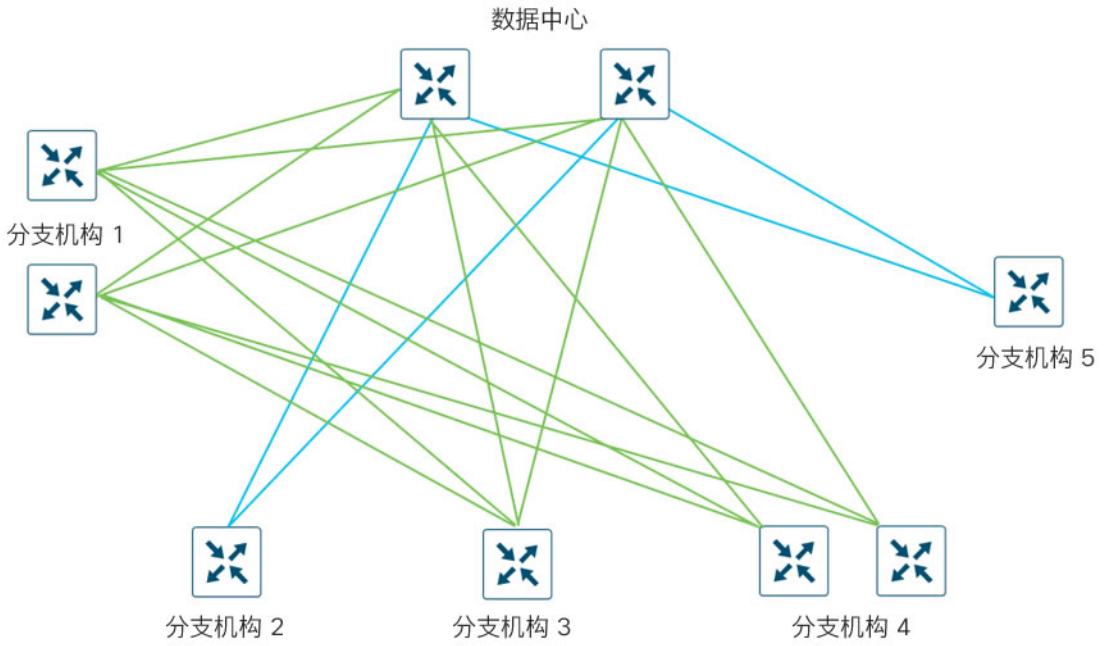
4. 将策略应用到站点和 VPN。在最后一步中，您将为新集中策略命名并对其进行说明。然后将各种策略定义应用到站点列表。可能还需要应用 VPN 列表。

如果要编辑现有集中策略，可以选择页面顶部的相应框导航至**拓扑**和**流量规则**页面，以配置或导入新策略。创建或导入后，您需要导航回**策略应用**并将策略定义关联到站点列表。



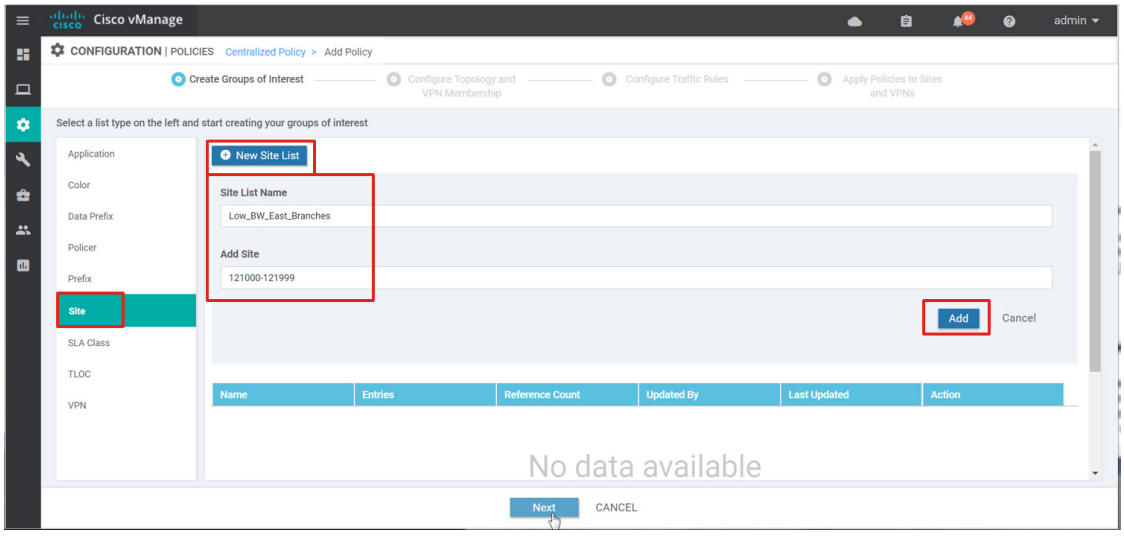
对于示例网络，创建集中策略以为低带宽站点（分支机构 2 和 5）创建中心辐射型拓扑。在下图中，分支机构 2 和 5 仅与数据中心 vEdge 路由器形成 IPSec 隧道。这是通过过滤路由和 TLOC 路由来完成的。

图 18　分支机构 2 和 5 的中心辐射型拓扑



1. 依次转到**配置 > 策略**，并确保选择**集中策略**选项卡。选择**添加策略**。

2. 创建各种站点的列表。在左列中选择**站点**。选择**新建站点列表**，然后在**站点列表名称**下键入 **Low_BW_East_Branches**。然后**添加站点**下键入 **121000-121999**。选择**添加**。



3. 重复第 2 步，创建以下列表:

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**

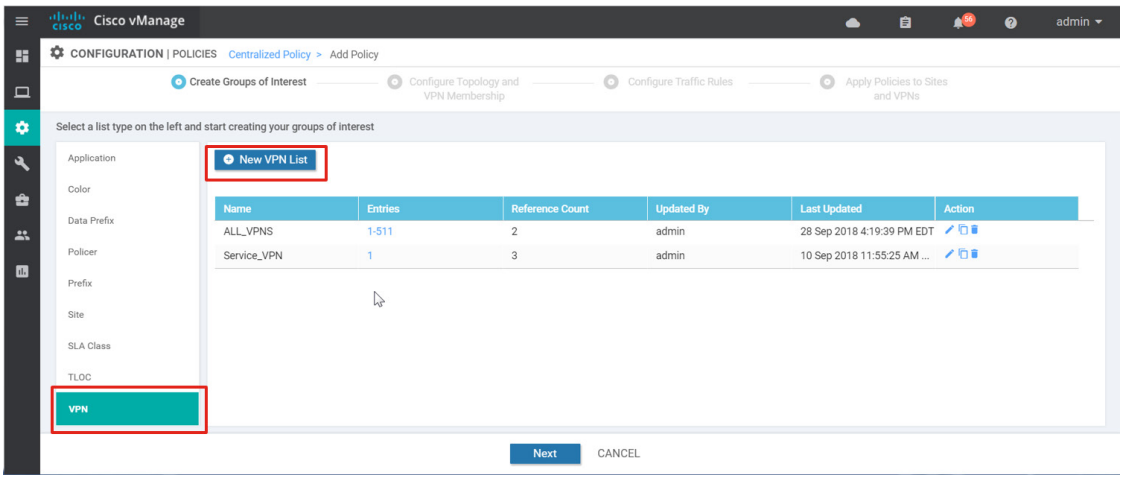
e. **ALL_SITES: 0-4294967295**

f. **All_US_Sites: 110000-129999**

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

4. 创建一个 VPN 列表。该策略将应用到服务端 VPN（即 VPN 1）。选择左侧的 **VPN**，然后选择**新建 VPN 列表**。键入 VPN 列表名称 (**Service_VPN**)，然后在**添加 VPN** 文本框中键入 **1**。选择 **Add（添加）**。

5. 添加另一个名为 **ALL_VPNS** 的 VPN 列表，包含 VPN 列表 **1-511**。选择**添加**。



6. 选择**下一步**。您现在将配置拓扑和 VPN 成员身份。

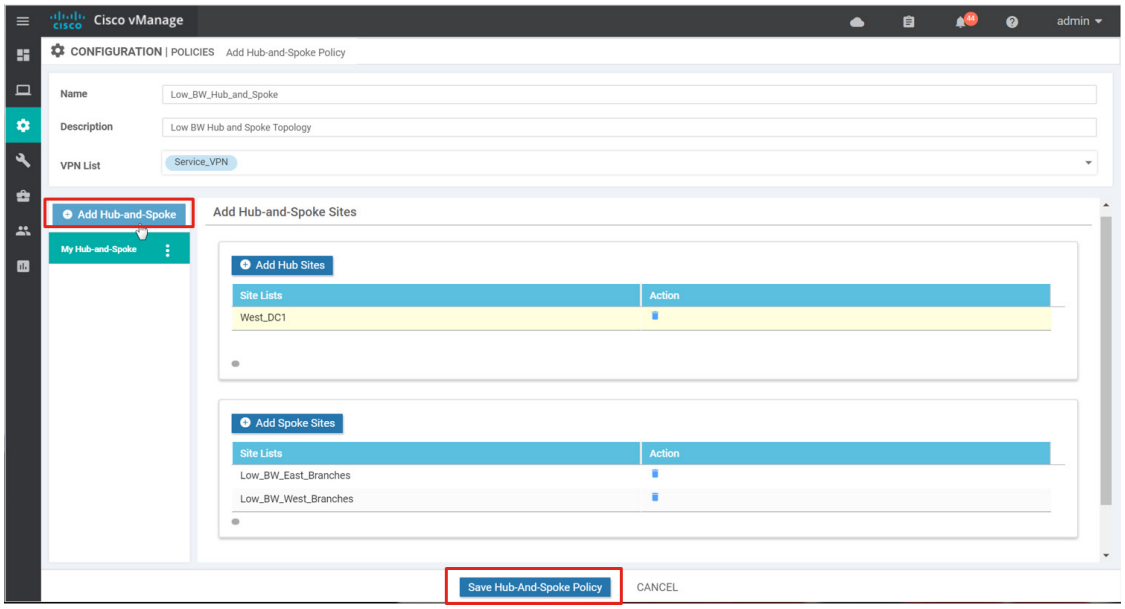
7. 确保您位于**拓扑**选项卡，然后选择**添加拓扑**。从下拉菜单中选择**中心辐射型**。

8. 输入名称 (**Low_BW_Hub_and_Spoke**) 和说明（**低带宽中心辐射型拓扑**）。从 VPN 列表中选择 **Service_VPN** 列表。

9. 选择**添加中心站点**。在站点列表下，选择 **West_DC1**，然后选择**添加**。

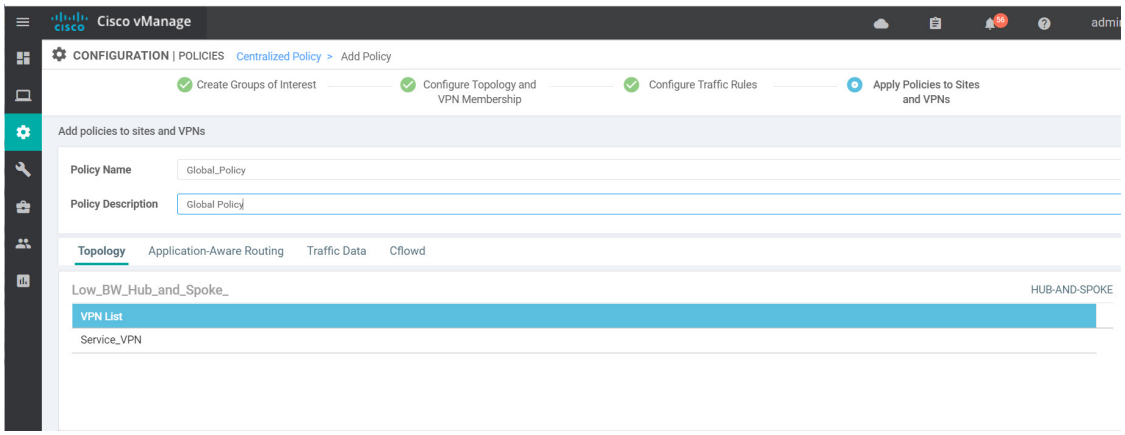
10. 选择 “添加分支站点”。选择 **Low_BW_East_Branches**，然后选择 “添加”。对 **Low_BW_West_Branches** 重复上述步骤。

11. 选择页面底部的**保存中心辐射型策略**。您刚刚完成了需要应用到站点列表的策略定义。



12. 选择**下一步**。再次选择**下一步**，跳过**流量规则**页面。

13. 在此页面上为集中策略命名。键入**策略名称** (**Global_Policy**) 和**策略说明**（**全局策略**），然后选择**保存策略**。

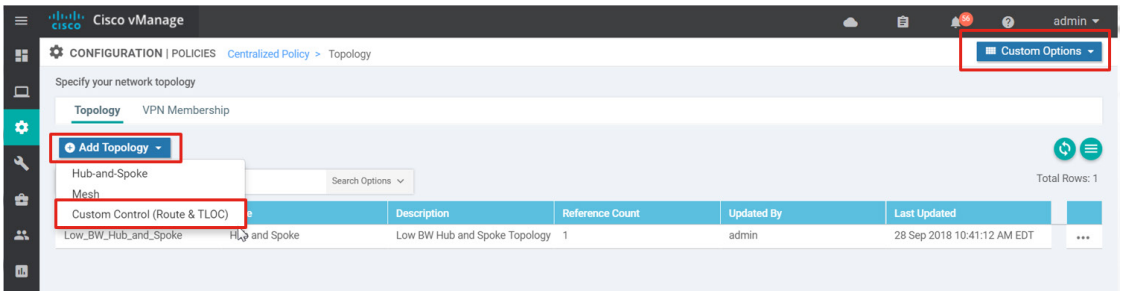


技术提示：使用预定义中心辐射型拓扑策略时，只有来自数据中心站点的 TLOC 和路由会分发到指定的低带宽站点。如果您希望在使用此策略时低带宽站点通过中心到达其他远程站点，请确保从数据中心分发汇总或默认路由。

请注意，高带宽站点仍然具有来自分支机构 2 和 5 的路由和 TLOC 信息，并尝试与这些分支机构形成 IPSec 隧道，但低带宽分支机构没有回到任何其他分支机构的连接。在这种情况下，您将在 vManage 控制面板中看到部分连接。解决此情况的一种简单方法是实现亦可从低带宽站点过滤路由和 TLOC。这将作为 vSmart 控制器上的出站策略应用到高带宽站点，因此仅过滤到高带宽站点的路由和 TLOC（将不更改到数据中心的路由和 TLOC）。如果需要通过数据中心站点连接到低带宽站点，则假定从数据中心站点为该连接通告某种汇总或默认值。

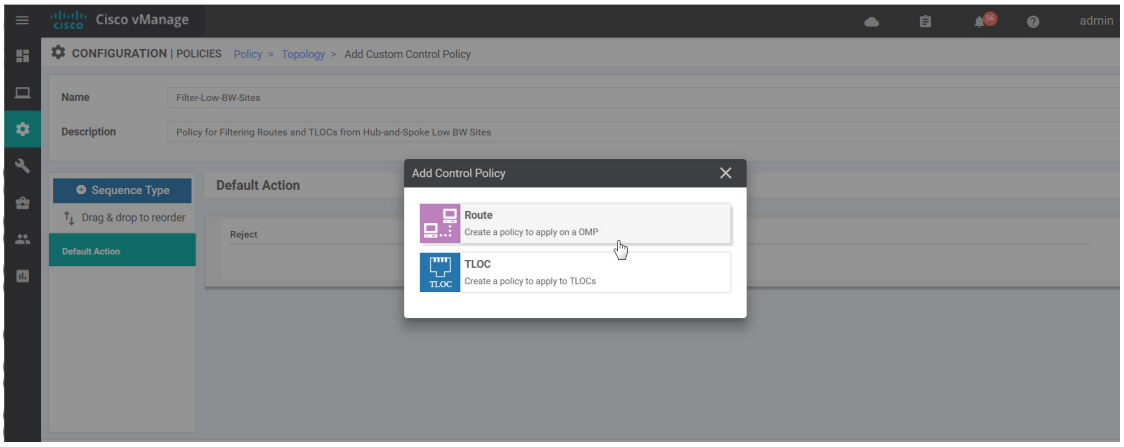
14. 在**配置 > 策略**页面上，选择页面右上角的**自定义选项**。从下拉菜单中选择**拓扑**，因为您要添加其他控制策略定义。

15. 选择**添加拓扑**，然后从下拉列表中选择**自定义控制（路由和 TLOC）**。



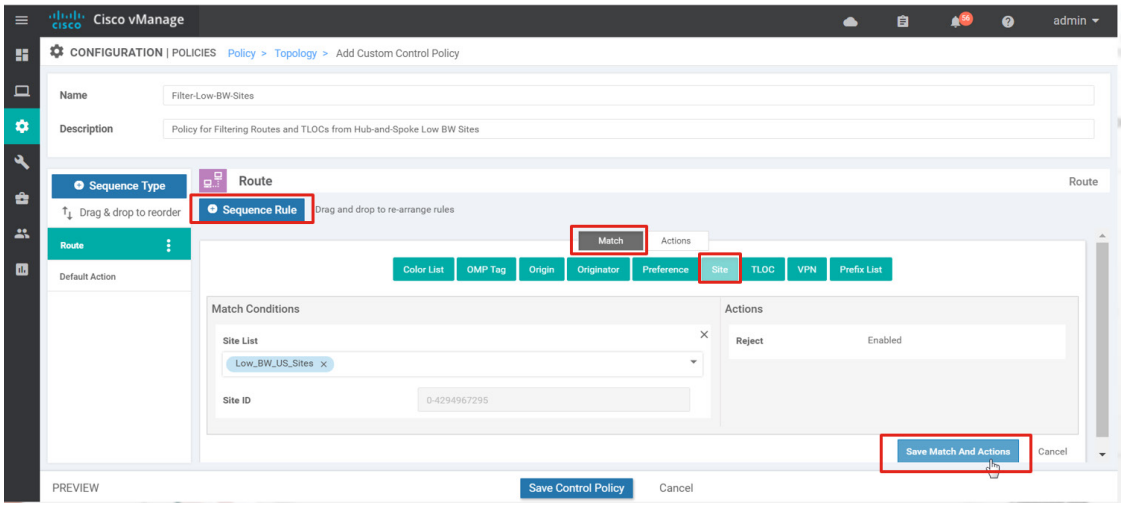
16. 输入名称 (**Filter-Low-BW-Sites**) 和说明（**用于过滤来自中心辐射型低带宽站点的路由和 TLOC 的策略**）。

17. 选择页面左侧的**序列类型**，然后在**添加控制策略**弹出窗口中，选择**路由**。



18. 选择**序列规则**。**匹配项**框将突出显示。选择**站点**，然后在**站点列表**下，选择 **Low_BW_US_Sites**。在**操作**下，默认值已设置为**拒绝**。

19. 选择**保存匹配项和操作**。

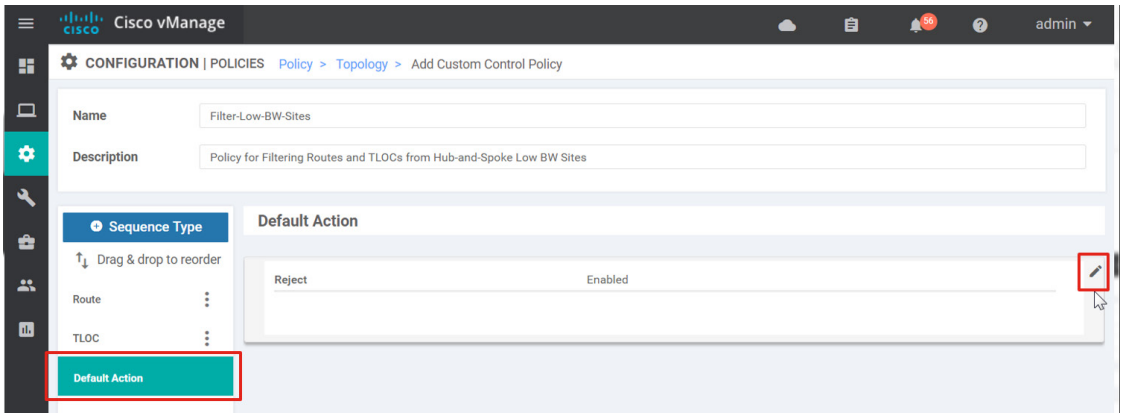


20. 选择页面左侧的**序列类型**，然后在**添加控制策略**弹出窗口中，选择 **TLOC**。

21. 选择**序列规则**。**匹配项**框将突出显示。选择**站点**，然后在**站点列表**下，选择 **Low_BW_US_Sites**。在**操作**下，默认值已设置为**拒绝**。

22. 选择**保存匹配项和操作**。

23. 从左列中选择**默认操作**。选择最右侧的**编辑**符号。选择**接受**框，然后选择**保存匹配项和操作**。

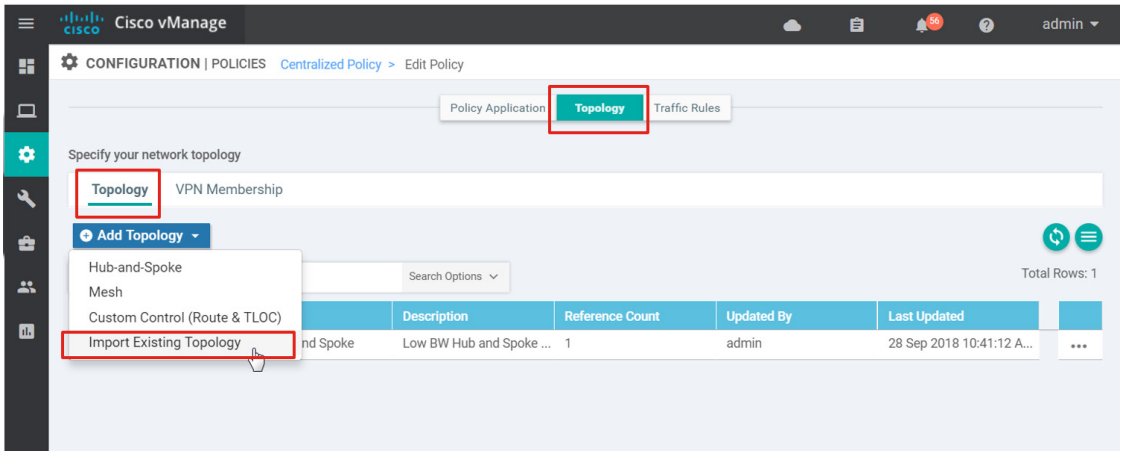


24. 选择**保存控制策略**以保存策略定义。

25. 由于策略定义是在名为 **Global_Policy** 的集中策略之外创建的，因此需要将其导入 **Global_Policy** 并应用到站点列表。依次转到**配置 > 策略**并确保已选择**集中策略**选项卡。

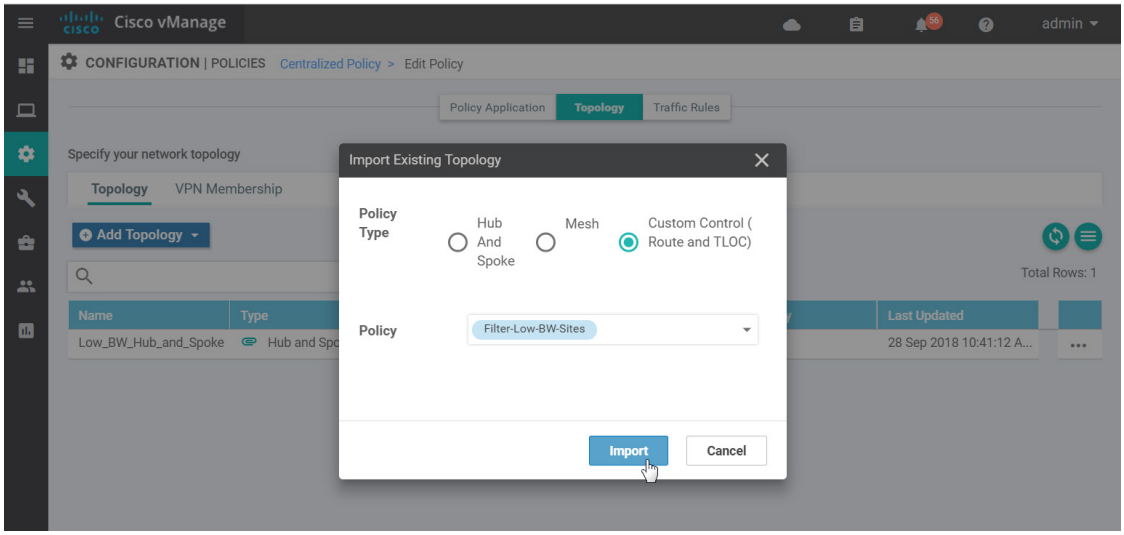
26. 选择名为 **Global_Policy** 的策略最右侧的 **...**，然后从下拉菜单中选择**编辑**。

27. 选择页面顶部的**拓扑**框。从下拉菜单中选择**添加拓扑**和**导入现有拓扑**。



28. 在**策略类型**的旁边，选择**自定义控制（路由和 TLOC）**单选按钮，然后在**策略**的旁边，从下拉列表框中选择 **Filter-Low-BW-Sites**。

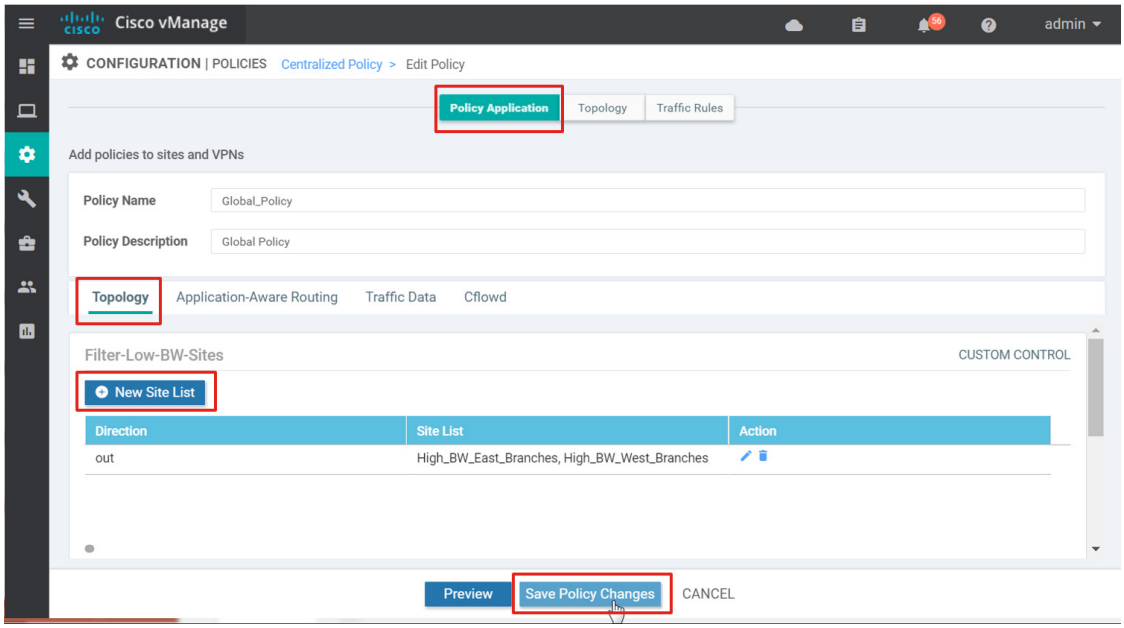
29. 选择**导入**。



30. 现在已导入策略定义，请选择页面顶部的**策略应用**框，以配置要将策略定义应用到的站点列表。

31. 在 **Filter-Low-BW-Sites** 部分下，选择**新建站点列表**，在**出站站点列表**下，选择 **High_BW_East_Branches** 和 **High_BW_West_Branches**。选择 “添加”。

32. 选择**保存策略更改**。



33. 现在已创建策略，可以将其与 vSmart 控制器关联并激活。在**集中策略**选项卡的**配置 > 策略**下，选择名为 **Global_Policy** 的策略最右侧的 **...**。从下拉菜单中选择**激活**。

34. 系统会弹出一个窗口，指出该策略将应用到可访问的 vSmart (1.1.1.5，1.1.1.4)。选择**激活**。该策略将被推送到 vSmart 控制器，状态将指示成功。

配置应用感知路由策略

应用感知路由策略配置作为集中策略的一部分进行配置。它会影响广域网边缘路由器上从服务 (LAN) 端流向传输隧道 (WAN) 端的流量。系统会匹配流量并将流量放入 SLA 类，流量具有一定的丢包、抖动和延迟值。路由行为如下：

- 在满足 SLA 类的所有隧道上对流量进行负载均衡。如果任何隧道都不满足 SLA，则通过任何可用隧道发送流量。
- 如果策略中指定了首选颜色，则只要满足 SLA，就会通过首选颜色隧道发送流量。如果任何隧道都不满足 SLA，则通过任何可用隧道发送流量。
- 如果指定了备用 SLA 首选颜色，则在没有满足 SLA 的路径时使用该隧道。如果备用隧道不可用，则使用另一条路径。
- 可以在策略中使用限制关键字，这意味着，如果没有隧道可以满足 SLA，则会丢弃流量。
- 策略可以配置为没有默认操作，这意味着，如果流量与列表中的任何序列都不匹配，则根据路由协议正常路由该流量。或者，此默认流量可放入 SLA 类。

创建应用感知路由策略包括三个主要步骤:

- 创建任何列表。
  - 创建 SLA 类列表，其中包括 SLA 类名称以及任何性能特征，例如延迟、丢包和抖动。支持四个 SLA 类。
  - 为要匹配和分配 SLA 类的流量创建任何应用列表。这样，您就可以对应用进行分组，以便将该组作为一个整体加以引用。
  - 根据需要创建任何站点列表、VPN 列表或数据前缀列表。路由策略应用到站点列表和 VPN 列表。数据前缀可用于匹配策略中的流量。
- 创建应用感知路由策略，其中包含匹配流量，这些流量会被放入特定的 SLA 类中。
- 将策略定义应用到站点列表和 VPN 列表。

示例策略包括以下配置步骤:

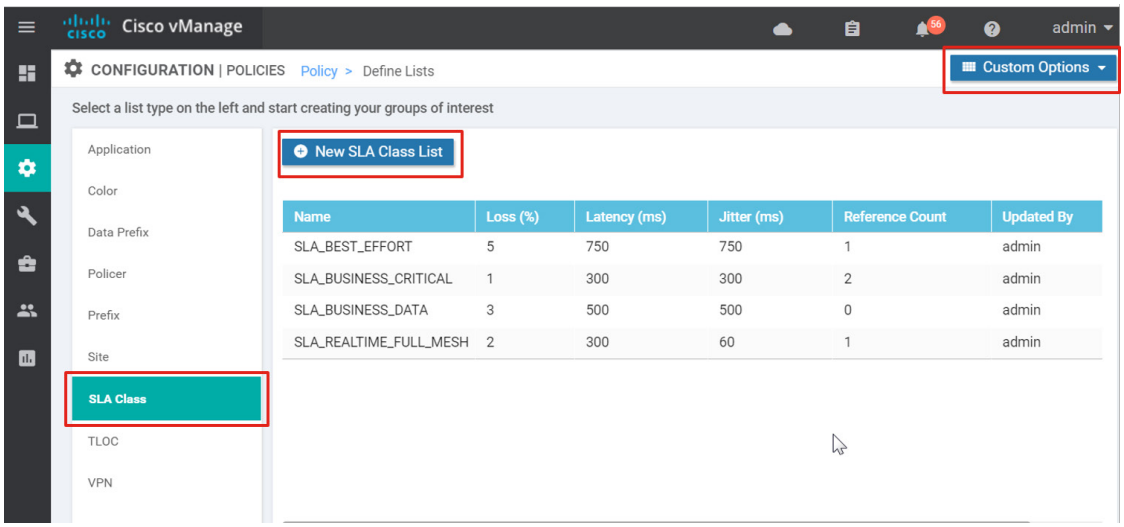
程序 1：创建列表

创建集中策略后，无法通过编辑策略来构建列表 - 您只能创建策略定义并通过集中策略配置应用它们。您需要在主策略页面上选择**自定义选项**才能修改或创建列表。

1. 在 vManage GUI 中，依次转到**配置 > 策略**。选择页面右上角的**自定义选项**，然后选择**集中策略**框中的**列表**。
2. 选择左侧的 **SLA 类**，然后选择**新建 SLA 类列表**。输入 **SLA 类列表名称**、**丢包率 (%)**、**延迟（毫秒）**和**抖动（毫秒）**。选择**添加**并对所有 SLA 类重复以上操作。使用以下设置:

应用感知路由策略 SLA **类列表（示例）**

SLA 类列表名称	丢包率 (%)	延迟（毫秒）	抖动（毫秒）
SLA_BEST_EFFORT	5	750	750
SLA_BUSINESS_CRITICAL	1	300	300
SLA_BUSINESS_DATA	3	500	500
SLA_REALTIME	2	300	60



3. 选择左侧的**应用**，然后选择**新建应用列表**。

4. 输入**应用列表名称**，然后选择几个应用作为列表的一部分。您可以在应用下拉搜索框中输入关键字来搜索各种应用。请注意，大多数应用都未缩写，这意味着 SSH 将显示为 Secure Shell，因此请适当调整关键字搜索。选择**添加**并对其他应用列表重复以上操作。使用以下设置示例:

应用感知路由策略应用列表（示例）

应用列表名称	应用
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. 创建数据前缀列表以在应用感知路由策略中使用。选择**数据前缀**，然后选择**新建数据前缀列表**。

6. 输入 “数据前缀列表名称” (**MGT_Servers**)，然后在 “添加数据前缀” 文本框中输入数据前缀列表 (**10.4.48.10/32,10.4.48.13/32,10.4.48.15/32,10.4.48.17/32**)。

7. 选择 **Add（添加）**。

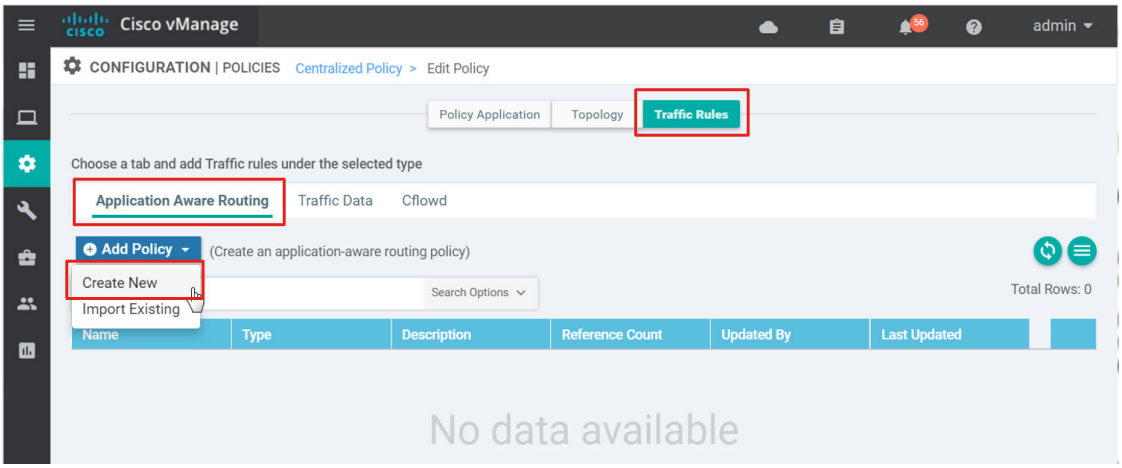
程序 2：创建应用感知路由策略

1. 依次转到**配置 > 策略**，并确保选择**集中策略**选项卡。

2. 在先前创建的集中策略 (**Global_Policy**) 旁边，选择页面右侧的 **...**，然后从下拉菜单中选择**编辑**。

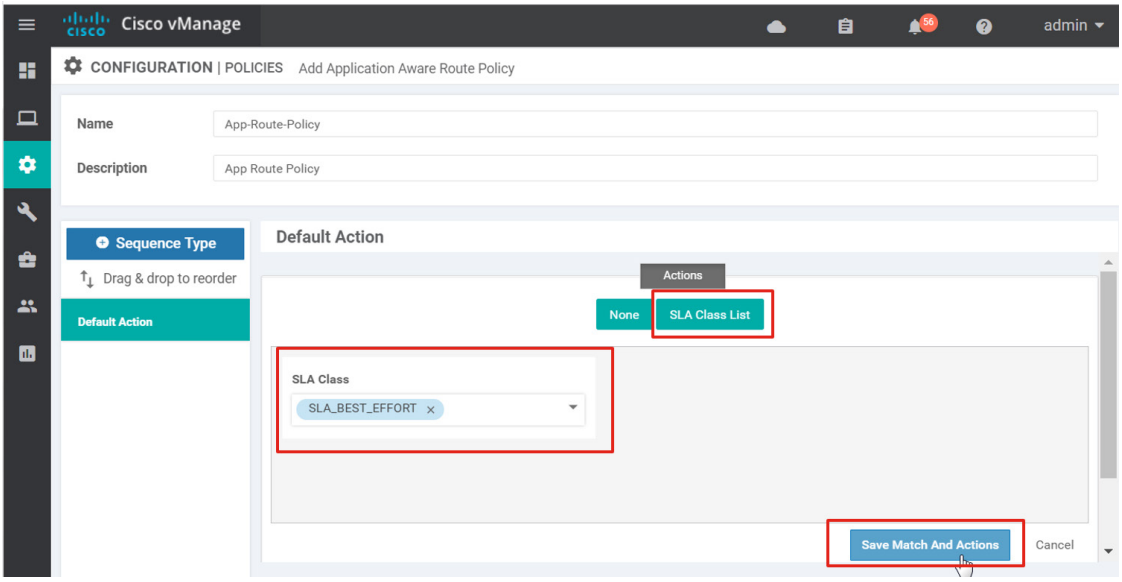
3. 应用感知策略是数据策略的一部分，在**流量规则**下列出。选择页面顶部的**流量规则**框，以在集中策略中创建新的应用感知策略。**应用感知路由**是此页面中的默认选项卡。

4. 选择**添加策略**，然后选择**新建**。



5. 输入策略定义的**名称**（**App-Route-Policy**）和**说明**（**应用路由策略**）。

6. 在**默认操作**下，选择**编辑**符号。默认值是 “无”。选择 **SLA 类列表**框，然后在 **SLA 类**文本框下，从下拉菜单中选择 **SLA_BEST_EFFORT**。选择**保存匹配项和操作**。

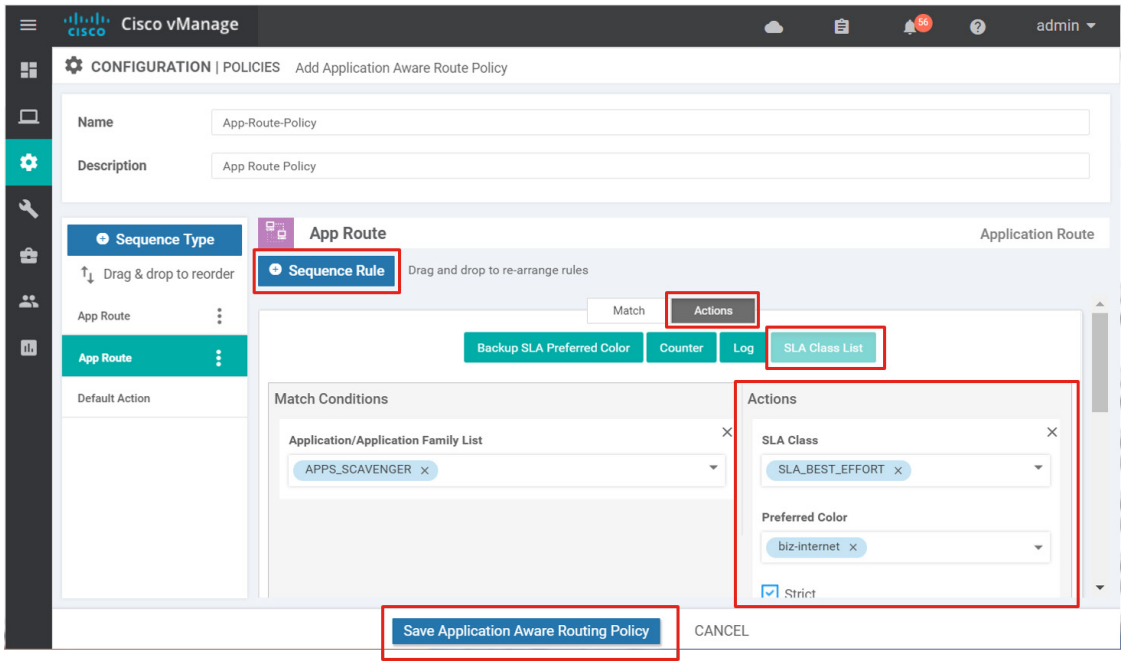


7. 选择左侧的**序列类型**，然后选择**序列规则**。

8. 选择**匹配**条件，然后选择**操作**框并选择操作。选择**保存匹配项和操作**。要添加另一个序列，请选择**序列规则**，然后重复上述操作。完成后，选择页面底部的**保存应用感知路由策略**。使用以下匹配项/操作选项示例：

应用感知路由策略应用路由策略（示例）

应用列表名称	应用
应用/应用系列列表：APPS_SCAVENGER	SLA 类：SLA_BEST_EFFORT 首选颜色：企业互联网 严格
DSCP：46	SLA 类：SLA_REALTIME 首选颜色：mpls
目标数据前缀：MGT_Servers	SLA 类：SLA_BUSINESS_CRITICAL
应用/应用系列列表： APPS_NETWORK_CONTROL	SLA 类：SLA_BUSINESS_CRITICAL
DSCP：10 12 14 18 20 22 26 28 30 34 36 38	SLA 类：SLA_BUSINESS_CRITICAL
DSCP：8 16 24 32 40 48 56	SLA 类：SLA_BUSINESS_DATA
DSCP：0	SLA 类：SLA_BEST_EFFORT 首选颜色：企业互联网

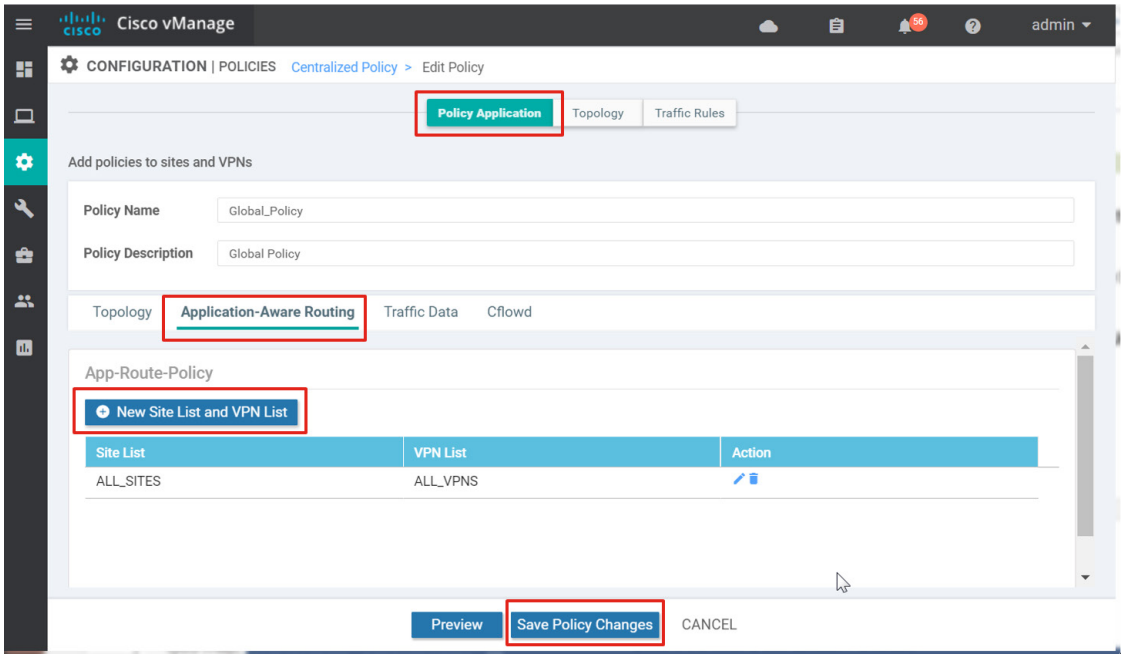


程序 3：应用策略定义

1. 现在已创建应用路由策略定义，请选择页面顶部的**策略应用**框。

2. 选择**应用感知路由**选项卡。在刚创建的策略定义下选择**新建站点列表和 VPN 列表**。

3. 选择**站点列表** (ALL_SITES)，选择 **VPN 列表** (ALL_VPNS)，然后选择**添加**。



4. 选择**保存策略更改**。

5. 系统将显示弹出窗口，指出该策略将应用到可访问的 vSmart 控制器。选择**激活**。系统会将该策略下载到 vSmart 控制器。

为 DPI 配置对称流量

DPI 在示例应用路由策略中用于对某些应用进行分类，并将这些应用放入不同的 SLA 类中。为使广域网边缘路由器上的 DPI 能够对大多数应用流量进行分类，广域网边缘路由器必须能够看到两个方向的网络流量。为确保双广域网边缘路由器站点的对称性，流量应在重叠的 LAN 到 WAN 和 WAN 到 LAN 这两个方向上都首选一个路由器。

在以下示例中，在 LAN 到 WAN 方向上，流量将受到影响:

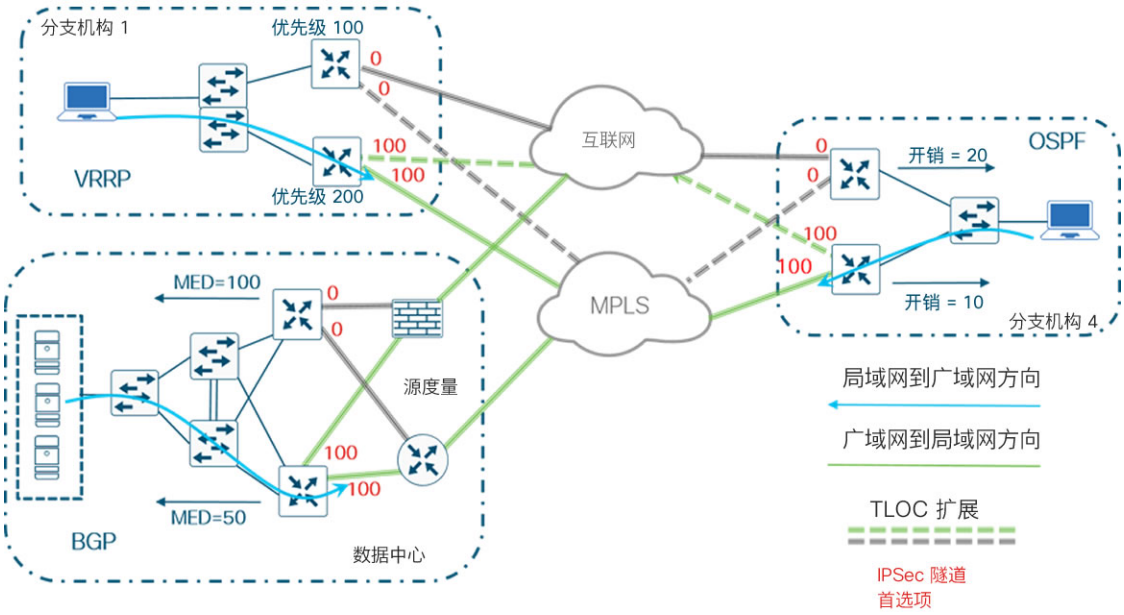
- 对于 VRRP，通过设置 VRRP 优先级
- 对于 OSPF，通过创建路由策略来修改从 OMP 分发到 OSPF 的路由的度量
- 对于 BGP，通过创建路由策略来修改从 OMP 分发到 BGP 的路由的 MED（度量）

在 WAN 到 LAN 方向上，流量将受到影响:

- 使用 IPSec 隧道首选项

每个双广域网边缘路由器站点的广域网边缘设备 1 将被选为流量的主广域网边缘路由器。

图 19　配置对称流量



程序 1：影响从 LAN 到 WAN 的流量

如何影响 LAN 到 WAN 方向的流量取决于本地站点上运行的协议。以下是如何使用 VRRP、OSPF 和 BGP 影响流量的说明。

VRRP

在 BR1-WE1 上将 VRRP 优先级设置为 200 并在 BR1-WE2 上将 VRRP 优先级设置为 100 时，已在分支机构 1 的广域网边缘路由器上将 VRRP 配置为首选 BR1-WE1。

OSPF

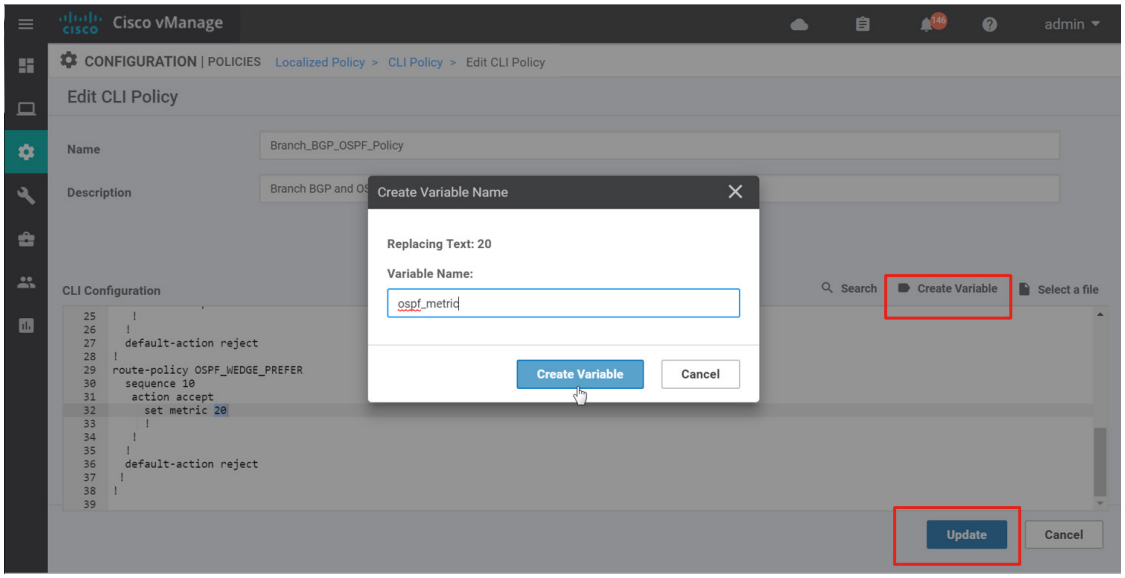
对于 OSPF，创建路由策略，修改从 OMP 重新分发到 OSPF 的路由的度量。

1. 依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。
2. 编辑 **Branch_BGP_OSPF_Policy**。选择所需策略最右侧的 “...”，然后选择**编辑**。
3. 将以下路由策略添加到现有策略中：

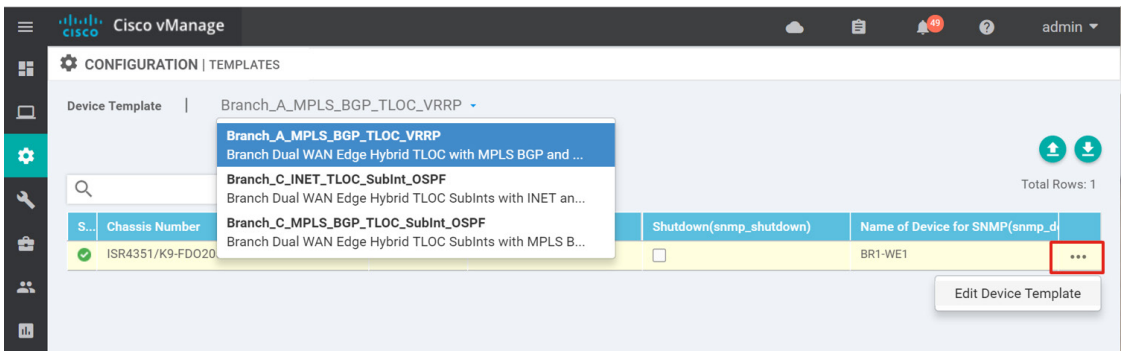
```
route-policy OSPF_WEDGE_PREFER
 sequence 10
  action accept
    set metric 20
    !
  !
```

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

4. 突出显示策略的**设置度量**行中的 **20**，然后选择**创建变量**。在弹出窗口的文本框中输入 **ospf_metric**，然后选择**创建变量**。选择**更新**以保存策略配置。



5. 在将更新后的策略推送到广域网边缘路由器之前，需要先为与该策略关联的所有广域网边缘路由器定义变量值 **ospf_metric**。所有三个设备模板都列在 GUI 左上角的下拉列表框中。选择设备模板时，与该设备模板关联的所有广域网边缘路由器都会显示在主屏幕上。在每台广域网边缘路由器的旁边，选择右侧的 **...**，然后选择**编辑设备模板**。

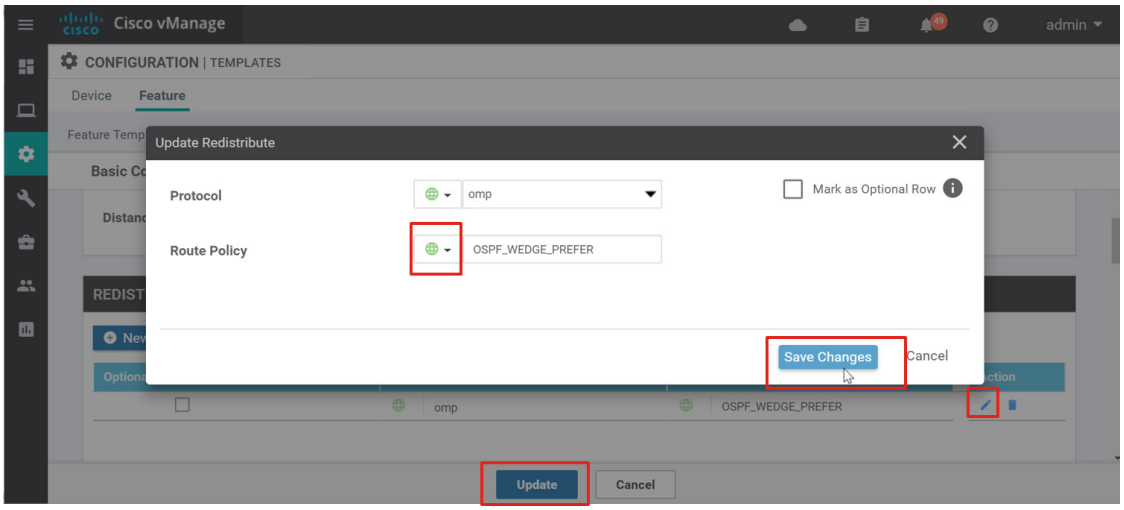


6. 填写必要的值。然后，选择**更新**并对其余设备模板重复上述操作。使用以下值。主路由器应获得较低的度量 (10)，而辅助路由器获得较高的度量 (20)。请注意，可以为 BR1-WE1 提供任何值，因为该设备的所有功能模板中都未使用 OSPF 路由策略。为了限制策略数量，我们选择在一个本地化策略中合并 BGP 和 OSPF 路由策略。

OSPF **度量值**

设备模板	设备	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. 选择**下一步**，然后选择**配置设备**。
8. 确认三台设备上的配置，然后选择**确定**。配置将被推出，屏幕将指示操作成功。
9. 更新策略后，可以在功能模板中引用路由策略。依次转到**配置 > 模板**，然后选择**功能**选项卡。
10. 编辑 **BR_LAN_OSPF** 功能模板
11. 在**功能模板**部分下，选择 OMP 协议旁边的**编辑**符号。
12. 在**路由策略**的旁边，选择**全局**，然后输入刚刚添加的路由策略 **OSPF_WEDGE_PREFER**。选择**保存更改**。
13. 选择**更新**以保存功能模板配置。

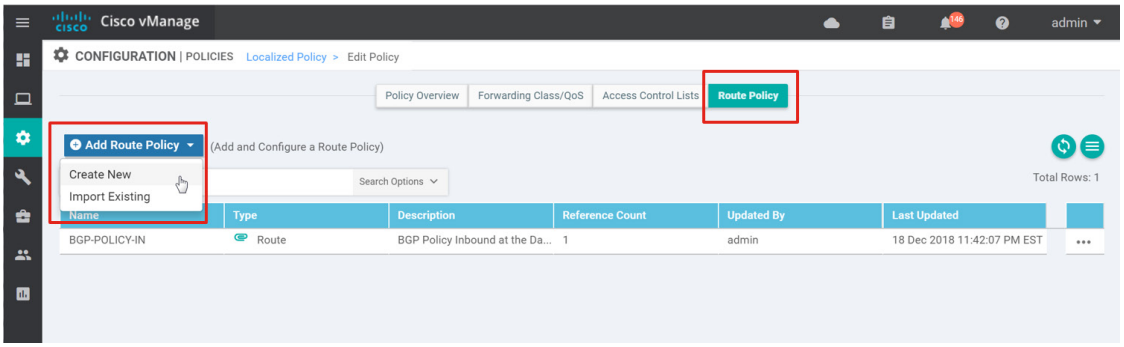


14. 选择**下一步**，然后选择**配置设备**。确认两台设备上的配置更改，然后选择**确定**。配置即被推出，屏幕将指示操作成功。

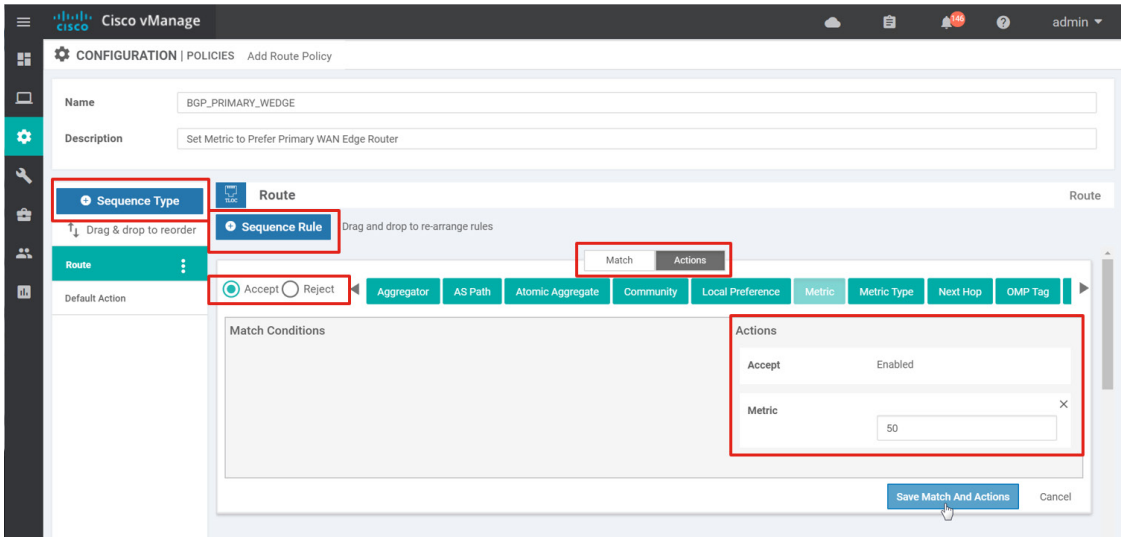
BGP

对于 BGP，创建路由策略，对数据中心内从 OMP 重新分发到 BGP 的路由设置 MED（度量）。数据中心本地策略是使用不允许使用变量的策略向导创建的，因此可以在名为 DC_Policy 的本地化策略中创建两个不同的路由策略。一个路由策略应用于主广域网边缘设备，另一个路由策略应用于辅助广域网边缘设备。

1. 依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。
2. 编辑 **DC_Policy**。选择所需策略最右侧的 "..."，然后选择**编辑**。
3. 选择页面顶部的**路由策略**框。
4. 点击**添加路由策略**按钮，然后从列表中选择**新建**。



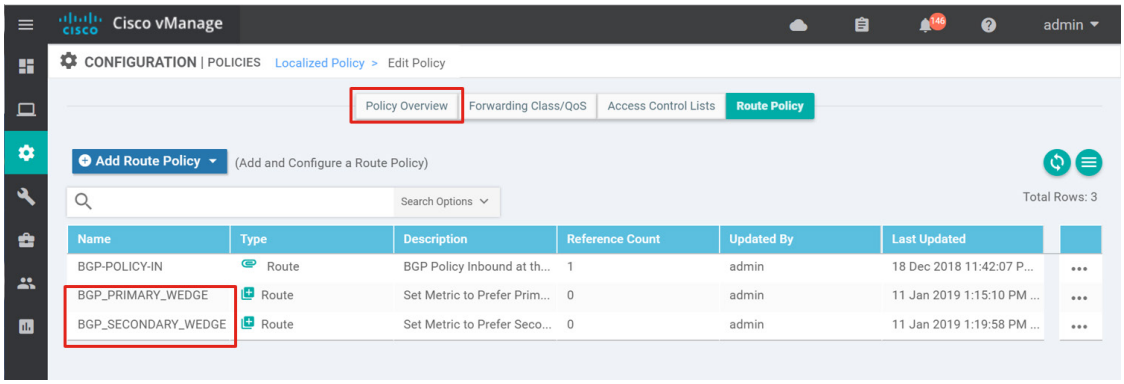
5. 填写新路由策略的名称 (**BGP_PRIMARY_WEDGE**) 和说明（**设置度量以首选主广域网边缘路由器**）。
6. 选择左侧的**序列类型**，然后选择**序列规则**。
7. 因为将匹配所有路由，所以请勿选择任何**匹配**条件。
8. 选择**操作**框，然后选择**接受**单选按钮。
9. 选择**度量**框，然后在文本框中输入 **50**。
10. 选择**保存匹配项和操作**。



11. 点击**保存路由策略**。

12. 重复上述步骤，使用**名称** (BGP_SECONDARY_WEDGE) 和**说明**（为辅助广域网边缘路由器设置度量）创建第二个路由策略。使用 100 作为**度量**。

13. 创建两个路由策略后，选择页面顶部的**策略概述**框。



14. 选择**保存策略更改**以保存本地化策略。配置更改将被推送到数据中心的 SD-WAN 路由器。

15. 选择**下一步**，然后选择**配置设备**

16. 确认两台设备上的配置，然后选择**确定**。配置将被推出，屏幕将指示操作成功。

17. 更新策略后，可以在功能模板中引用路由策略。依次转到**配置 > 模板**，然后选择**功能**选项卡。

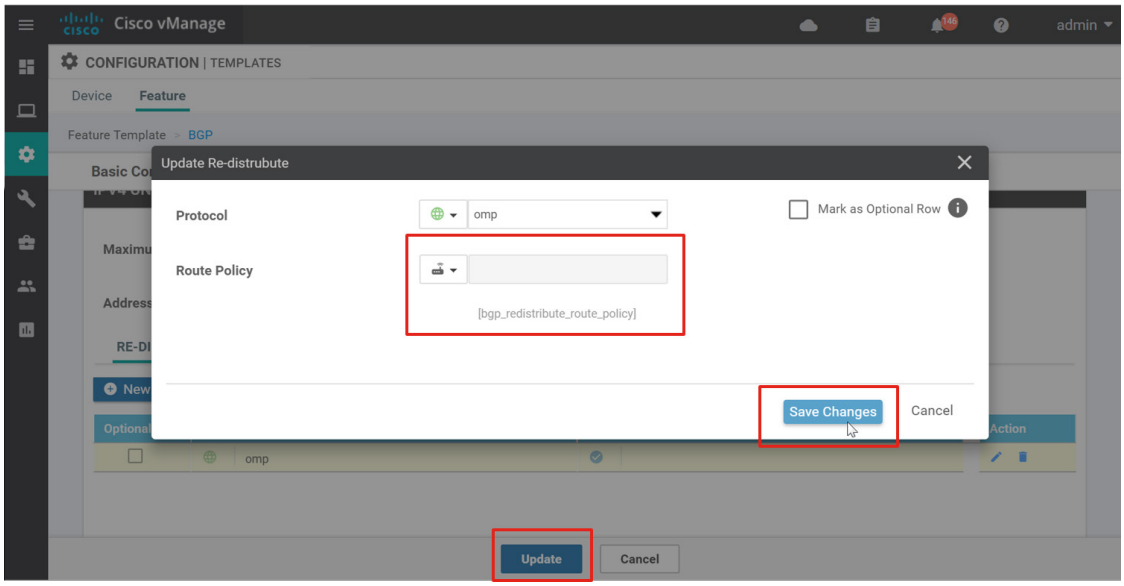
18. 编辑 **DC_LAN_BGP** 功能模板。

19. 在**重新分发**下的 **IPv4 单播地址系列**部分下，选择 OMP 协议旁边的**编辑**符号。

20. 在**路由策略**的旁边，选择**特定设备专用**并使用默认变量名称 **bgp_redistribute_route_policy**。

21. 选择**保存更改**。

22. 选择**更新**以保存功能模板配置。



需要先定义刚刚添加的路由策略变量，然后才可以推送配置。

23. 选择 **dc1-we1** 右侧的 **...**，然后从下拉列表中选择**编辑设备模板**。

24. 在路由策略 (bgp_redistribute_route_policy) 的旁边，输入 **BGP_PRIMARY_WEDGE**。

25. 选择**更新**。

26. 对 **dc1-we2** 重复上述步骤，使用 **BGP_SECONDARY_WEDGE** 作为路由策略。

27. 点击**下一步**，然后点击**配置设备**。确认两台设备上的配置更改，然后选择**确定**。配置即被推出，屏幕将指示操作成功。

程序 2：影响重叠上从 WAN 到 LAN 的流量

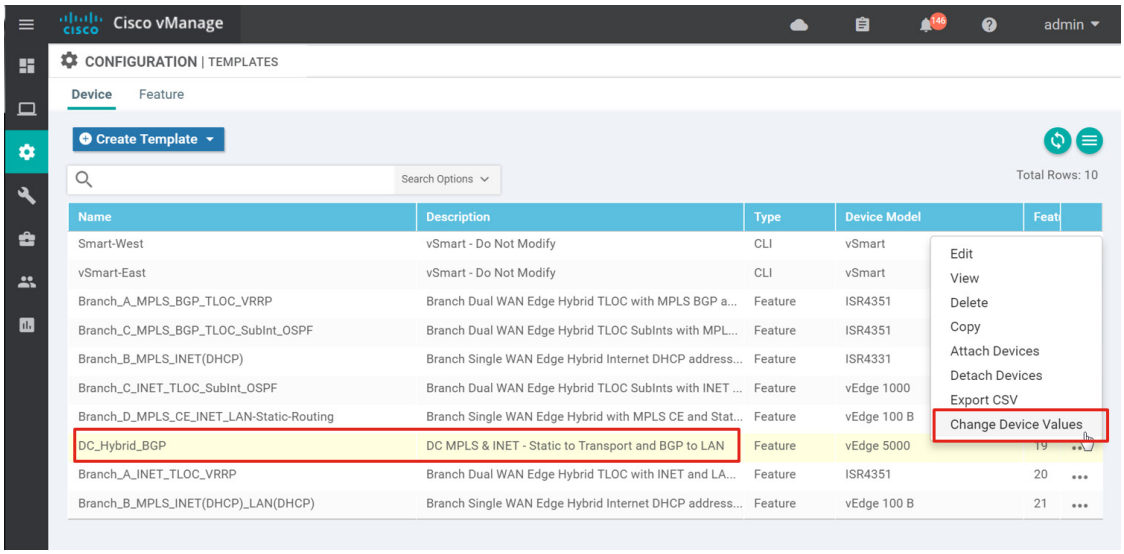
IPSec 隧道首选项

有多种方法可以影响重叠中从 WAN 到 LAN 方向的流量，但最简单的方法之一是通过 IPSec 隧道首选项。此参数包含在 MPLS 和互联网 VPN 接口以太网模板的 “隧道” 部分中，并且在创建功能模板时已为其创建了变量。最初，所有隧道的隧道首选项均设置为 0。通过将主广域网边缘设备的 IPSec 隧道首选项更改为 100，在双广域网边缘设备站点上将首选项更改为首选广域网边缘设备 1 而不是广域网边缘设备 2。只需要修改三个设备模板：

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

1. 依次转到**配置 > 模板**，并确保选择**设备**选项卡。

2. 转到 **DC_Hybrid_BGP** 设备模板的右侧，选择 **...**，然后从下拉菜单中选择**更改设备值**。



3. 在 **dc1-we1** 的右侧，选择 **...**，然后选择**编辑设备模板**。在 **vpn0_mpls_tunnel_ipsec_pref** 和 **vpn0_inet_tunnel_ipsec_pref** 的旁边，键入 **100**。**DC1-WE2** 值已设置为 0，因此无需修改。选择**更新**。

4. 选择**下一步**，然后选择**配置设备**。系统会显示弹出窗口，要求您确认两个设备上的配置更改。选中复选框，然后选择**确定**。系统随即将更新的配置推送到 vEdge 设备，并应指示操作成功。

5. 对设备模板 **Branch_A_MPLS_BGP_TLOCEXT_VRRP** 和 **Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF** 重复第 1 至 5 步。对于 BR1-WE1 和 BR4-WE1，将 **vpn0_mpls_tunnel_ipsec_preference** 和 **vpn0_inet_tunnel_ipsec_preference** 的隧道 IPSec 首选项值更改为 **100**。

配置服务质量

以下是配置六类 QoS 模型的示例。匹配流量的访问列表配置为集中数据策略，而不是本地化策略。访问列表显示了可以对流量进行分类的各种方式。还给出了重写策略的示例，其在外部隧道报头策略中重新标记 DSCP 以支持服务提供商的较小类别的 QoS 模型。

本示例中使用以下类别:

用于示例 QoS 策略的服务类别

类名	流量类型	DSCP 值
VOICE	语音流量	ef (46)
INTERACTIVE_VIDEO	交互式视频（视频会议）	af41、af42、af43（34、36、38）
BULK	批量数据（FTP、邮件、备份）	af11、af12、af13（10、12、14）
CONTROL_SIGNALING	路由以及语音和视频通话信令	cs6 (48)、cs3 (24)
CRITICAL_DATA	网络管理、事务、视频流、任务关键型	cs2、cs4、cs5、af21、af22、af23、af31、af32、af33（16、32、40、18、20、22、26、28、30）
CLASS_DEFAULT	尽力而为	所有其他

下表说明了每个转发类的带宽百分比和缓冲区百分比、拥塞避免算法以及外部隧道 DSCP 值:

带宽、拥塞避免和隧道 DSCP 值

服务类别	带宽（调度）	避免拥塞	用于重写策略的隧道 DSCP 值
VOICE	10（优先级队列）	---	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)

以下是配置服务质量所需的步骤:

1. 将每个 QoS 转发类映射到输出队列（本地化策略）。
2. 配置 QoS 调度程序，为每个转发类（本地化策略）分配调度方法、带宽百分比、缓冲区百分比和丢弃算法。
3. 创建 QoS 映射，对所有 QoS 调度程序分组（本地化策略）。
4. 创建重写策略（可选）（本地化策略）。
5. 定义用于匹配流量的访问列表并分配到转发类（本地化策略或集中策略）。

6. 将分类访问列表应用到接口（本地化策略或集中式策略）。在本地化策略中，通过在 VPN 接口以太网模板中引用访问列表来完成此操作。对于集中策略，通过将 QoS 数据策略应用到站点和 VPN 列表来完成此操作。

7. 将 QoS 映射和（可选）重写策略应用到出口接口（在 VPN 接口以太网模板中配置）。

程序 1：配置本地化策略

可以使用 CLI 策略或通过本地策略 GUI 来配置本地化策略。

CLI 策略

1. 依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。

2. 在 Branch_Policy 的右侧，选择 “...”，然后选择**编辑**。

3. 通过配置以下内容或将以下内容复制到已创建的本地化策略中，将 QoS 类映射到输出队列：

```
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. 通过配置以下内容或将以下内容复制到本地化策略中，为每个类配置 QoS 调度程序：

```
!
 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. 通过配置以下内容或将以下内容复制到本地化策略中，配置 QoS 映射以对 QoS 调度程序进行分组:

```
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
!
```

技术提示：对于 vEdge Cloud 和 vEdge 5000 路由器，要为传输端隧道接口启用 QoS 调度和整形，必须在策略中使用 **cloud-qos** 命令。此外，要为服务端接口启用 QoS 调度和整形，必须在策略中使用 **cloud-qos-service-side** 命令。

6. （可选）通过配置以下内容或将以下内容复制到本地化策略中，创建重写策略以修改隧道外部 DSCP 值：

```
!
 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
!
```

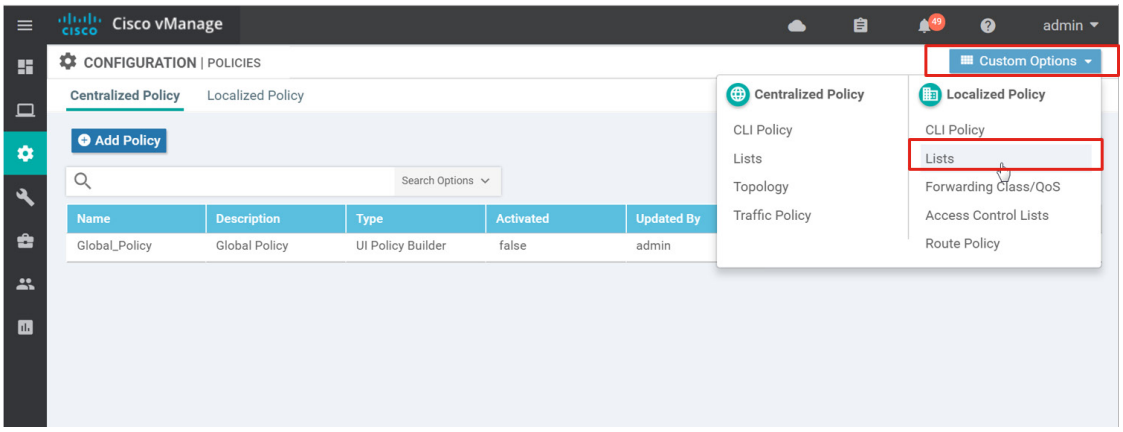
7. 选择**更新**，选择**下一步**，然后选择**配置设备**。选中相应复选框并选择**确定**，确认对配置的更改。修改后的本地化策略将下载到已使用 **Branch_Policy** 配置的设备。

8. 对另一分支机构策略 **Branch_BGP_OSPF_Policy** 以及任何其他策略重复第 1 至 7 步。

本地化策略 GUI

要使用本地化策略 GUI 配置 QoS，请先创建转发类并在 “列表” 部分将其分配到队列，然后再添加 QoS 映射来定义本地化策略中每个队列的特征。

1. 依次转到**配置 > 策略**，点击**自定义选项**按钮，然后选择**本地化策略**下的**列表**。

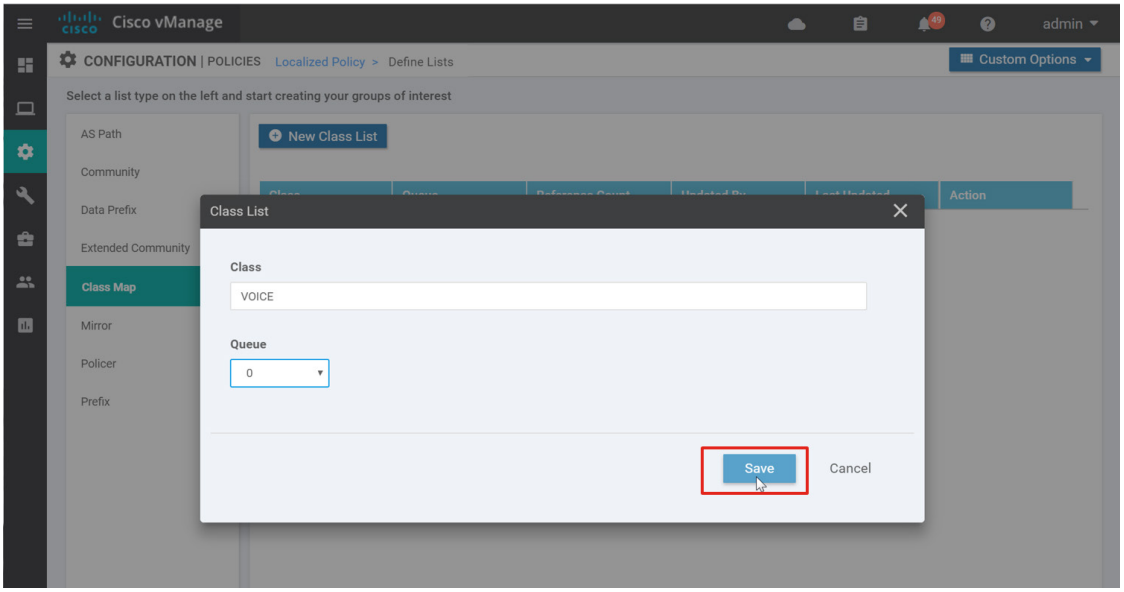


2. 选择左侧的**类映射**。

3. 点击**新建类列表**按钮。

4. 在**类**文本框下，输入 **VOICE**。在**队列**下，从下拉列表框中选择 **0**。

5. 点击**保存**。



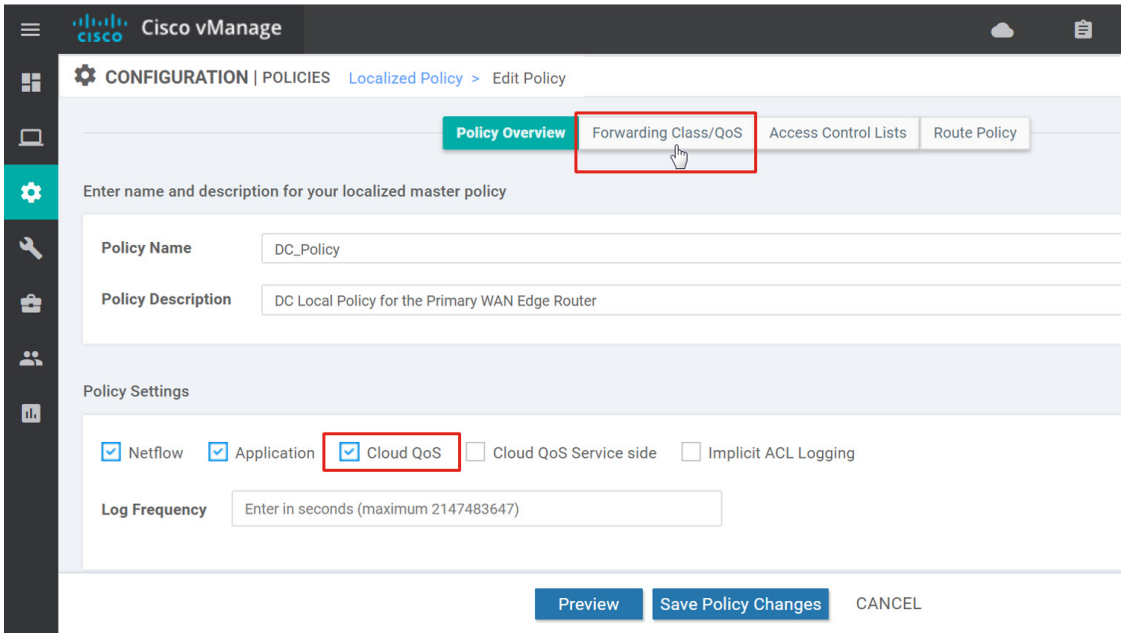
6. 重复前面三个步骤，添加其余类列表:

类列表和队列映射

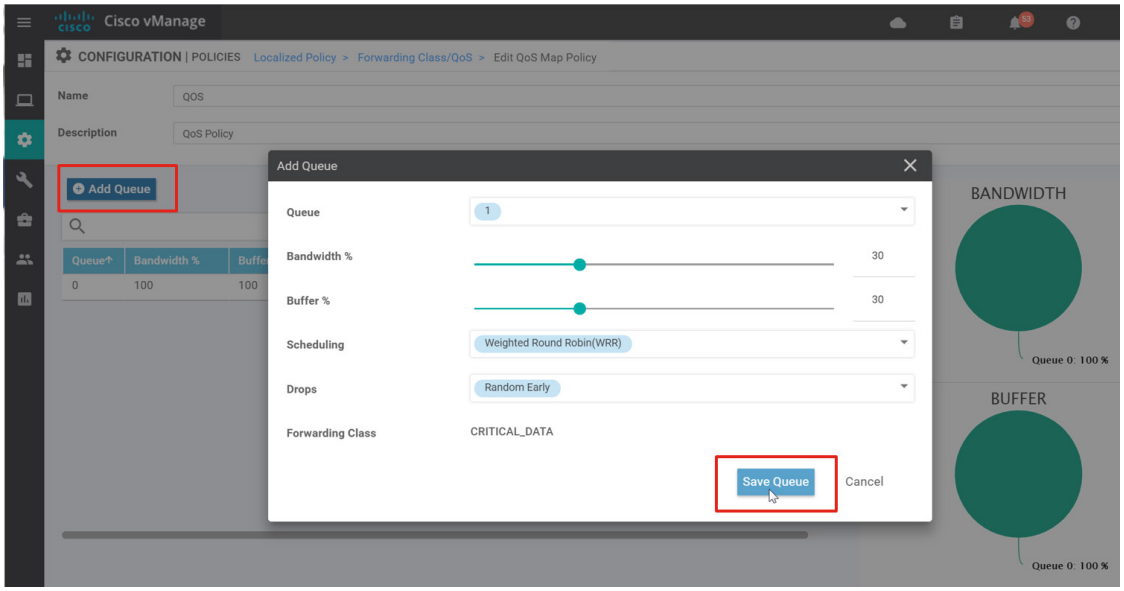
类	队列
VOICE	0
CRITICAL_DATA	1
BULK	2

类	队列
CLASS_DEFAULT	3
INTERACTIVE_VIDEO	4
CONTROL_SIGNALING	5

7. 接下来，依次转到**配置 > 策略**，然后选择**本地化策略**选项卡。
8. 在 **DC_Policy** 的右侧，选择 “...”，然后选择**编辑**。
9. 由于数据中心路由器是 vEdge 5000，因此请选中**云 QoS** 复选框以对传输端启用 QoS。
10. 点击页面顶部的**转发类/QoS** 框。



11. 在 **QoS 映射**选项卡中，点击**添加 QoS 映射**框，然后从下拉列表中选择**新建**。
12. 输入**名称** (**QOS**) 和**说明**（**QoS 策略**）。
13. 默认情况下已定义队列 0，且无法对其进行修改。点击**添加队列**按钮。
14. 在**队列**的旁边，选择 **1**。将**带宽 %** 和 **缓冲区 %** 滑块滑动到 **30**。在**丢弃**的旁边，从下拉列表框中选择**随机早期**。
15. 点击**保存队列**按钮。



16. 重复前面三个步骤，添加其余队列信息：

带宽和缓冲区值及丢弃算法

队列	带宽/缓冲区	丢弃
1	30/30	随机早期 (RED)
2	10/10	随机早期 (RED)
3	20/20	随机早期 (RED)
4	20/20	随机早期 (RED)
5	10/10	尾部丢弃

现在，应该还为 QoS 队列 0 留有 10% 的带宽和缓冲区。

17. 点击**保存策略**按钮。

18. 选择**策略重写**选项卡以添加重写策略（可选）。

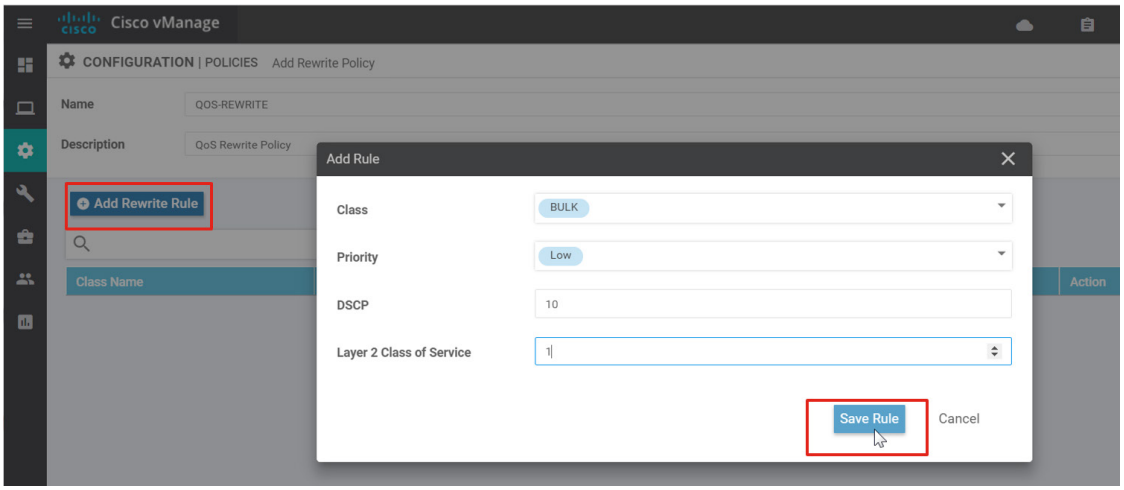
19. 点击**添加重写策略**按钮，然后选择**新建**。

20. 输入**名称** (**QOS-REWRITE**) 和**说明**（**QoS 重写策略**）

21. 点击**添加重写规则**按钮。

22. 在**类**的旁边，选择 **BULK**。在**优先级**的旁边，选择**低**。在 **DSCP** 的旁边输入 **10**，然后在**第 2 层服务类别**的旁边输入 **1**。

23. 点击**保存规则**按钮。



24. 重复前面三个步骤，添加其余重写信息：

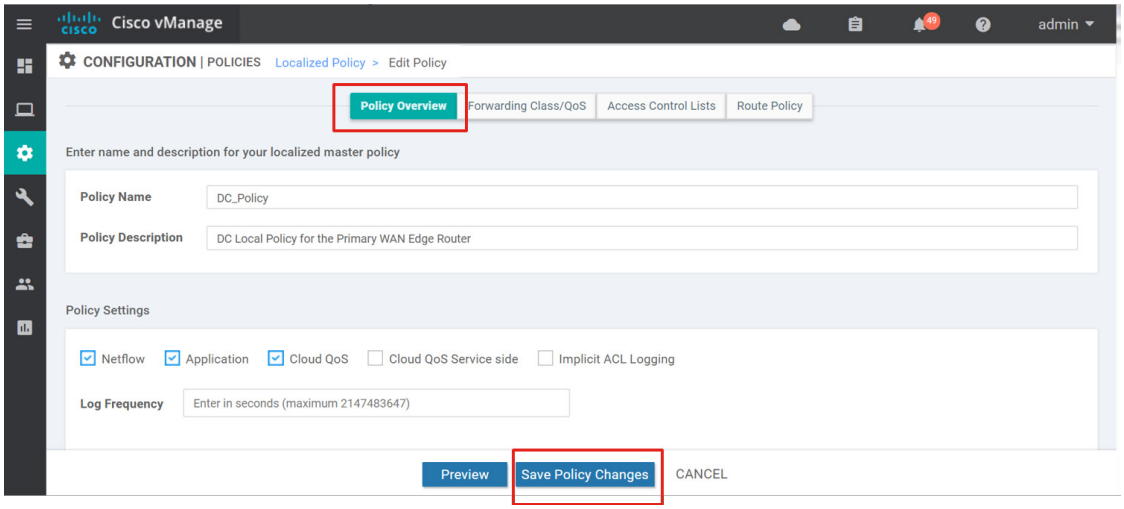
QoS 重写信息

类	优先级	DSCP	第 2 层服务类别
BULK	低	10	1
BULK	高	10	1
DEFAULT	低	0	0
DEFAULT	高	0	0
CONTROL_SIGNALING	低	18	2
CONTROL_SIGNALING	高	18	2
CRITICAL_DATA	低	18	2
CRITICAL_DATA	高	18	2
INTERACTIVE_VIDEO	低	34	4
INTERACTIVE_VIDEO	高	34	4

25. 完成后，点击**保存策略**按钮。

26. 选择页面顶部的**策略概述**框。

27. 点击**保存策略更改**以保存对本地化主策略的更改。



配置更改将被推送到与经过修改的本地化策略关联的设备。

28. 点击**下一步**，点击**配置设备**，选中相应复选框以确认两台设备上的配置更改，然后点击**确定**。vManage 应指示操作成功。

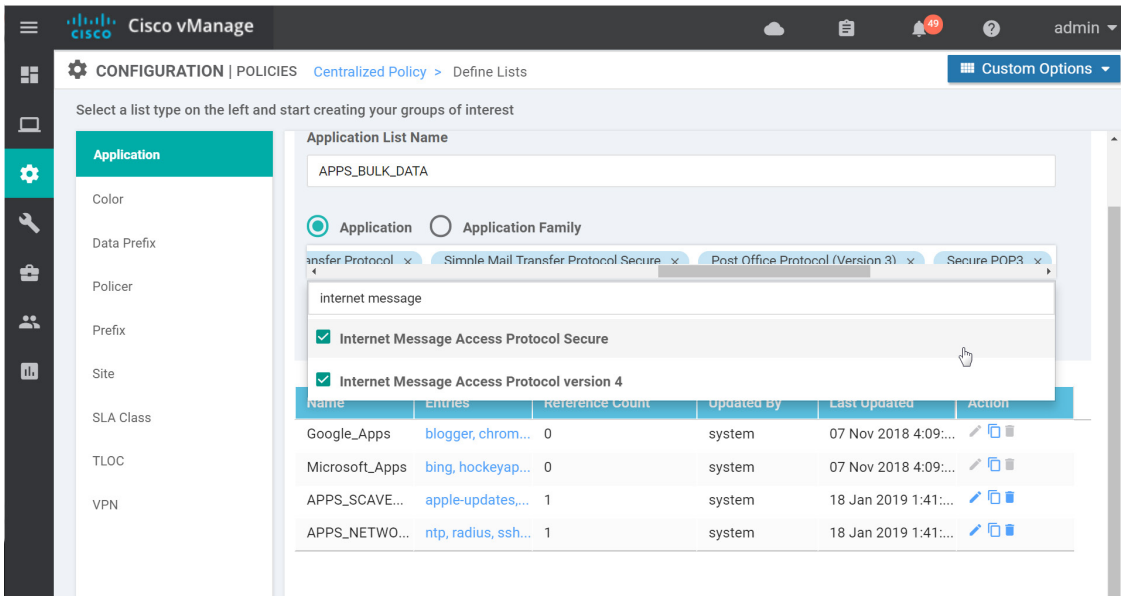
程序 2：定义 QoS 分类访问列表

此示例使用集中策略配置 QoS 分类访问列表。

1. 依次转到**配置 > 策略**并确保已选择**集中策略**选项卡。
2. 选择**自定义选项**，然后在**集中策略**部分，从下拉菜单中选择**列表**。
3. 选择左侧的**应用**，然后选择**新建应用列表**。
4. 输入**应用列表名称**，然后选择几个应用作为列表的一部分。您可以在应用下拉列表框中输入关键字来搜索各种应用。请注意，大多数应用都未缩写，这意味着 SSH 将显示为 Secure Shell，因此请适当调整关键字搜索。选择**添加**并对其他应用列表重复以上操作。使用以下设置示例。请注意，可能已经定义了 APPS_SCAVENGER 列表，因为它是在应用感知路由策略配置下定义的。

服务质量应用列表（示例）

应用列表名称	应用
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. 点击**添加**按钮以保存应用列表。

6. 从左侧菜单中选择**数据前缀**。确保已配置名为 **MGT_Servers** 的数据前缀列表，该列表是在应用感知路由策略下定义的。如果存在该列表，请跳转至第 7 步。

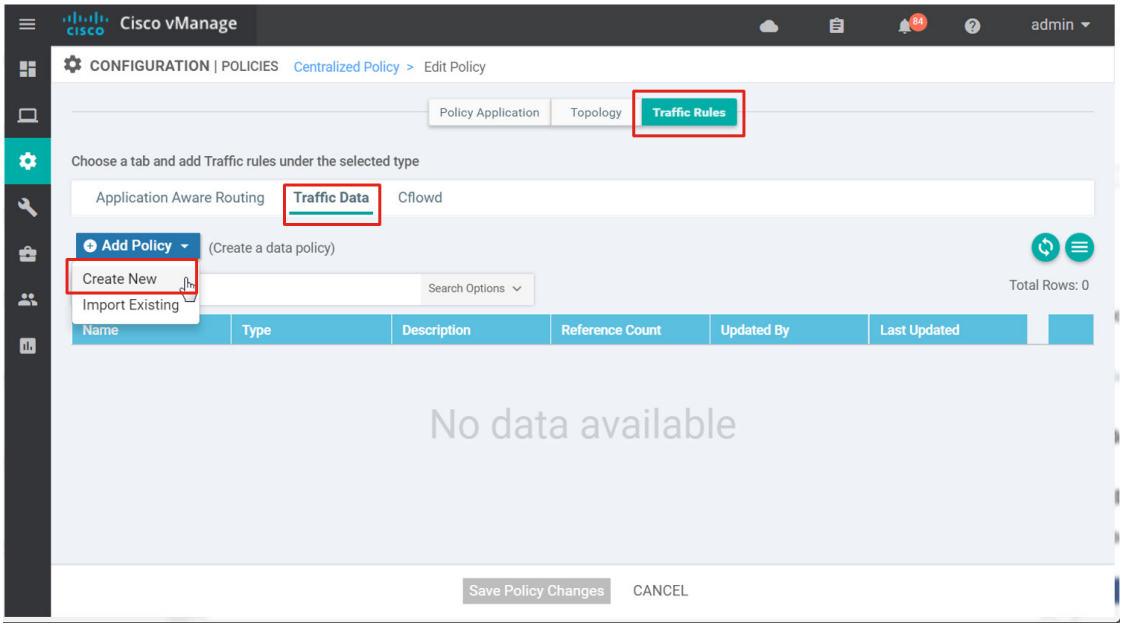
7. 如果未配置数据前缀列表 MGT_Servers，则创建要在 QoS 策略中使用的数据前缀列表。选择**新建数据前缀列表**。键入**数据前缀列表名称** (**MGT_Servers**)，在**添加数据前缀**文本框中，键入数据前缀列表 (**10.4.48.10/32,10.4.48.13/32,10.4.48.15/32,10.4.48.17/32**)，然后选择**添加**。

8. 依次转到**配置 > 策略**并确保已选择**集中策略**选项卡。

9. 在 **Global_policy** 的右侧，选择 **...**，然后选择**编辑**。

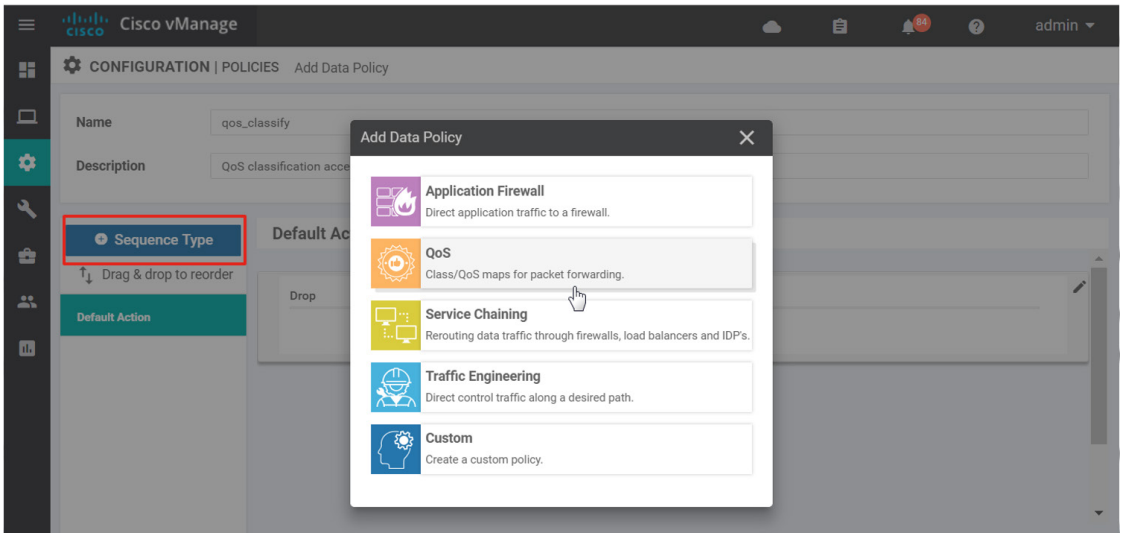
10. 选择页面顶部的**流量规则**框，以创建集中数据策略。

11. 选择**流量数据**选项卡。选择**添加策略**，然后从下拉菜单中选择**新建**。

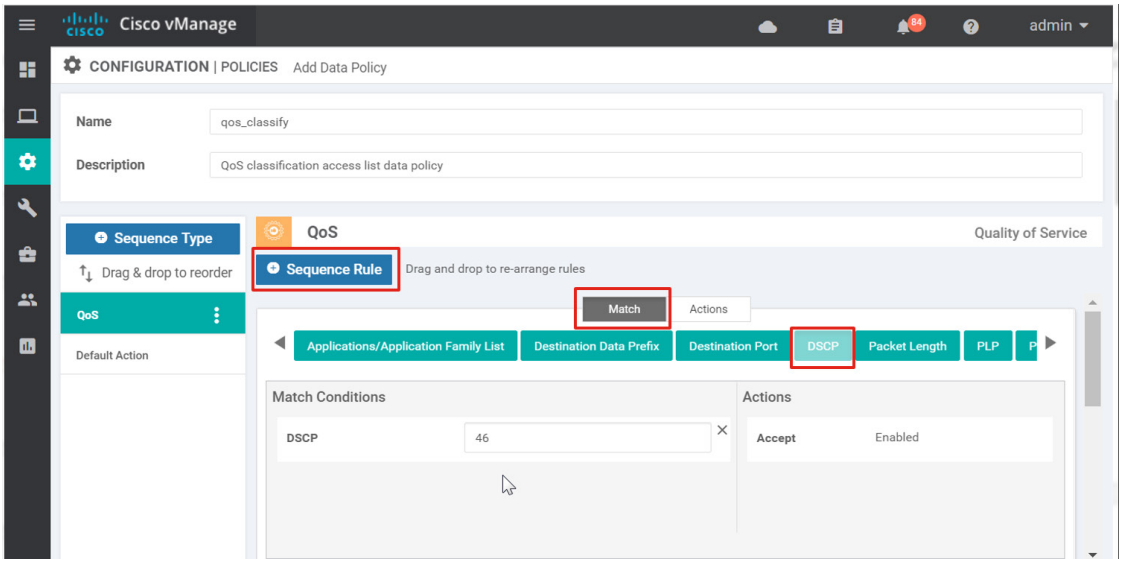


12. 输入名称 (**qos_classify**) 和说明（**QoS 分类访问列表数据策略**）。

13. 选择**序列类型**，然后从**添加数据策略**弹出窗口中选择 **QoS**。

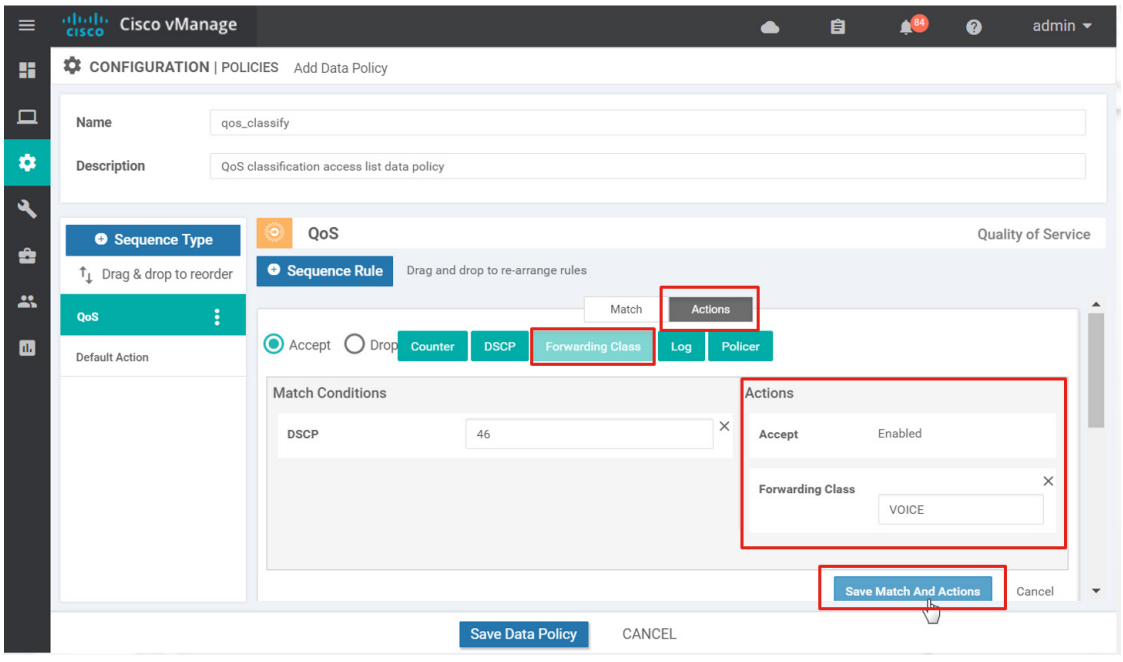


14. 选择**序列规则**，然后选择匹配条件 (**DSCP 46**)。



15. 选择**操作**框，选择**接受**或**丢弃**单选按钮（**接受**），然后选择操作（**转发类 VOICE**）。

16. 选择**保存匹配项和操作**。



17. 对其余匹配项/操作语句重复第 12 至 15 步:

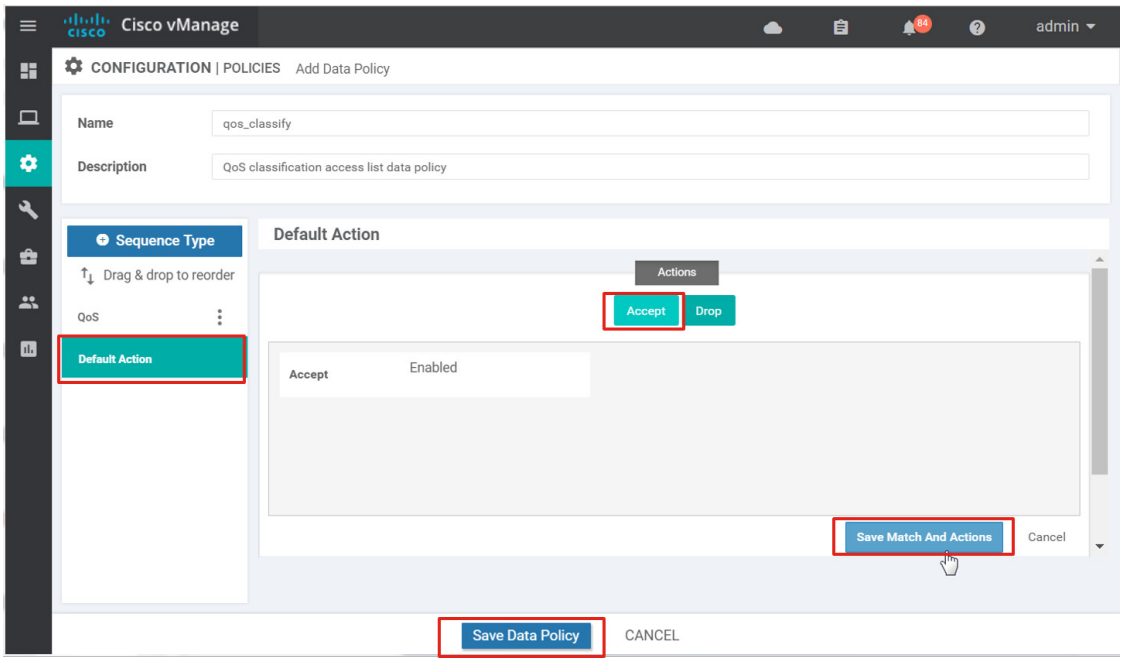
QoS 分类访问列表

匹配条件	接受或丢弃	操作
DSCP 46	接受	转发类 VOICE
DSCP 34 36 38	接受	转发类 INTERACTIVE_VIDEO
DSCP 10 12 14	接受	转发类 BULK
应用/应用系列列表 APPS_BULK_DATA	接受	转发类 BULK DSCP 10
DSCP 48 24	接受	转发类 CONTROL_SIGNALING
目标数据前缀 MGT_Servers 协议 17 6	接受	转发类 CRITICAL_DATA DSCP 16
DSCP 24	接受	转发类 CONTROL_SIGNALING
目标端口 11000-11999 1300 1718 1719 1720 5060 5061 协议 6	接受	转发类 CONTROL_SIGNALING DSCP 24
DSCP 16 32 40 18 20 22 26 28 30	接受	转发类 CRITICAL_DATA
DSCP 8 0	接受	转发类 CLASS_DEFAULT
应用/应用系列列表 APPS_SCAVENGER	接受	转发类 CLASS_DEFAULT DSCP 0

18. 选择左侧的**默认操作**，然后选择编辑符号。

19. 选择**接受**框，然后选择**保存匹配项和操作**。

20. 选择**保存数据策略**。



21. 现在，您可以应用该策略了。选择页面顶部的**策略应用**框。

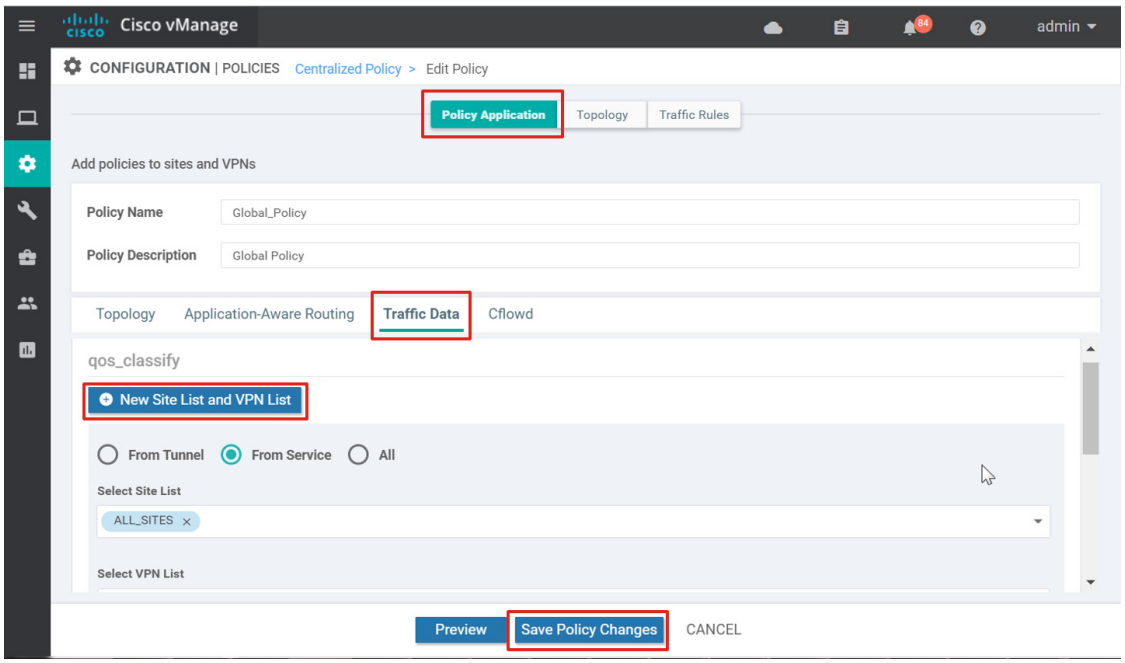
22. 选择**流量数据**选项卡。

23. 在 **qos_classify** 策略部分下，选择**新建站点列表和 VPN 列表**。

24. 选择**来自服务**单选按钮，因为这要应用于 LAN（即服务端）入站方向。

25. 在**选择站点列表**框下选择 **ALL_SITES**，在**选择 VPN 列表**框下选择 **ALL_VPNS**。选择**添加**。

26. 选择**保存策略更改**。



27. 系统将显示弹出窗口，指出该策略将应用到 vSmart 控制器。选择**激活**。

28. vManage 会将配置推送到 vSmart 控制器并指示操作成功。

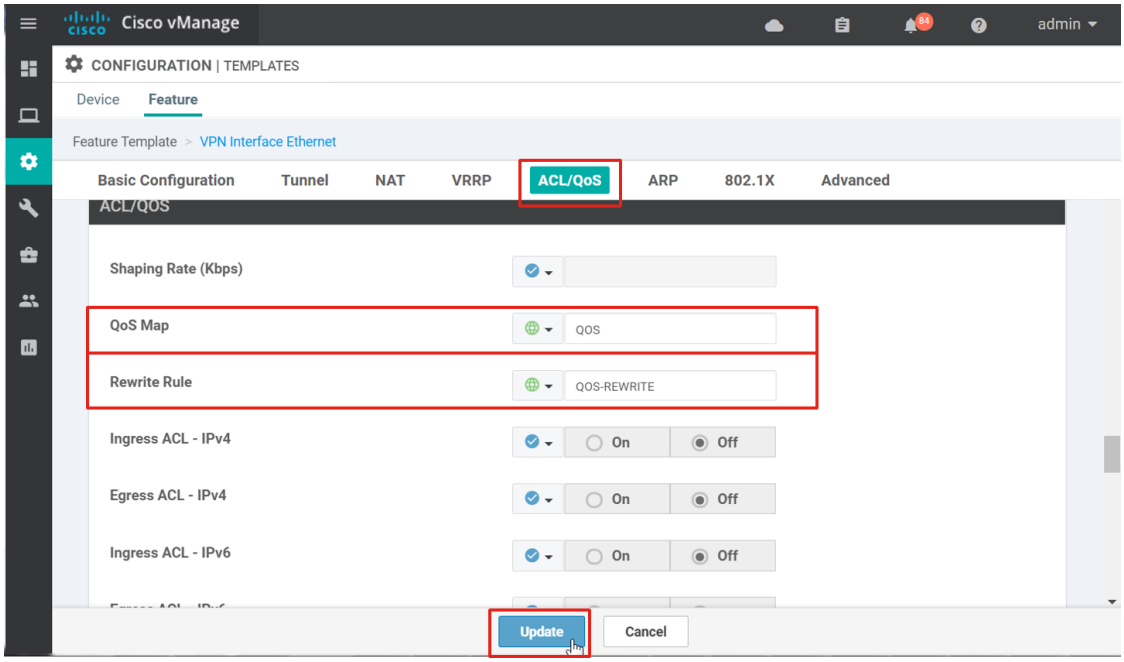
程序 3：更新功能模板

由于使用集中策略配置和应用 QoS 分类访问列表，因此不需要通过接口功能模板配置分类 QoS 访问列表。但是，需要在 VPN 接口功能模板中引用所创建的 QoS 映射和重写策略，然后才能应用。

需要修改以下功能模板（此示例中假设只有分支机构模板，请注意，仅物理接口支持 QoS，子接口不支持）：

- BR_MPLS_INT
- BR_INET_INT
- BR_INET_INT_DHCP

1. 依次转到**配置 > 模板**，并确保选择**功能**选项卡。
2. 选择 **BR_MPLS_INT** 模板右侧的 **...**，然后从下拉菜单中选择**编辑**。
3. 在 **ACL/QOS** 部分的 **QoS 映射**旁边，选择**全局**，然后在文本框中输入 **QOS**。如果根据站点存在不同的 QoS 策略，则可以将此设置改为特定设备专用变量。
4. 在**重写规则**下，选择**全局**，然后输入 **QOS-REWRITE**。
5. 选择**更新**。



6. 选择**下一步**，然后选择**配置设备**。系统会弹出一个窗口，要求您确认多个设备上的更改。选中复选框，然后选择**确定**。

7. 对其余两个功能模板 **BR_INET_INT** 和 **BR_INET_INT_DHCP** 重复第 1 至 6 步。

附页

附录 A: 产品列表

本部署指南中对以下产品和版本进行了验证。

位置	产品	软件版本
云	思科 vManage NMS	18.3.5
云	思科 vSmart 控制器	18.3.5
云	思科 vBond 协调器	18.3.5
数据中心	思科 vEdge 5000 系列路由器	18.3.5
分支机构	思科 vEdge 1000 系列路由器	18.3.5
分支机构	思科 vEdge 100 系列路由器	18.3.5
分支机构	思科 ISR 4331 IOS XE SD-WAN 路由器	16.9.4
分支机构	思科 ISR 4351 IOS XE SD-WAN 路由器	16.9.4

位置	产品	软件版本
数据中心	思科 ASR 1002	3.16.8S
数据中心	思科 Catalyst® 3850 交换机	3.6.8E
数据中心	思科 ASA 5512 防火墙	9.6(4)20
分支机构	思科 Catalyst 3850 交换机	3.6.8E
分支机构	思科 Catalyst 2960X 交换机	15.2(4)E6
分支机构	Catalyst 3750E 交换机	15.2(4)E6
分支机构	Catalyst 3650 交换机	3.6.8E
分支机构	4321 集成多业务路由器 (ISR)/K9	16.3.7

附录 B：为 SD-WAN 部署准备 IOS XE 路由器

在网络中部署 IOS XE SD-WAN 设备之前：

- 确保已经满足所有硬件和软件要求。
- 根据需要升级 ROMMON 映像：
- 将设备从 IOS XE 转换为 IOS XE SD-WAN 代码。
- 使用 IOS XE 设备信息更新思科即插即用连接门户，以便对加入 SD-WAN 重叠网络的 IOS XE SD-WAN 设备进行身份验证。

程序 1：检查硬件和软件要求

必须满足所有硬件和软件要求之后，才能将设备从 IOS XE 转换为 IOS XE SD-WAN 软件并将设备部署到 SD-WAN 重叠中。

要查阅所有硬件和软件要求，请访问 https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_Cisco_IOS_XE_Routers。

一些主要的要求总结如下：

- 确保您有支持的路由器型号和支持的接口模块。卸下不支持的模块。在 CLI 上，使用 **show inventory** 命令检查有没有不支持的硬件接口模块。
- 确保满足 DRAM 和启动闪存要求。
- 确保 IOS XE 路由器运行的 ROMMON 至少是支持 SD-WAN 映像的最低 ROMMON 版本，不过，建议使用最新维护版本。
- 确保您有智能许可帐户。
- 确保 SD-WAN 控制器运行的软件至少是 18.3 版
- 如果是 vEdge 和 IOS XE 混合环境，请确保 vEdge 路由器的软件为 17.2.1 版或更高版本；如果将两种设备部署在同一站点，请确保 vEdge 路由器的软件为 18.3 版或更高版本。

技术提示：在 IOS XE SD-WAN 软件版本 16.9 中，必需卸下所有不支持的模块之后才能将 IOS XE 路由器转换为 SD-WAN 代码。如果不这样做，代码就无法完全安装并正常运行，而且可能导致无法将 vManage 模板部署到设备。如果转换为 SD-WAN 代码并卸下不支持的模块后，发现该接口仍出现在 **show sdwan running-config** 命令的输出中，您可以在 **reload** 后输入 **request platform software sdwan config reset** 来清除配置。

另请参阅《思科 IOS XE 路由器上的软件定义广域网：端到端视图》，了解有关要求、许可、升级流程、典型部署情况和初始软件版本警告的信息：https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-741071.pdf

程序 2：升级 ROMMON 映像

使用 CLI 命令 show rom-monitor 或 show platform 查看当前 ROMMON 版本。在 show platform 下，ROMMON 版本位于 Firmware Version 下的 R0 旁边。如果 ROMMON 不需要升级，请跳到下一个程序。

```
ISR4351#show rom-monitor r0

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

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

1. 连接到路由器的管理控制台。

```
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. 运行 **upgrade rom-monitor** 命令开始 ROMMON 升级过程。注意：请勿中断 ROMMON 升级，因为在某些情况下，中断升级可能会导致路由器无法恢复。

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

3. 重新加载路由器，使新的 ROMMON 版本持久生效。

```
ISR4351#reload
```

4. 当路由器完成启动时，验证 ROMMON 版本。

```
ISR4351#sh rom-mon R0


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

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

有关详细信息，请访问 https://www.cisco.com/c/en/us/td/docs/routers/access/4400/cpld/isr4400_hwfp.html。

程序 3：升级到 SD-WAN 映像

1. 连接到路由器的管理控制台。

2. 将 IOS XE SD-WAN 映像从外部文件服务器复制到启动闪存中。

```
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. 备份当前运行的配置并将其保存到路由器的启动闪存中。

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

Destination filename [original-xe-config]?


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

4. 删除所有现有引导语句。

```
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. 配置指向新 SD-WAN 映像的 boot system 命令。

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

6. 确保将配置寄存器设置为 0x2102，以便映像从启动闪存正常启动。

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

ISR4351(config)#end
```

7. 保存配置，以便保存 boot 变量。

```
ISR4351#write mem
```

8. 验证 BOOT 变量是否指向 XE SD-WAN 映像，以及配置寄存器是否已设置为 0x2102 或者将在下次重新加载时设置为 0x2102。

```
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. 从路由器中删除所有现有配置。

```
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. 重新加载路由器。如果系统提示您保存配置，请输入 No。

```
ISR4351#reload
Proceed with reload? [confirm]
```

11. 路由器将使用 XE SD-WAN 映像重新启动。路由器启动后，应显示初始配置对话框。当系统提示进入初始配置对话框时，请输入 No。当系统提示终止自动安装时，请输入 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. 路由器将完成启动。系统可能会显示路由器提示符或提示您输入用户名/密码。如果系统显示 **Router>** 提示符，请输入 **enable**。如果系统提示您输入用户名/密码，请使用默认用户名 **admin** 和默认密码 **admin** 登录。然后，系统应该会显示**路由器**提示符。如果尚未进入使能模式，请输入 **enable**。

```
Router>enable
Router#
```

或

```
User Access Verification


Username: admin

Password:

Router#
```

13. 停止 PnP 并允许 XE SD-WAN 软件包安装。安装可能需要一分钟多一点的时间才能完成。

```
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. 路由器完成 SD-WAN 软件包解压后，使用 **request platform software sdwan software reset** 命令激活路由器上的 SD-WAN 映像。SD-WAN 软件包激活后，路由器会自动重新启动。激活过程可能需要 2 分钟多一点的时间才能完成，而重新启动大约需要 4 分钟到 4.5 分钟。

```
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. 路由器重新启动后，您应该会看到系统配置对话框。当系统提示进入初始配置对话框时，请输入 **no**。当系统提示终止自动安装时，请输入 **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. 系统可能会显示**路由器**提示符或提示您输入**用户名/密码**。如果系统显示 **Router>** 提示符，请输入 **enable**。如果系统提示您输入**用户名/密码**，请使用默认用户名 **admin** 和默认密码 **admin** 登录。然后，系统应该会显示**路由器**提示符。如果尚未进入使能模式，请输入 **enable**。

```
Router>enable

Router#
```

或

```
User Access Verification

Username: admin

Password: admin

Router#
```

17. 如果您需要进入配置模式，请先停止 PnP。在禁用 PnP 之前，您无法进入配置模式。

```
Router#pnpa service discovery stop
PNP-EXEC-DISCOVERY (1): Stopping PnP Discovery...
```

18. 验证系统状态。

```
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
```

技术提示：请注意，如果您尝试发出 sdwan 命令（例如 **show sdwan system**）但收到**无法连接到服务器**错误，请务必先使用 **pnp service discovery stop** 命令禁用 PnP。

19. 要确保 PnP 在下一次开机或重新启动时运行，您可以运行 CLI 命令 **request platform software sdwan config reset** 来清除配置。

20. 如果需要，请使用必要的信息配置即插即用 (PnP) 连接门户，以便重叠网络中的控制器可以对路由器授权。通过该门户，还可以在网络中自动调配 IOS XE SD-WAN 设备。有关 PnP 连接门户的详细信息，请参阅附录 C。

恢复到 IOS XE:

1. 确保 IOS XE 映像位于启动闪存中。如果并非如此，请确保可访问外部文件服务器，然后将该映像复制到启动闪存中。

```
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. 根据需要发出 CLI 命令 **request platform software sdwan config reset**，以删除 SD-WAN 启动配置。

```
ISR4351#request platform software sdwan config reset

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

3. 将配置寄存器设置为 0x0，以引导至 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. 重新加载路由器。

```
ISR4351#reload
Proceed with reload? [confirm]
```

5. 进入 ROMMON 后，启动位于启动闪存中的所需 IOS XE 映像。

```
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. 配置指向当前映像的引导语句。

```
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. 将配置寄存器设置为 0x2102，并保存配置。

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

Router(config)#end

Router#write mem

Building configuration...

[OK]
```

附录 C：即插即用 (PnP) 连接门户

PnP 门户位于以下网址：http://software.cisco.com。在此网站上，您可以下载软件，通过 PnP 连接门户管理设备，以及管理许可证。您可以使用传统方法管理许可证，也可以通过智能账户进行管理。使用智能许可需要智能账户，它们可以提供一个集中的位置供您管理整个组织中的思科许可证。设置智能账户后，您便可灵活地创建子账户（虚拟账户）来帮助管理组织内不同部门、区域或位置的许可证。虚拟账户就像一个文件夹，您可以根据业务职能添加多个虚拟账户。要在 PnP 连接门户上创建控制器配置文件，需要智能账户和虚拟账户。

有关智能账户和智能许可的详细信息，请访问:

https://cisco.com/go/smartaccounts

https://cisco.com/go/smartlicensing

即插即用连接门户 (https://software.cisco.com/#pnp-devices) 包含广域网边缘设备列表。此外，您还可以在该门户中执行以下两项操作:

- 创建广域网边缘设备硬件的序列号授权文件，您可以手动将其加载到 vManage 中。或者，您也可以允许 vManage 与 PnP 账户同步，无需手动干预即可下载序列号授权信息。如果没有序列号授权文件，广域网边缘路由器就无法加入重叠网络。
- 启用 IOS XE SD-WAN 路由器的自动网络调配。门户中将创建一个控制器配置文件，用于定义您的 vBond 和组织名称信息。在启动时，IOS XE SD-WAN 路由器会查找 devicehelper.cisco.com，而该网站会将路由器定向至 PnP 门户。PnP 门户会检查路由器的序列号，并向路由器推送关键参数，例如 vBond IP 地址和组织名称。路由器通过门户联系 vBond 协调器，控制器连接也从门户发起。PnP 门户信息用于填充非接触调配 (ZTP) 服务器，因此可以启用 vEdge 路由器以实现自动网络调配。

如果您有思科云托管的控制器部署，则 PnP 门户中应该已经创建了控制器配置文件。此外，通过思科商务工作空间 (CCW) 订购并关联了智能账户和虚拟账户的广域网边缘设备应该也会被自动推送到 PnP 门户。vEdge 设备信息会自动从 PnP 服务器推送到 ZTP 服务器，以实现自动调配。

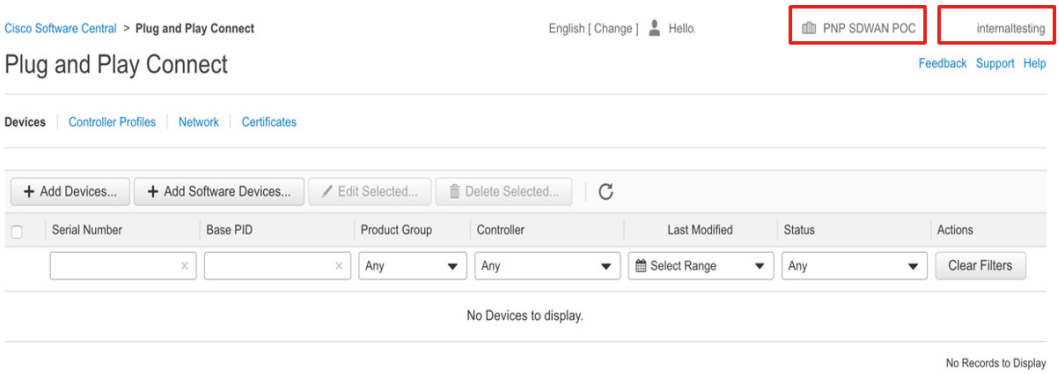
对于本地控制器部署，可以手动创建控制器配置文件，也可以手动添加 PnP 门户中尚无的广域网边缘设备。

在 PnP 连接门户页面中，您可以执行以下操作：

- 创建控制器配置文件（如果尚未创建）
- 将广域网边缘设备添加到门户，并将其与控制器配置文件关联
- 下载授权设备序列号文件

程序 1：登录 PnP 连接门户

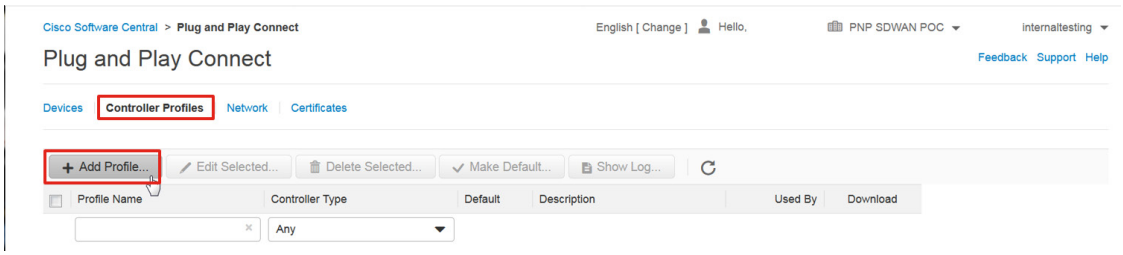
1. 导航至 https://software.cisco.com
2. 在“网络即插即用”部分，点击**即插即用连接**。如果您尚未登录，系统会提示您输入思科账户用户名和密码。系统将打开**即插即用连接**对话框。
3. 在**即插即用连接**门户中的右上角，找到与智能账户关联的虚拟账户。注意：如果您无法导航至此页面，请确保输入的登录用户 ID 和凭证具有与之关联的有效智能账户和虚拟账户。



如果您尚未创建控制器配置文件，请立即创建。如果您有思科托管控制器型号，应在控制器配置文件中预先填充与 vBond 控制器相关的信息，而且您可以跳过程序 2。

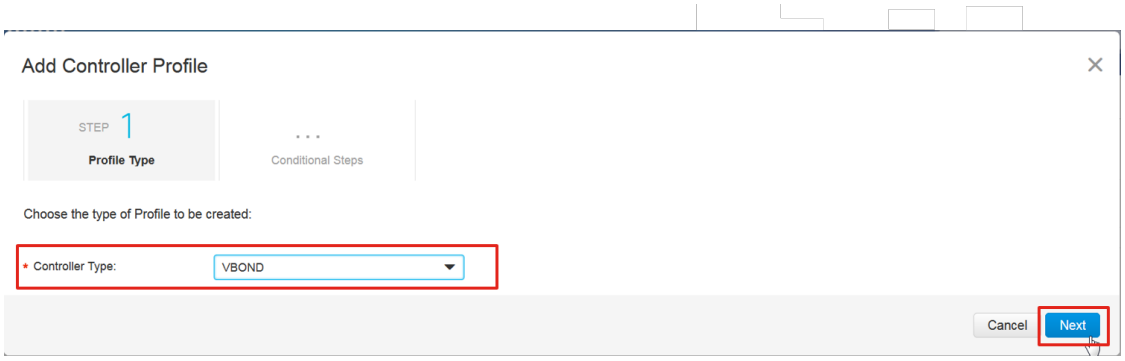
程序 2：配置控制器文件

1. 在**即插即用连接**标题正下方，点击位于**设备**选项卡右侧的**控制器配置文件**选项卡。
2. 点击**添加配置文件**。系统将打开添加控制器配置文件对话框，其中突出显示了步骤 1 配置文件类型。



3. 在**控制器类型**下拉列表中，选择 **vBond**。

4. 点击**下一步**。此时会突出显示**步骤 2 配置文件设置**，并显示配置文件设置字段。



5. 在**配置文件名称**字段中，输入您正在创建的控制器配置文件的名称（在本示例中为 **ENB-SOLUTIONS-VBOND**）。

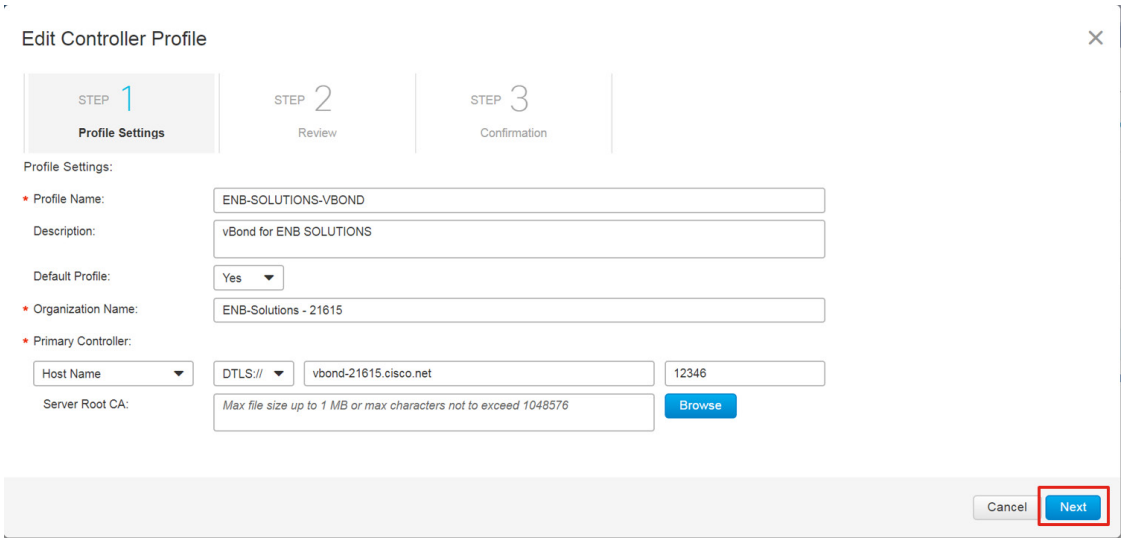
6. 在**说明**字段中，输入您正在创建的配置文件的说明（**ENB SOLUTIONS 的 vBond**）。此字段为选填字段。

7. 如果不存在其他控制器配置文件，请在**默认配置文件**下拉列表框中，选择**是**。无论设置如何，添加到 PnP 连接门户的每台广域网边缘设备都需要与一个配置文件关联。

8. 在**组织名称**字段中，输入组织名称 (**ENB-Solutions - 21615**)。您可以在 vManage GUI 中的**管理 > 设置**屏幕下找到组织名称。

9. 在**主控制器**下拉列表框中，选择**域名**或 **IPv4**，然后填写 vBond 主机名或 IP 地址。在本示例中，从下拉列表框中选择**主机名**，然后在文本框中输入 **vbond-21615.cisco.net**。

10. 点击**下一步**。



11. 检查您刚刚配置的选项。如果正确无误，请选择**提交**；否则，请返回更正相关设置。

12. 显示的窗口指出，配置文件已成功创建。选择**完成**

程序 3：将广域网边缘设备添加到门户

您可以通过思科商务工作空间流程手动添加尚未添加到门户的广域网边缘设备。

要将 IOS XE 设备添加到 PnP 门户，您需要知道序列号、基本 PID（产品标识符）和证书序列号。在 IOS XE 代码中的 CLI 模式下，发出 **show crypto pki certificates CISCO_IDEVID_SUDI** 命令可获取此信息。出于 PnP 的目的，将机箱序列号和 SUDI 证书（安全唯一设备标识符）绑定到智能账户，以实现 IOS XE 设备的身份验证和轻松调配。请注意，使用的软件至少需要为 3.14.0s 版或更高版本，才能为 ISR4k 运行此命令。

```
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
```

如果您已转换为 SD-WAN 映像，则请改为使用 **show sdwan certificate installed** 命令。

```
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
```

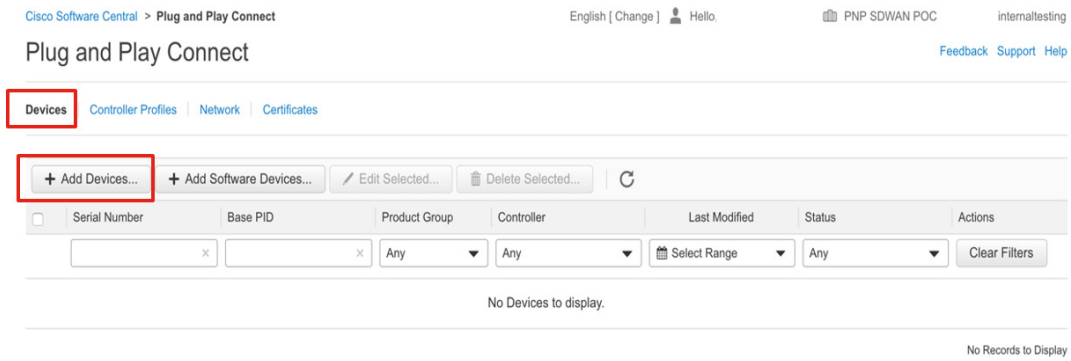
```
            Not After : Dec 16 01:53:51 2026 GMT
        Subject: serialNumber=PID:ISR4351/K9 SN:FDO205108CB, O=Cisco,
```

或者，您也可以使用 **show sdwan certificate serial**:

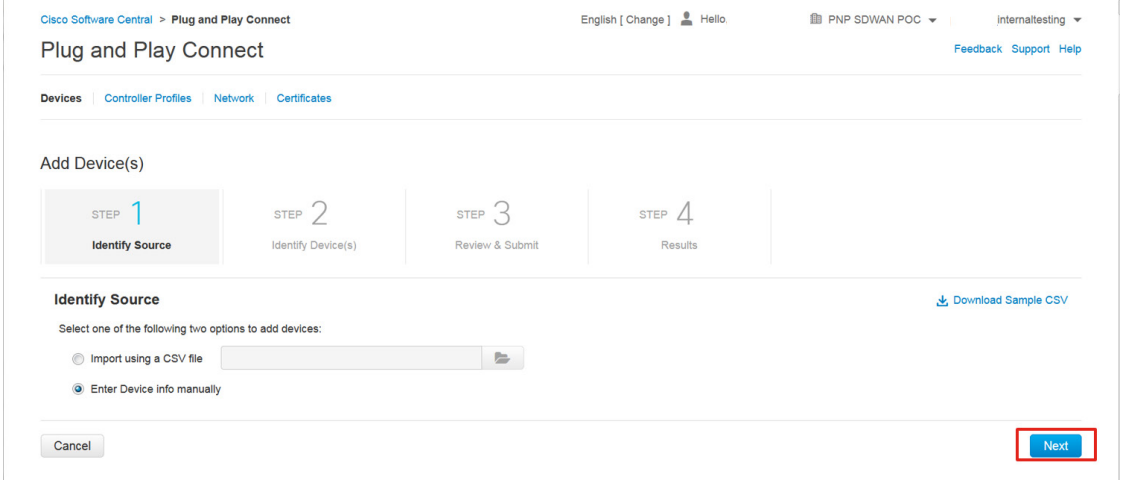
```
Router#show sdwan certificate serial
Chassis number: ISR4351/K9-FDO205108CB   Board ID serial number: 01373974
```

对于 vEdge 路由器，您需要设备的序列号和 PID 才能将设备添加到门户。如果尚不知道这些信息，可以使用 **show hardware inventory** CLI 命令检索。

1. 导航至 https://software.cisco.com。
2. 在**网络即插即用**部分下，点击**即插即用连接**。
3. 确保右上角选择的虚拟账户正确。
4. 系统应默认选择**设备**选项卡。选择**添加设备**。



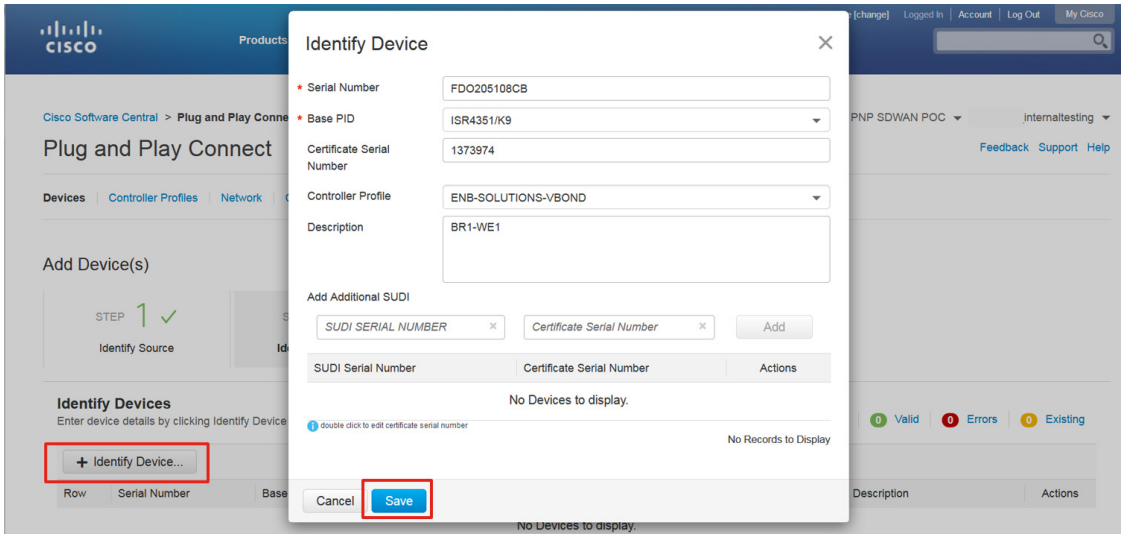
5. 首先要确定如何输入设备信息，是手动输入还是通过 .csv 文件输入。选择**手动输入设备信息**旁边的单选按钮，然后点击**下一步**。



6. 点击**识别设备**按钮。系统将弹出一个窗口，提示您输入**序列号**和**基本 PID**、与设备关联的**控制器配置文件**和**说明**。

7. 输入设备的**序列号** (**FDO205108CB**) 和**基本 PID** (**ISR4351/K9**)。选择**基本 PID** 文本框后，输入要搜索的值，按回车键，然后选择与您的设备相匹配的 PID。选择 PID 后，系统将显示其他字段。输入**证书序列号** (**1373974**)，然后选择使用 PnP 时要与设备关联的**控制器配置文件** (**ENB-SOLUTIONS-VBOND**)。输入可选的**说明** (**BR1-WE1**)，然后点击**保存**。

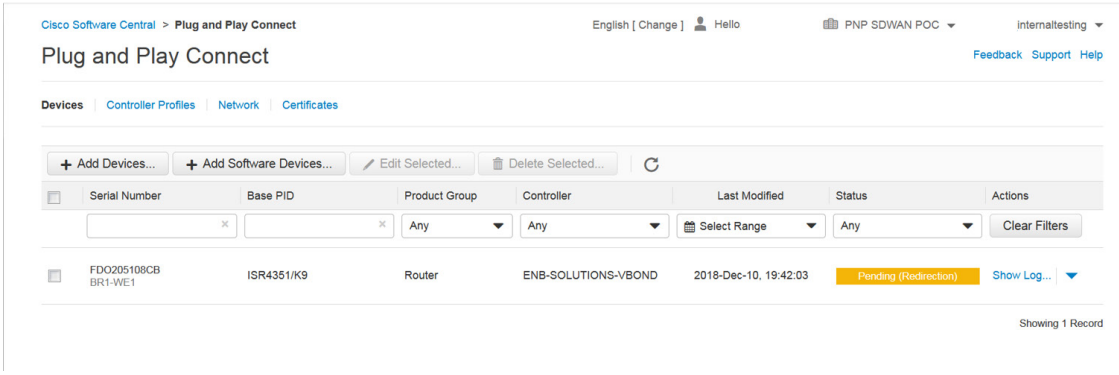
请注意，证书序列号为十六进制格式，不含前导 0x。



8. 选择**下一步**。检查设备信息，然后点击**提交**。如果需要修改设备信息，请点击**后退**按钮。

9. 单击**提交**。显示的页面将指出已成功添加 1 台设备。

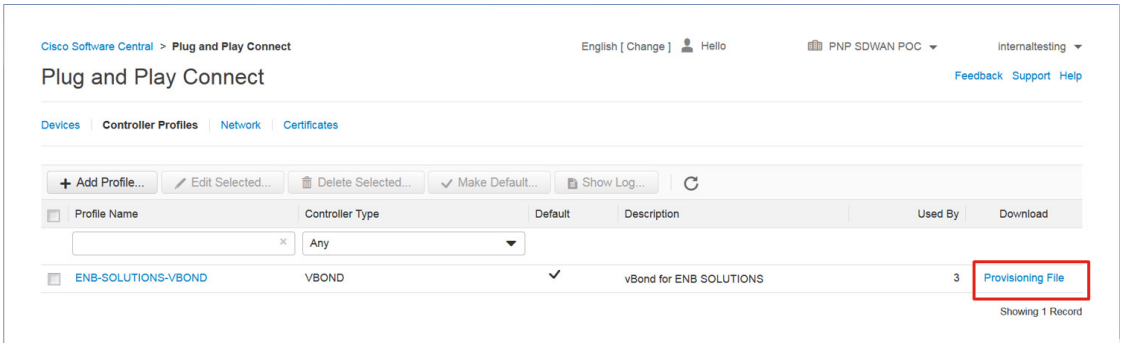
10. 选择**完成**以刷新页面，然后返回到**设备**选项卡。



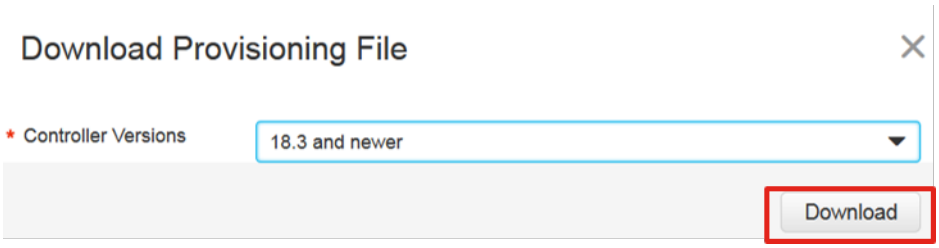
11. 重复上述步骤，添加其他设备。

下载授权序列号文件

1. 导航至 https://software.cisco.com。
2. 在**网络即插即用**部分下，点击**即插即用连接**。
3. 确保右上角选择的虚拟账户正确。
4. 点击**控制器配置文件**。
5. 在正确的控制器配置文件 (**ENB-SOLUTIONS-VBOND**) 旁边，点击**调配文件**文本。



6. 在弹出窗口中，从下拉列表框中选择控制器版本。请选择 **18.3 版及更高版本**。点击**下载**并将文件保存到您的计算机上。默认情况下，文件将另存为 serialFile.viptela。



附录 D：vEdge 出厂默认设置

下文说明了如何将 vEdge 路由器重置为出厂默认设置（通常不需要执行此操作）。还说明了在插槽 0 中安装了网络模块的新 vEdge 5000 硬件路由器的默认出厂设置配置。

可以通过发出 **request software reset** 命令将配置重置为出厂默认设置。也可以通过按下重置按钮超过 10 秒钟来恢复出厂默认配置。释放按钮后路由器将重新启动。出厂默认用户名/密码为 admin/admin。

1. 设置默认软件（可选）。在重置为出厂默认设置之前，如果尚未更改默认软件版本，则可能需要更改默认软件版本。系统将加载默认软件版本，不一定是您升级到的最后一个版本，并且将删除所有其他代码版本。在 CLI 中，发出 **show software** 命令来查看默认版本：

```
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. 在执行模式下键入 request **software set-default** [**version**] 以更改代码版本，在系统询问您是否确定要继续时回答 **yes**。

```
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. 要将配置重置为出厂默认设置，请在执行模式下使用 **request software reset** 命令，并在系统询问您是否确定要继续时回答 **yes**。

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

4. 使用 **show version** 命令重置后验证代码版本。

```
vedge# show version
17.2.5
```

以下是 vEdge 5000 的出厂默认设置配置：

```
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
 !
```

附录 E：手动升级广域网边缘路由器

下文提供了通过 VPN 512 (vEdge) 或 Mgmt-intf VRF 接口 (cEdge) 使用外部 FTP 服务器进行升级的示例。此过程假设此接口已配置并包含具有 IP 地址的接口，并且可通过该接口访问 FTP 服务器。所需的代码应该在服务器的 FTP 默认目录中可用。

vEdge 路由器

在这种情况下，我们从 FTP 服务器 192.168.254.51 加载 viptela-17.2.5-x86_64.tar.gz（vEdge 5K 软件）。

首先，验证服务器是否可访问:

```
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
```

然后安装软件。将使用单独的命令激活该软件。激活将导致 vEdge 路由器使用所选代码版本重新启动。

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
```

现在，使用以下命令激活新软件版本，在系统询问您是否要继续时回答 “yes”。然后 vEdge 路由器将重新启动并引导到所需的软件版本。

```
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
```

重新启动完成后，vEdge 路由器将在控制台上指示当前运行的软件版本。

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


viptela 17.2.5


vedge login:
Password:
```

您还可以发出 “show version” 命令来查看当前软件版本。

```
vedge# show ver
17.2.5
```

IOS XE SD-WAN 路由器

在这种情况下，我们从 FTP 服务器 192.168.254.51 加载 isr4300-ucmk9.16.9.4.SPA.bin（ISR 4300 IOS XE SD-WAN 软件）。

首先，验证服务器是否可访问。

```
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#
```

接下来，将映像复制到启动闪存中，确保已定义 FTP 的源接口。

```
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]
```

然后安装软件。这会将 .bin 文件解压为多个 .pkg 文件。将使用单独的命令激活该软件。激活会导致 IOS XE SD-WAN 路由器使用所选代码版本重新启动。

```
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
```

需要执行以下命令才能完成安装。如果在激活前未完成此操作，路由器将在 15 分钟后回滚到以前的代码版本。

```
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
```

现在，使用以下命令激活新软件版本。然后，IOS XE SD-WAN 路由器将重新启动并引导到所需的软件版本。

```
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.
```

重新启动完成后，您可以登录并发出 “show version” 命令查看当前软件版本。

```
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
```

附录 F：配套的网络设备配置

为方便起见，以下是示例网络中配套网络设备的部分配置。

数据中心 CE 路由器:

```
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
!
```

数据中心防火墙 (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
```

分支机构 1 交换机堆叠 (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
```

分支机构 3 交换机 (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
!
```

分支机构 4 交换机 (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
!
```

分支机构 5 交换机 (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
!
```

分支机构 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
!
```

附录 G: vEdge 配置模板摘要

为方便起见，本部分概述了示例网络中的广域网边缘设备功能模板、设备模板和 SD-WAN 设备变量值。

共享功能模板

系统功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：系统

模板名称：System_Template

说明：系统模板

系统功能模板设置

部分	参数	类型	变量/值
基本配置	站点 ID	特定设备专用	system_site_id
	系统 IP	特定设备专用	system_system_ip
	主机名	特定设备专用	system_hostname
	设备组	特定设备专用	system_device_groups
	控制台波特率 (bps)	特定设备专用	system_console_baud_rate
GPS	纬度	特定设备专用	system_latitude
	经度	特定设备专用	system_longitude
高级	端口跳变	特定设备专用	system_port_hop
	端口偏移量	特定设备专用	system_port_offset

日志记录功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：日志记录

模板名称：Logging_Template

说明：日志记录模板

日志记录功能模板设置

部分	参数	类型	变量/值
服务器	主机名/IP 地址	全局	10.4.48.13
	VPN ID	全局	1
	源接口	全局	loopback0

NTP 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：基本信息/NTP

模板名称：NTP_Template

说明：NTP 模板

NTP 功能模板设置

部分	参数	类型	变量/值
服务器	主机名/IP 地址	全局	time.nist.gov

AAA 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：基本信息/AAA

模板名称：AAA_Template

说明：AAA 模板

AAA 功能模板设置

部分	参数	类型	变量/值
身份验证	身份验证顺序	下拉列表	local
本地/新建用户	名称/密码/用户组	全局	oper1/oper1/operator
	名称/密码/用户组	全局	netadmin1/netadmin1/netadmin

OMP 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：基本信息/OMP

模板名称：OMP_Template

说明：OMP 模板

OMP 功能模板设置

部分	参数	类型	变量/值
基本配置	每前缀通告的路径数	全局	16
	ECMP 限制	全局	16
通告	互联	全局	关闭
	静态	全局	关闭

双向转发检测 (BFD) 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：基本信息/BFD

模板名称：BFD_Template

说明：BFD 模板

BFD 功能模板设置

部分	参数	类型	变量/值
基本配置	轮询间隔	全局	120000

安全功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：基本信息/安全

模板名称：Security_Template

说明：安全模板

安全功能模板设置

部分	参数	类型	变量/值
基本配置	重放窗口	全局/下拉列表	4096

VPN512 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：VPN/VPN

模板名称：VPN512_Template

说明：VPN 512 带外管理

VPN512 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	512
	名称	全局	管理 VPN
IPv4 路由/新建 IPv4 路由	前缀	全局	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn512_mgt_next_hop_ip_addr

VPN 接口 (VPN512)

设备：除 vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：VPN512_Interface

说明：VPN 512 管理接口

VPN512 接口功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	全局	否
	接口名称	特定设备专用	vpn512_mgt_int_x|x
	说明	全局	管理接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn512_mgt_int_ip_addr|maskbits

VPN 接口以太网 Loopback0

设备：除 vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：Loopback0

说明：环回接口 0

VPN512 接口以太网功能模板设置（环回接口 0）

部分	参数	类型	变量/值
基本配置	关闭	全局	否
	接口名称	全局	loopback0
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lo0_int_ip_addr|maskbits

横幅功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：其他模板/横幅

模板名称：Banner_Template

说明：横幅模板

横幅功能模板设置

部分	参数	类型	变量/值
基本配置	MOTD 横幅	全局	这是专用网络。它仅供在获得授权的情况下使用。

SNMP 功能模板

设备：除 vManage 和 vSmart 之外的所有设备

模板：其他模板/SNMP

模板名称：SNMP_Template

说明：SNMP 模板

SNMP 功能模板基本配置设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	snmp_shutdown
	SNMP 的设备名称	特定设备专用	snmp_device_name
	设备位置	特定设备专用	snmp_device_location
SNMP 版本	SNMP 版本	单选按钮	V2
SNMP 版本/视图和社区	视图/名称	全局	isoALL
	视图/对象标识符	全局	1.3.6.1
	社区/名称	全局	c1sco123
	社区/授权	全局/下拉列表	只读
	社区/视图	全局	isoALL
SNMP 版本/陷阱	陷阱组/组名称	全局	SNMP GRP
	陷阱组/陷阱类型模块/模块名称	全局	all
	陷阱组/陷阱类型模块/严重性级别	全局	严重、重要、次要
	陷阱目标服务器/VPN	全局	1
	陷阱目标服务器/IP 地址	全局	10.4.48.13
	陷阱目标服务器/UDP 端口	全局	162
	陷阱目标服务器/陷阱组名称	全局	SNMP GRP
	陷阱目标服务器/社区名称	全局	c1sco123
	陷阱目标服务器/源接口	全局	loopback0

数据中心功能模板

数据中心传输端 VPN (VPN 0) 功能模板

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN 接口以太网

模板名称：DC_ VPN0

说明：数据中心传输端 VPN 0

VPN 0 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	0
	名称	全局	传输端 VPN
	增强 ECMP 键控	全局	开启
DNS	主 DNS 地址	全局	64.100.100.125
	辅助 DNS 地址	全局	64.100.100.126
IPv4 路由	前缀	全球	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn0_mpls_next_hop_ip_addr
	下一跳地址	特定设备专用	vpn0_inet_next_hop_ip_addr

数据中心 VPN 接口 (MPLS)

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN 接口以太网

模板名称：DC_ MPLS_Interface

说明：数据中心 MPLS 接口

VPN 0 VPN 接口以太网功能模板设置 (MPLS)

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启

部分	参数	类型	变量/值
	允许服务 > DHCP	全局	关闭
	允许服务 > NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

数据中心 VPN 接口（互联网）

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN 接口以太网

模板名称：DC_INET_Interface

说明：数据中心互联网接口

VPN 0 接口以太网功能模板设置（互联网）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
基本配置	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
	限制	全局	关闭
	允许服务 > DHCP	全局	关闭
	允许服务 > NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
高级	清除不分段	全局	开启

数据中心服务端 VPN 1

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN

模板名称：DC_VPN1

说明：数据中心服务端 VPN 1

数据中心 VPN 1 功能模板设置

部分	参数	类型	变量/值
基本配置	VPN	全局	1
	名称	全局	服务端 VPN 1
	增强 ECMP 键控	全局	开启
通告 OMP	BGP	全局	开启

数据中心 VPN 接口以太网 1

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN 接口以太网

模板名称：DC_LAN _INT1

说明：数据中心局域网接口 1

数据中心 VPN 接口功能模板设置（接口 1）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits

数据中心 VPN 接口以太网 2

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：VPN/VPN 接口以太网

模板名称：DC _LAN_INT2

说明：数据中心局域网接口 2

数据中心 VPN 接口功能模板设置（接口 2）

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr|maskbits

数据中心局域网边界网关协议 (BGP)

设备：ASR1001-HX、ASR1001-X、ASR1002-HX、ASR1002-X、vEdge 2000、vEdge 5000

模板：其他模板/BGP

模板名称：DC_LAN_BGP

说明：数据中心局域网 BGP 模板

BGP 功能模板配置设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_bgp _shutdown
	AS 编号	特定设备专用	lan_bgp_as_num
	路由器 ID	特定设备专用	lan_bgp_as_num
	传播 AS 路径	全局	开启
IPv4 单播地址系列	最大路径数	全局	2
	地址系列	下拉列表	ipv4 单播
	重新分发/协议	下拉列表	omp
	网络/网络前缀	特定设备专用	bgp_network_lo_addr|maskbits
邻居 (1)	地址	特定设备专用	lan_bgp_neighbor1_addr
	说明	特定设备专用	lan_bgp_neighbor1_description
	远程 AS	特定设备专用	lan_bgp_neighbor1_remote_as
	地址系列	全局	开启

部分	参数	类型	变量/值
	地址系列	全局	ipv4 单播
	关闭	特定设备专用	lan_bgp_neighbor1_shutdown
	高级选项/密码	特定设备专用	lan_bgp_neighbor1_password
	高级选项/保持时间（秒）	全局	3
	高级选项/保持时间（秒）	全局	9
邻居 (2)	地址	特定设备专用	lan_bgp_neighbor2_addr
	说明	特定设备专用	lan_bgp_neighbor2_description
	远程 AS	特定设备专用	lan_bgp_neighbor2_remote_as
	地址系列	全局	开启
	地址系列	下拉列表	ipv4 单播
	关闭	特定设备专用	lan_bgp_neighbor2_shutdown
	高级选项/密码	特定设备专用	lan_bgp_neighbor2_password
	高级选项/保持时间（秒）	全局	3
	高级选项/保持时间（秒）	全局	9

分支机构功能模板

分支机构 VPN 0 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN

模板名称：BR_VPN0

说明：分支机构传输端 VPN 0

分支机构 VPN 0 功能模板

部分	参数	类型	变量/值
基本配置	VPN	全局	0
	名称	全局	传输端 VPN
	增强 ECMP 键控	全局	开启

部分	参数	类型	变量/值
DNS	主 DNS 地址	全局	64.100.100.125
	辅助 DNS 地址	全局	64.100.100.126
IPv4 路由	前缀	全局	0.0.0.0/0
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn0_mpls_next_hop_ip_addr
	下一跳地址	特定设备专用	vpn0_inet_next_hop_ip_addr

分支机构 MPLS 接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_MPLS_INT

说明：具有静态 IP 的分支机构 MPLS 接口

分支机构 VPN0 MPLS 接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启
隧道 > 允许服务	BGP	全局	开启
	DHCP	全局	关闭
	NTP	全局	开启

部分	参数	类型	变量/值
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

分支机构 MPLS 子接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_MPLS_SUBINT

说明：具有静态 IP 的分支机构 MPLS 子接口

分支机构 VPN0 MPLS 子接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_mpls_int_shutdown
	接口名称	特定设备专用	vpn0_mpls_int_x|x.VLAN
	说明	全局	MPLS 接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_mpls_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_mpls_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_mpls_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	mpls
	限制	全局	开启
允许服务	BGP	全局	开启
	DHCP	全局	关闭
	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_mpls_tunnel_ipsec_preference
高级	清除不分段	全局	开启

分支机构互联网接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_INET_INT

说明：具有静态 IP 的分支机构互联网接口

分支机构 VPN0 互联网接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
允许服务	DHCP	全局	关闭
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

分支机构互联网 DHCP 接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_INET_INT_DHCP

说明：具有 DHCP IP 的分支机构互联网接口

分支机构 VPN0 互联网接口动态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_gex|x
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	动态
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
允许服务	DHCP	全局	开启
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

分支机构互联网子接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_INET_SUBINT

说明：具有静态 IP 的分支机构互联网子接口

分支机构 VPN0 互联网子接口静态 IP 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_inet_int_shutdown
	接口名称	特定设备专用	vpn0_inet_int_x|x.VLAN
	说明	全局	互联网接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_inet_int_ip_addr|maskbits
	上行带宽	特定设备专用	vpn0_inet_int_bandwidth_up

部分	参数	类型	变量/值
	下行带宽	特定设备专用	vpn0_inet_int_bandwidth_down
隧道	隧道接口	全局	开启
	颜色	全局	企业互联网
允许服务	DHCP	全局	关闭
允许服务	NTP	全局	开启
隧道 > 高级选项 > 封装	首选项	特定设备专用	vpn0_inet_tunnel_ipsec_preference
NAT	NAT	特定设备专用	nat-enable
高级	清除不分段	全局	开启

分支机构 TLOC 扩展接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_TLOC_EXT_INT

说明：分支机构 TLOC 扩展接口/子接口

分支机构 VPN0 TLOC 扩展接口/子接口功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_tloc_ext_int_shutdown
	接口名称	特定设备专用	vpn0_tloc_ext_int_x|x_or_x|x.VLAN
	说明	全局	TLOC 扩展接口
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	vpn0_tloc_ext_int_ip_addr|maskbits
高级	TLOC 扩展	特定设备专用	vpn0_tloc_ext_wan_int_x|x

分支机构 WAN 父接口功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_WAN_Parent_INT

说明：分支机构 WAN 父接口

分支机构 VPN0 WAN 父接口功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_wan_parent_int_shutdown
	接口名称	特定设备专用	vpn0_wan_parent_int_x|x
	说明	全局	WAN 父接口
高级	IP MTU	全局	1504

分支机构 VPN 0 MPLS BGP 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/BGP

模板名称：BR_VPN0_MPLS_BGP

说明：与提供商相连的分支机构 VPN 0 MPLS BGP

分支机构 VPN0 MPLS BGP 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	vpn0_bgp _shutdown
	AS 编号	特定设备专用	vpn0_bgp_as_num
	路由器 ID	特定设备专用	vpn0_bgp_router_id
IPv4 单播地址系列	最大路径数	全局	2
	地址系列	下拉列表	ipv4 单播
	网络/网络前缀	特定设备专用	bgp_tloc_ext_prefix_to_advertise
邻居	地址	特定设备专用	vpn0_bgp_neighbor_addr
	说明	特定设备专用	vpn0_bgp_neighbor_description
	远程 AS	特定设备专用	vpn0_bgp_neighbor_remote_as
	地址系列	全局	开启
	地址系列	下拉列表	ipv4 单播
	入站路由策略	全局	开启

部分	参数	类型	变量/值
	策略名称	全局	DENY-ALL
	关闭	特定设备专用	vpn0_bgp_neighbor_shutdown

分支机构 VPN1 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN

模板名称：BR_VPN1

说明：分支机构 VPN1

分支机构 VPN 1 基础功能模板

部分	参数	类型	变量/值
基本配置	VPN	全局	1
	名称	全局	服务端 VPN
	增强 ECMP 键控	全局	开启
通告 OMP	互联	全局	开启
	集合	全局	开启
	汇聚/前缀	特定设备专用	vpn1_omp_aggregate_prefix
	汇聚/仅汇聚	全局	开启
IPv4 路由 [标记为可选行]	前缀	特定设备专用	vpn1_lan_static_route_prefix|maskbits
	网关	单选按钮	下一跳
	下一跳地址	特定设备专用	vpn1_lan_next_hop_ip_addr

分支机构 LAN 接口 1 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT1

说明：分支机构 LAN 接口 1

分支机构 VPN 1 接口 1 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10

分支机构 LAN 接口 2 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT2

说明：分支机构 LAN 接口 2

分支机构 VPN 1 接口 2 功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10

分支机构 LAN 接口 1 VRRP 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT1_VRRP

说明：分支机构 LAN 接口 1 VRRP

分支机构 VPN 1 接口 1 VRRP 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int1_shutdown
	接口名称	特定设备专用	lan_int1_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int1_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int1_ip_addr|maskbits
高级	DHCP 帮助程序	全局	10.4.48.10
VRRP	组 ID	全局	1
	优先级	特定设备专用	lan_int1_vrrp_priority
	跟踪 OMP	全局	关闭
	跟踪前缀列表	全局	Default-Route
	IP 地址	特定设备专用	lan_int1_vrrp_ip_addr

分支机构 LAN 接口 2 VRRP 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_INT2_VRRP

说明：分支机构 LAN 接口 2 VRRP

分支机构 VPN 1 接口 2 VRRP 功能模板设置

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_int2_shutdown
	接口名称	特定设备专用	lan_int2_x|x_or_x|x.VLAN
	说明	特定设备专用	lan_int2_description
IPv4 配置	IPv4 地址	单选按钮	静态
	IPv4 地址	特定设备专用	lan_int2_ip_addr/maskbits
高级	DHCP 帮助程序	全局	10.4.48.10
VRRP	组 ID	全局	2
	优先级	特定设备专用	lan_int2_vrrp_priority

部分	参数	类型	变量/值
	跟踪 OMP	全局	关闭
	跟踪前缀列表	全局	Default-Route
	IP 地址	特定设备专用	lan_int2_vrrp_ip_addr

分支机构 LAN 父接口模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：VPN/VPN 接口以太网

模板名称：BR_LAN_Parent_INT

说明：分支机构 LAN 父接口

分支机构 VPN 1 LAN 父接口功能模板

部分	参数	类型	变量/值
基本配置	关闭	特定设备专用	lan_parent_int_shutdown
	接口名称	特定设备专用	lan_parent_int_x|x
	说明	全局	LAN 父接口
高级	IP MTU	全局	1504

分支机构 LAN 数据 VLAN DHCP 服务器功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/DHCP 服务器

模板名称：BR_LAN_DATA_DHCP_Server

说明：用于数据 VLAN 的分支机构 LAN DHCP 服务器

用于数据 VLAN 的分支机构 VPN 1 LAN DHCP 服务器功能模板

部分	参数	类型	变量/值
基本配置	地址池	特定设备专用	data_dhcp_addr_pool|maskbits
	排除地址	特定设备专用	data_dhcp_addr_exclude_range
高级	域名	全局	cisco.local
	默认网关	特定设备专用	data_dhcp_default_gateway
	DNS 服务器	全局	10.4.48.10

分支机构 LAN 语音 VLAN DHCP 服务器功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/DHCP 服务器

模板名称：BR_LAN_VOICE_DHCP_Server

说明：用于语音 VLAN 的分支机构 LAN DHCP 服务器

用于语音 VLAN 的分支机构 VPN 1 LAN DHCP 服务器功能模板

部分	参数	类型	变量/值
基本配置	地址池	特定设备专用	voice_dhcp_addr_pool|maskbits
	排除地址	特定设备专用	voice_dhcp_addr_exclude_range
高级	域名	全局	cisco.local
	默认网关	特定设备专用	voice_dhcp_default_gateway
	DNS 服务器	全局	10.4.48.10
	TFTP 服务器	全局	10.4.48.19

分支机构 LAN OSPF 功能模板

设备：除 ASR1K、vEdge 2000、vEdge 5000、vManage 和 vSmart 之外的所有设备

模板：其他模板/OSPF

模板名称：BR_LAN_OSPF

说明：分支机构 LAN OSPF

LAN OSPF 功能模板

部分	参数	类型	变量/值
基本配置	路由器 ID	特定设备专用	lan_ospf_router_id
重新分发	协议	全局	omp
区域	区域号	全局	0
	接口/接口名称	特定设备专用	lan_ospf_int_x|x
	接口/接口成本	特定设备专用	lan_ospf_int_cost
	接口/高级/OSPF 网络类型	全局下拉列表	点对点

部分	参数	类型	变量/值
	接口/身份验证/身份验证类型	全局下拉列表	message-digest
	接口/消息摘要/消息摘要密钥 ID	全局	22
	接口/消息摘要/消息摘要密钥	特定设备专用	lan_ospf_message_digest_key
区域范围	地址	特定设备专用	lan_ospf_area_range_addr_0
高级	参考带宽 (Mbps)	全局	100000
	来源	全局	开启

数据中心设备模板

设备型号：vEdge 5000

模板名称：DC_Hybrid_BGP

说明：数据中心 MPLS 和 INET – 传输静态和局域网 BGP

数据中心设备模板：DC_Hybrid_BGP

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0		DC_VPN0
	VPN 接口	DC_MPLS_Interface
	VPN 接口	DC_INET_Interface
VPN 512		VPN512_Template
	VPN 接口	VPN512_Interface
VPN1		DC _VPN1

模板类型	模板子类型	模板名称
	BGP	DC_LAN_BGP
	VPN 接口	DC_LAN_INT1
	VPN 接口	DC_LAN_INT2
	VPN 接口	Loopback0
横幅		Banner_Template
策略		DC_Policy
安全策略		
SNMP		SNMP_Template

分支机构设备模板

Branch_A_MPLS_BGP_TLOCEXT_VRRP

设备型号：ISR 4351

模板名称：Branch_A_MPLS_BGP_TLOCEXT_VRRP

说明：分支机构双广域网边缘设备混合 TLOC 扩展，具有 MPLS BGP 以及 LAN 端中继和 VRRP

Branch_A_MPLS_BGP_TLOCEXT_VRRP **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
	VPN 接口	BR_TLOC_EXT_INT

模板类型	模板子类型	模板名称
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN _INT1_VRRP
	VPN 接口	BR_LAN _INT2_VRRP
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_A_INET_TLOCEXT_VRRP

设备型号：ISR 4351

模板名称：Branch_A_INET_TLOCEXT_VRRP

说明：分支机构双广域网边缘设备混合 TLOC 扩展，具有 INET 以及 LAN 端中继和 VRRP

Branch_A_INET_TLOC_VRRP **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
	VPN 接口	BR_TLOC_EXT_INT

模板类型	模板子类型	模板名称
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN _INT1_VRRP
	VPN 接口	BR_LAN _INT2_VRRP
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

Branch_B_MPLS_INET(DHCP)

设备型号：ISR 4331

模板名称：Branch_B_MPLS_INET(DHCP)

说明：分支机构单广域网边缘设备混合互联网 DHCP 地址，具有 LAN 中继

Branch_B_MPLS_INET(DHCP)

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT_DHCP

模板类型	模板子类型	模板名称
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

设备型号：vEdge 100 B

模板名称：Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

说明：分支机构单广域网边缘设备混合互联网 DHCP 地址，具有 LAN 中继和 DHCP 服务器

Branch_B_MPLS_INET(DHCP)_LAN(DHCP) **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT_DHCP
	VPN 接口	BR_LAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface

模板类型	模板子类型	模板名称
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口 > DHCP 服务器	BR_LAN_DATA_DHCP_Server
	VPN 接口	BR_LAN_INT2
	VPN 接口 > DHCP 服务器	BR_LAN_VOICE_DHCP_Server
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

设备型号：ISR 4351

模板名称：Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

说明：分支机构双广域网边缘设备混合 TLOC 扩展 SubInt，具有 MPLS BGP 以及 LAN 端 OSPF

Branch_C_MPLS_BGP_TLOCEXT_Subint_OSPF **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	BGP	BR_VPN0_MPLS_BGP
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_SUBINT
	VPN 接口	BR_TLOC_EXT_INT

模板类型	模板子类型	模板名称
	VPN 接口	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_C_INET_TLOCEXT_SubInt_OSPF

设备型号：vEdge 1000

模板名称：Branch_C_INET_TLOCEXT_SubInt_OSPF

说明：分支机构双广域网边缘设备混合 TLOC 扩展 SubInt，具有 INET 以及 LAN 端 OSPF

Branch_C_INET_TLOC_SubInt_OSPF **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_SUBINT
	VPN 接口	BR_INET_INT
	VPN 接口	BR_TLOC_EXT_INT

模板类型	模板子类型	模板名称
	VPN 接口	BR_WAN_Parent_INT
VPN 512	VPN	VPN512_Template
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	OSPF	BR_LAN_OSPF
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_BGP_OSPF_Policy
SNMP		SNMP_Template

Branch_D_MPLS_CE_INET_LAN-Static-Routing

设备型号：vEdge 100 B

模板名称：Branch_D_MPLS_CE_INET_LAN-Static-Routingg

说明：分支机构单广域网边缘设备混合，具有适用于 LAN 的 MPLS CE 和静态路由

Branch_D_MPLS_CE_INET_LAN-Static-Routing **设备模板**

模板类型	模板子类型	模板名称
系统		System_Template
	日志记录	Logging_Template
	NTP	NTP_Template
	AAA	AAA_Template
BFD		BFD_Template
OMP		OMP_Template
安全		Security_Template
VPN0	VPN	BR_VPN0
	VPN 接口	BR_MPLS_INT
	VPN 接口	BR_INET_INT
VPN 512	VPN	VPN512_Template

模板类型	模板子类型	模板名称
	VPN 接口	VPN512_Interface
VPN1	VPN	BR_VPN1
	VPN 接口	BR_LAN_INT1
	VPN 接口	Loopback0
横幅		Banner_Template
策略		Branch_Policy
SNMP		SNMP_Template

数据中心变量值

DC1-WE1：DC_Hybrid_BGP

数据中心 1 广域网边缘设备 1 设备模板变量值

变量	值
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

变量	值
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)	☐

变量	值
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

* 对于 IPSec 隧道首选项，请配置一个大于 0 的数字（在示例中为 100）以首选此设备来路由流量，从而确保 DPI 的对称性。

DC1-WE2：DC_Hybrid_BGP

数据中心 1 广域网边缘设备 2 设备模板变量值

变量	值
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

变量	值
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

变量	值
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

分支机构变量值

BR1-WE1：Branch_A_MPLS_BGP_TLOCEXT_VRRP

分支机构 1 广域网边缘设备 1 设备模板变量值

变量	值
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)	☐

变量	值
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

变量	值
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

* 对于 IPSec 隧道首选项，请配置一个大于 0 的数字（在示例中为 100）以首选此设备来路由流量，从而确保 DPI 的对称性。

BR1-WE2: Branch_A_INET_TLOCEXT_VRRP

分支机构 1 广域网边缘设备 2 设备模板变量值

变量	值
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

变量	值
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)

分支机构 2 广域网边缘设备 1 设备模板变量值

变量	值
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

变量	值
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

* 填写互联网传输链路的任何下一跳值；从 DHCP 收到的动态 IP 网关值应覆盖此值。

BR3-WE1：Branch_B_MPLS_INET(DHCP)_LAN(DHCP)

分支机构 3 广域网边缘设备 1 设备模板变量值

变量	值
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	☐

变量	值
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

变量	值
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

* 填写互联网传输链路的任何下一跳值；从 DHCP 收到的动态 IP 网关值应覆盖此值。

BR4-WE1：Branch_C_MPLS_BGP_TLOCEXT_SubInt_OSPF

分支机构 4 广域网边缘设备 1 设备模板变量值

变量	值
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

变量	值
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]	

变量	值
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

* 对于 IPSec 隧道首选项，请配置一个大于 0 的数字（在示例中为 100）以首选此设备来路由流量，从而确保 DPI 的对称性。

BR4-WE2：Branch_C_INET_TLOCEXT_SubInt_OSPF

分支机构 4 广域网边缘设备 2 设备模板变量值

变量	值
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

变量	值
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]	

变量	值
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

分支机构 5 广域网边缘设备 1 设备模板变量值

变量	值
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

变量	值
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)	☐

变量	值
Name of Device for SNMP(snmp_device_name)	BR5-WE1
Location of Device(snmp_device_location)	Branch 5

附录 H：广域网边缘路由器 CLI 等效配置

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 [管理员密码]
!
```

```
  user netadmin1
   password [netadmin1 密码]
   group    netadmin
  !
  user oper1
   password [oper1 密码]
   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（部分）

```
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（部分）

```
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（部分）

```
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（部分）

```
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（部分）

```
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（部分）

```
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
 !
```

关于本指南

本手册中所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括（但不限于）适销性、适合特定用途和非侵权保证，或因交易习惯或贸易惯例而产生的保证。任何情况下，思科或其供应商均不对任何间接性、特殊性、后果性或附带性损害承担责任，包括（但不限于）因使用或未使用这些设计而导致的利润损失或数据丢失或损坏，即使思科或其供应商已被告知存在此类损害的可能性。

这些设计如有更改，恕不另行通知。用户对这些设计的使用负有全部责任。这些设计并不构成思科及其供应商或合作伙伴的技术建议或其他专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

CCDE、CCENT、Cisco Eos、Cisco Lumin、Cisco Nexus、Cisco StadiumVision、Cisco TelePresence、Cisco WebEx、Cisco 徽标、DCE 和 Welcome to the Human Network 为商标；Changing the Way We Work，Live，Play，and Learn 和 Cisco Store 为服务标志；以及 Access Registrar、Aironet、AsyncOS、Bringing the Meeting To You、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、CCSP、CCVP、Cisco、Cisco Certified Internetwork Expert 徽标、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems 徽标、思科统一计算系统 (Cisco UCS)、思科 UCS B 系列刀片服务器、思科 UCS C 系列机架式服务器、思科 UCS S 系列存储服务器、思科 UCS 管理器、思科 UCS 管理软件、思科统一交换矩阵、思科以应用为中心的基础设施、思科 Nexus 9000 系列和思科 Nexus 7000 系列。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 和 Webex 徽标是 Cisco Systems，Inc. 和/或其附属公司在美国和其他某些国家/地区的注册商标。

本文档或网站中提及的所有其他商标均属于其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(0809R)

© 2019 思科系统公司。版权所有。

反馈与讨论

有关我们指南的评论和建议，请参加思科社区上的讨论。