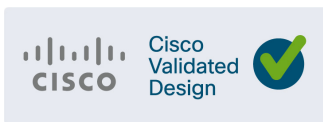




Extended Enterprise Implementation Guide for Cisco SD-WAN Deployments

Implementation Guide

February 2020



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED "AS IS."

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

©2020 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED



Contents

Extended Enterprise CVD	7
References	7
Scope and Audience for this Document	7
What is in this Guide?	8
Implementation Overview	8
Prerequisites	8
Deployment Steps	9
Deployment Example	9
Remote Site Connections	10
Remote Site Examples	11
Validated Hardware and Software Matrix	12
Network Planning	13
Policies	14
QoS deployment	16
Localized policies	17
Traffic Symmetry for DPI on Dual Router Scenarios	18
Configure Localized Policy	19
Configure Route Policy	23
Centralized Policy	25
Configuration of a Centralized Policy	27
Create Groups of Interest	27
Configure Topology and VPN Membership	29
Configure Traffic Rules	31
Apply policies to sites and VPNs	33
Activate Policy	33
Editing Policy Elements	34
Template Configuration	34
Configuring Feature Templates	35
Feature Templates for Transport VPN	37
VPN 0 Template Reference	37
VPN Internet Interface Template Reference	39
VPN Cellular Interface Template Reference	40
VPN Cellular Interface for Expansion Module Template Reference	41
Feature Templates for Service VPN	42
Service VPN 1 Template Reference	42

Service VPN 10 Template Reference	42
Service VPN 11 Template Reference	43
Service VPN Interface SVI 1	43
Service VPN Interface SVI 2 (Optional)	44
Switchport Template	45
VPN Interface Ethernet Loopback0	48
OSPF Template	49
DHCP Template (Optional)	49
4G LTE Configuration	50
Cellular Profile (Optional)	52
Device Templates	53
IOS XE SD-WAN router with LTE Transport	54
IOS XE SD-WAN router with Cellular and Internet Transport	58
IOS XE SD-WAN router with Dual LTE	60
Modifying Templates	61
Cisco Plug and Play Connect	63
Prerequisites	64
Adding a device on PnP Connect	64
Load authorized WAN edge serial numbers to vManage	66
Method 1: Sync to the Smart Account	66
Method 2: Upload File Manually	66
Stage Devices (Optional)	66
Attach device to template	67
Add Variables with a File	67
Add Variables Manually	68
Modify Variables	68
Generate Bootstrap Configuration File	68
Bring up Devices	69
Plug and Play	69
Prerequisites	69
Bootstrap	69
Prerequisites	70
Activate Devices in Staging State	70
Device Onboarding Troubleshooting	70
Device is Not Authorized by vBond	71
Router Configuration Failure	72
Configuration Reset	73
Device Management	74
Software Upgrade	74
Uploading Images on vManage	74
Activate an Image	75

Best Practices	75
Reboot a Device	75
Generate Admin Tech	76
Monitor	76
Main Dashboard	76
Geography	78
Network	79
System Status	80
WAN Information	81
Control Connections	81
Events	81
Alarms	82
Troubleshooting	83
Real Time	84
Caveats and Limitations	87
System feature template settings	91
Logging feature template settings	91
NTP feature template settings	92
AAA feature template settings	92
OMP feature template settings	92
Security feature template settings	92
Banner template settings	93
SNMP template settings	93
OSPF Configuration on Industrial Ethernet Switch	95
Configuration on Industrial Ethernet Switch Connected to Routers Running VRRP	96
Device Template Values for IR1101_CELL_with_TRUNK	97
Device Template Values for IR1101_INET_and_CELL	100
Device Template Values for IR1101_DUAL_CELL_EM	102
Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK	105



Extended Enterprise Implementation Guide for Cisco SD-WAN Deployments

This *Extended Enterprise Implementation Guide for Cisco SD-WAN Deployments* describes the implementation of the design defined in the *Extended Enterprise SD-WAN Design Guide*. This guide incorporates a broad set of technologies, features, and applications for helping customers extend the enterprise information technology (IT) services to outdoor spaces.

Cisco Validated Designs (CVDs) provide the foundation for systems design and deployment and are based on common use cases or engineering system priorities. Each guide details the methodology for building solutions, and more importantly, the recommendations have been comprehensively tested by Cisco engineers to help ensure a faster, more reliable, and predictable deployment.

Extended Enterprise CVD

An enterprise has production, storage, distribution, and outdoor facilities. IT reach extends beyond the traditional carpeted space to non-carpeted spaces as well. IT can now extend network connectivity, security policy, and management to the outside, warehouses, and distribution centers with the same network operating systems and network management that offer automation, policy enforcement, and assurance inside. Cisco Software-Defined WAN (SD-WAN) is a secure architecture that is open, programmable, and scalable. Managed through the Cisco vManage console you can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and remote sites to improve network speed, security, and efficiency.

This CVD outlines the steps for both IT and operations teams to accomplish business goals by digitizing the operations in the outdoor spaces of an enterprise. It includes guidance for implementing Extended Enterprise use cases with the customer's existing Cisco SD-WAN architecture.

References

To learn more about Extended Enterprise solutions, please visit:

- <https://www.cisco.com/go/extendedenterprise>
- <https://www.cisco.com/go/iotcvd>

Scope and Audience for this Document

This implementation document provides deployment guidance for an Extended Enterprise network design. It is a companion to the associated design and deployment guides for enterprise networks, which provide guidance on how to deploy the most common implementations of Cisco SD-WAN. This guide discusses the extended enterprise implementation for Cisco SD-WAN deployments.

For the associated deployment guides, design guides, and white papers, refer to the following documents:

- Cisco Enterprise Networking design guides:
 - <https://www.cisco.com/go/designzone>

Implementation Overview

- Cisco IoT Solutions validated design guides:
 - <https://www.cisco.com/go/iotcvd>
- Cisco Extended Enterprise Solutions Overview:
 - <https://www.cisco.com/go/extendedenterprise>
- *CVD SD-WAN Design Guide* at the following URL:
 - <https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-WAN-dg.html>
- *Cisco Extended Enterprise Cisco SD-WAN End-to-End Deployment Guide*:
 - <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Deployment-2018OCT.pdf>

What is in this Guide?

This document is organized in the following sections:

Implementation Overview, page 8	Discusses overall network topology and considerations
Network Planning, page 13	Detailed list explaining required network planning activities
Policies, page 14	Details configuration of centralized and localized policies needed for extended enterprise implementation
Template Configuration, page 34	Explains feature templates and device templates. It provides a blueprint for feature template configuration and shows how to integrate them into a device template.
Device Onboarding, page 63	Provides steps to add Cisco IR1101 running IOS XE SD-WAN image to the SD-WAN overlay
Device Management, page 74	Shows how to perform operational actions on Cisco IR1101 using vManage
Monitor, page 76	Explains how to use vManage to monitor and troubleshoot SD-WAN network
Caveats and Limitations, page 87	Lists known caveats and limitations

Implementation Overview

The Cisco SD-WAN for an Extended Enterprise deployment is based on the *Cisco SD-WAN End-to-End Deployment Guide* and expands its scope to non-carpeted spaces using Cisco 1100 Series Industrial Integrated Services Routers as the SD-WAN edge router. This implementation supports controllers running on the Cisco cloud-managed service or on customer premises.

Prerequisites

- This guide assumes that the user has already installed Cisco SD-WAN controllers. For more details on installation see the following resources:
 - On-premises deployments: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html>
 - Cloud deployments: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/knowledge-base/cloudops.html>

Implementation Overview

- Data center and enterprise branch sites are already configured per *Cisco SD-WAN End-to-End Deployment Guide*.
- Cisco WAN Edge routers are installed and ready to be configured. The IOS XE SD-WAN routers should already be converted from IOS XE to SD-WAN code. See **Appendix A - Upgrade Cisco IR1101 with IOS XE SD-WAN Image** for information on the conversion.
- Devices adjacent to the Cisco WAN Edge routers are configured.

The Cisco SD-WAN solution and its associated concepts are understood, although no deployment experience is required. See the **Extended Enterprise SD-WAN Design Guide** for background information.

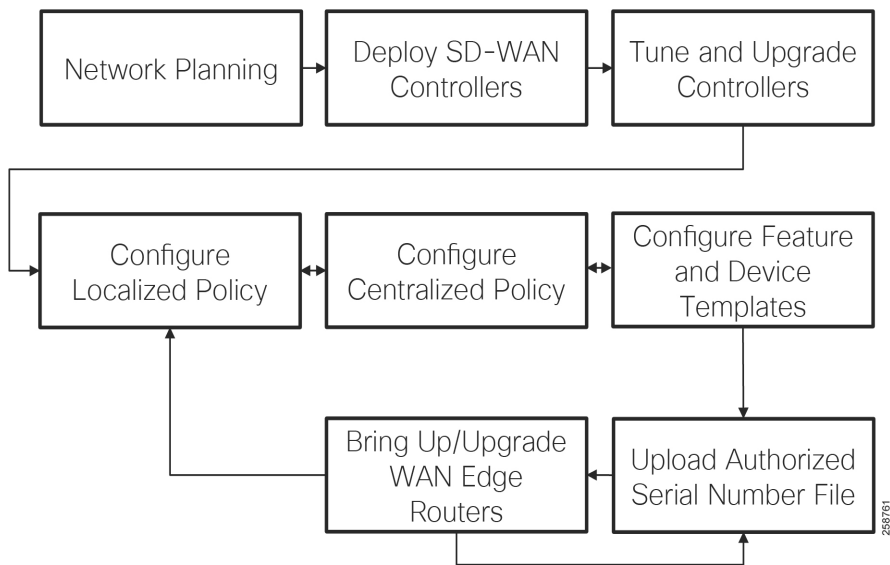
- vBond IP address or hostname must be configured under the vManage administration settings.
- vSmart is attached to a template.

Deployment Steps

As explained in the accompanying design guide, in order to have a fully functional SD-WAN overlay, there are a number of steps that need to be taken. The following image illustrates one example workflow that can be used as a reference. The order on the workflow for configuring policies and templates is flexible, the diagram shows the order followed in this guide.

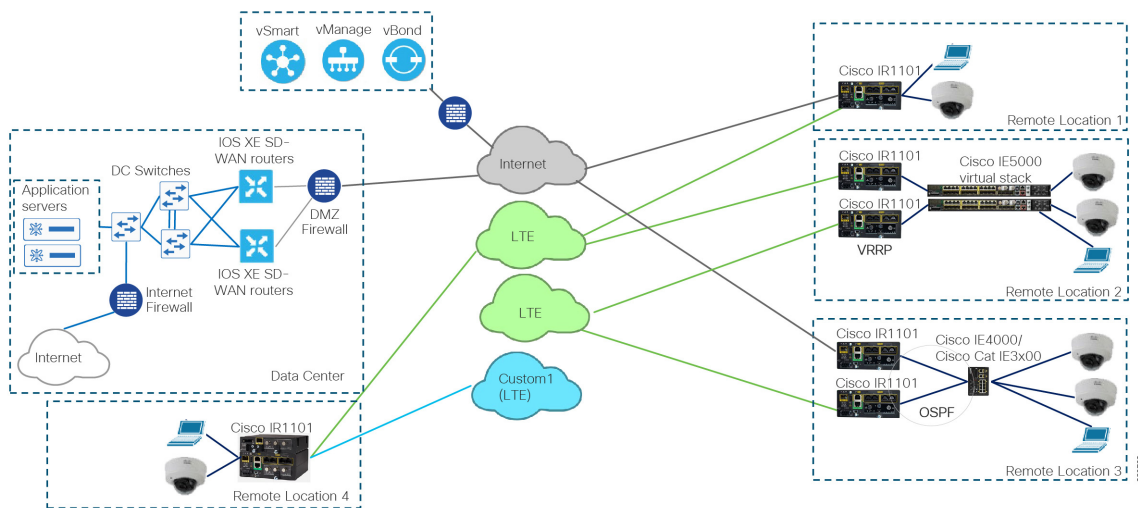
For Extended Enterprise deployment, it is assumed that these steps are already implemented for enterprise devices as explained in the prerequisites. This guide will focus on the details pertaining to the addition of a non-carpeted remote site such as network planning considerations for extended enterprise, template and policies configuration, and onboarding of Cisco IR1101. In addition, this guide will cover management, monitoring, and troubleshooting for the Cisco IR1101.

Figure 1 Deployment Flow Chart



Deployment Example

The following diagram shows the validated topology including a data center and four remote sites. In addition to the remote sites, branches can be added to the topology as shown in the **Cisco SD-WAN End-to-End Deployment Guide**. The four remote locations shown in the topology are an extension to the enterprise design.

Figure 2 Validation Topology

The routers are connected using different transport networks. In this implementation only public transports are used: Internet and Long-Term Evolution (LTE) networks. Tunnels are created on the device to send encrypted data over a transport and each tunnel on a device uses a different color. A color is one of the Cisco SD-WAN tunnel identifiers, there are 16 available colors to assign to a specific tunnel. In this example, tunnels use three colors: biz-internet, lte, and custom1 for an optional LTE network connection on a router. In the topology diagram biz-internet is shown as gray, lte as green and custom1 as blue. The tunnels are created without using the “restrict” setting, allowing you to establish inter-color tunnels. This means that remote site tunnels using biz-internet color can establish tunnels to other locations using the LTE or custom1 color as an example.

The SD-WAN controllers are deployed on premises, but the Cisco cloud-managed service is also supported. Controllers are reachable via the Internet transport. There is one vManage, one vSmart controller, and one vBond orchestrator; redundancy for the controllers is not covered in this guide.

Each IOS XE SD-WAN router attempts to make a connection to the controllers over each transport. It will initially connect to a vBond and will then connect to the vSmart controllers over each transport. Only one vManage connection is made from the IOS XE SD-WAN router, and it will depend on which transport first connected to it, but this preference is configurable.

Remote Site Connections

The design considers IOS XE SD-WAN router network connectivity as follows:

- Control connections: secure connectivity between the router and the SD-WAN controllers using Datagram Transport Layer Security (DTLS). It is established on the transport VPN (VPN0).
- Transport connections: secure tunnels between IOS XE SD-WAN routers. It is established using the transport VPN (VPN 0).
- Service VPNs: carry service-side data for devices connected to the IOS XE SD-WAN routers. Multiple service VPNs can be configured to provide traffic segmentation.

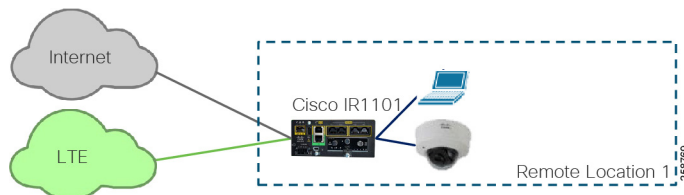
Note: the out-of-band management network (VPN 512) is not used for remote sites because it requires an additional connection.

Remote Site Examples

Each of the remote locations is an example of implementation:

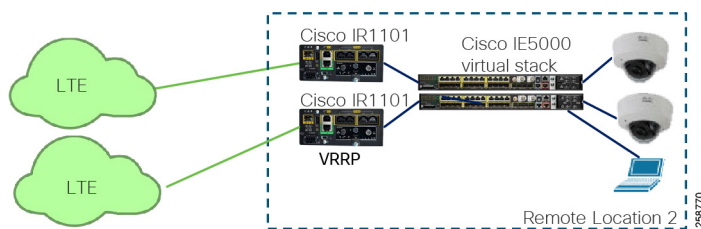
- Remote location 1 shows a single router with two WAN connections, one wired and one LTE.

Figure 3 Remote Location 1



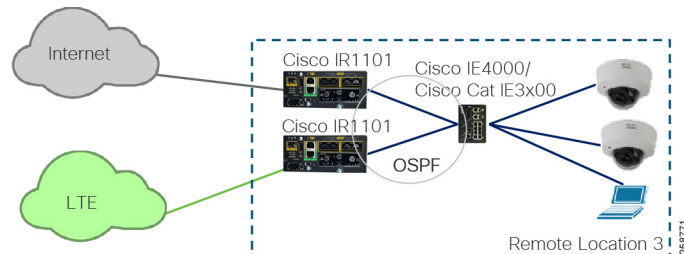
- Remote location 2 shows a site with two routers running Virtual Router Redundancy Protocol (VRRP) for hardware redundancy. Optionally, the routers may be connected to a virtual stack of switches to provide redundancy on the access switch too. Note that the switches need to be in a stack configuration because currently there is no support for channel or spanning tree protocol. Additionally, the connected switch can provide Power over Ethernet (PoE) to devices connected to it.

Figure 4 Remote Location 2

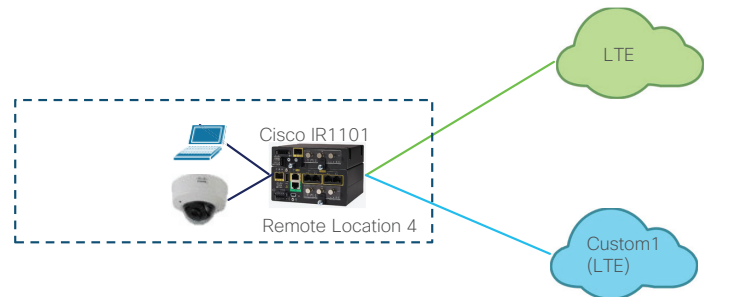


- Remote location 3 shows a site with two routers connected to a switch using Layer 3 connections and running Open Shortest Path First (OSPF) as the routing protocol to provide hardware redundancy for the Cisco IR1101. The router interfaces are configured for OSPF network point-to-point for each interface connected to the switch. As previous stated, the connected switch could be a stack of switches or a single switch. In this example, a single switch is used. The access switch is also used to provide PoE to devices.

Figure 5 Remote Location 3



- Remote location 4 shows a Cisco IR1101 with an expansion module. In this configuration the router can have dual LTE connections. A wired connection in addition to this is also possible but not shown in this example.

Figure 6 Remote Location 4


In all cases, static default routes pointing to the next-hop gateways are configured for tunnel establishment on all transports. Also, transport interfaces are configured for DHCP in order to dynamically obtain an IP address and gateway address. Nevertheless, an example of static configuration will be shown for reference.

Service-side configuration in this deployment has three service VPNs: shared services (VPN 1), IoT devices (VPN 10), and employee (VPN 11). This is to showcase how to configure segmentation on the service side, and by using the service-side segmentation IoT devices can be isolated from employee services for security. As an example, IP cameras connected to the IoT devices VPN are completely isolated from employee devices.

Service networks on the Cisco IR1101 are configured using Switched Virtual Interface (SVI). An SVI must belong to only one VPN but multiple SVIs can belong to same VPN. For example, IP Cameras and Badge readers can use different IP ranges but belong to the IoT VPN at the same time. The switchports on the Cisco IR1101 can be configured as trunks carrying multiple SVIs when connecting to a switch as in remote locations 2 and 3. Alternatively, they can be configured as access ports for directly connected devices as in remote locations 1 and 4.

It is not necessary that every remote site is configured with all service VPNs. Templates for a specific location can be customized to exclude service VPNs not needed at a site. For example, a site with only IoT endpoints does not need employee or shared services VPNs.

Validated Hardware and Software Matrix

The following table contains a list of the verified hardware and software components.

Table 1 Validated Components

Role	Cisco Platform	Version
Extended enterprise remote site WAN routers	IR1101	IOS XE SD-WAN 16.12.1d
Extended enterprise remote site WAN routers expansion module	IRM-1100-SPMI	NA
Cellular Modules for Cisco IR1101	P-LTEA-EA P-LTEA-US P-LTEA-VZ	NA
Extended enterprise Service Side Switch/Router	IE4000 / IE5000	15.2(7)E0
	Catalyst IE3200 / IE3300 / IE3400	16.12.1
SD-WAN controller	vBond, vSmart, vManage	19.2
Data center WAN routers	ISR4321	IOS XE SD-WAN 16.12.1d

Network Planning

As part of network planning it is important to consider the following items when deploying templates and policies:

- Device placement, system IP addresses, and site IDs; For site ID, consider using 32 bits for site identification as shown in the table. This numbering system allows for scale.

Table 2 Recommended for Site ID

Continent	Country	Site Number
1-7	1-999	1-9999

- Define transports and colors: Which devices will be connected to which transport? This will influence which interface templates are needed on the device.
- Define services for a site: What service networks do you need? What is the desired Segmentation? Which sites need access to which services?
- Plan for LAN networks: Do you need switch ports or access ports on the local site? Is the IOS XE SD-WAN router connected to a switch?
- Define redundancy options for a site: Are you using a routing protocol such as OSPF? Are you using VRRP for hardware?
- Is there a preferred path for devices with multiple transports? Deep Packet Inspection (DPI) may require selecting a preferred path for traffic symmetry as explained later in the document.

Consider policies that may be needed. Policies can be created as part of planning or during day-n operations, but it is recommended to determine policy items before deployment. The policy wizard guides you through complete policy configuration, so knowing beforehand what policy elements are important for your deployment may simplify the process. Moreover, local policies need to be applied to device and feature templates; for this reason, configuring policies before templates eliminates the need to edit templates later.

For centralized policies consider:

- What is the desired topology or connectivity among WAN Edge routers? Is the topology applicable to all VPNs?
- What are SLA classes and requirements?
- What traffic needs to be classified and how?
- Do you need policers for incoming traffic?
- Do you need to restrict any applications?

For localized policies consider:

- Do you require any access control lists (ACLs)?
- What is the bandwidth distribution for different types of traffic?
- Is there a need for different scheduling policies depending on interface, for example LTE versus wired interfaces?
- Do you need any policies that affect local routing?

Policies

Policy influences the flow of data traffic among the IOS XE SD-WAN routers in the overlay network. There is a clear separation between control and data plane policies. Control policies affect the flow of routing information in the network control plane while data policies affect the flow of data traffic in the network data plane.

Policies are configured either centrally or locally. Centralized policy is provisioned on the centralized vSmart controllers in the overlay network, and localized policy is provisioned on the IOS XE SD-WAN routers. Centralized policies affect network wide while localized policies affect local network and interfaces.

Some results can be achieved using either policy, and this guide provides an example for a centralized policy as well as a local policy both affecting data and control planes. An explanation of key policy components and objective is provided in addition to steps for configuration.

The examples provided showcase a subset of use cases, but it is not a comprehensive guide to SD-WAN policies. For more information and options please refer to <https://www-author4.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration-guides-list.html>

In this deployment we describe the policies in the following table:

Policies

Table 3 Policy examples used in the implementation

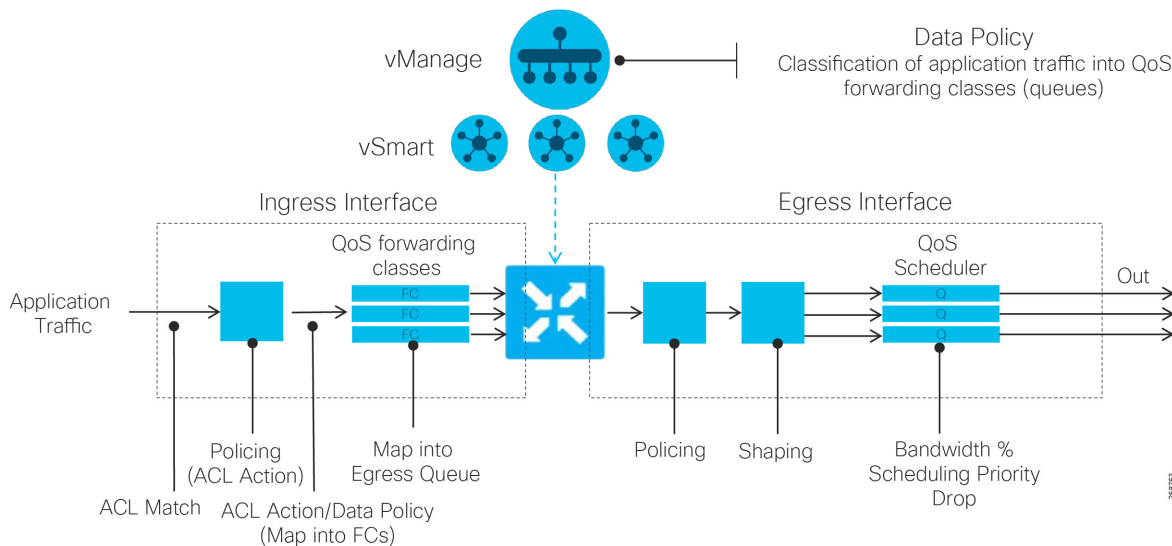
Use case	Description	Type of policy used	Implementation
Configurable VPN Topology	A VPN topology is configured mirroring <i>Cisco SD-WAN End-to-End Deployment Guide</i> , using hub and spoke topology for low bandwidth sites and mesh for high bandwidth sites. Alternatively, different topologies can be applied per VPN.	Centralized control	Configured in vManage Applied to vSmart affecting OMP routing information sent to IOS XE SD-WAN routers
Ensure SLA compliance	Application Aware Routing policies ensure SLA compliant path through the SD-WAN fabric. The SLA class defines loss, latency and jitter thresholds.	Centralized Application aware routing	Configured on vManage, enabled on vSmart controllers and enforced on IOS XE SD-WAN routers
Consistent classification and policing	Classify incoming data packets into multiple forwarding classes based on importance. Police incoming traffic. Match could be done based on application, DSCP, packet properties, source or destination. Localized policies could also be used, but note that localized policies do classification using up to layer 4 parameters. Centralized policies provide layer 7 visibility.	Centralized data policy	Configured on vManage, enabled on vSmart controllers and enforced on IOS XE SD-WAN routers
Schedule traffic based on importance	QoS map is defined to specify bandwidth and loss priority for every forwarding class. This enables you to determine how to prioritize data packets for transmission to the destination.	Localized data policy	Configured on vManage and applied to IOS XE SD-WAN router. Associated to a WAN interface on the router.
Influence local routing	Is used to influence routing decisions on the local site. On this implementation, it is used in the following cases: <ul style="list-style-type: none"> ■ To establish a preferred route for OSPF in a redundant router configuration. ■ To guarantee VRRP switchover when the primary loses connection to the transport. 	Localized control policy	Configured on vManage and applied to IOS XE SD-WAN router. Associated to features templates.
Create policies that restrict undesired communication	ACLs can be created to limit communication. It is possible to configure as centralized policy too.	Localized data policy	Configured on vManage and applied to IOS XE SD-WAN router. Associated to a WAN interface on the router.

QoS deployment

The following diagram shows how quality of service (QoS) works on IOS XE SD-WAN routers. At the service side traffic is classified according to a data policy, marked, re-marked, policed, and mapped into a forwarding class. On the transport side, traffic is policed, shaped, and scheduled. For this implementation, classification and ingress policing is done using centralized policies. Centralized policies are preferred instead of localized policies because it allows for application-aware classification, and it can be applied to all routers consistently from vSmart and eliminates the need to configure the policy on the specific interface templates.

On the other hand, scheduling and shaping can only be done in localized policies. Policing at the egress side is not covered in this document but it may be desired when there is a significant bandwidth difference between transports. Also, re-marking is not covered in this document but it is covered in the Cisco SD-WAN End-to-End Deployment Guide; the guide describes how to rewrite the DSCP values in the tunnel header in the event that the service provider supports less DSCP classes in use.

Figure 7 XE SD-WAN QoS



The following is an example of configuring a six-class QoS model. The table illustrates the bandwidth percentage and buffer percentage, the congestion avoidance algorithm. This is provided as an example; implementation parameters will depend of specific network requirements. In XE SD-WAN, the QoS configuration is limited to a maximum of eight classes.

Note: Queue 0 is always priority or Low-Latency Queuing (LLQ) and is used for Bidirectional Forwarding Detection (BFD) and SD-WAN control traffic. In this implementation voice traffic shares the low latency queue with SD-WAN control traffic.

Table 4 QoS Deployment Example

Class	DSCP	Scheduling Type	Bandwidth (Wired interface)%	Bandwidth (LTE interface)%	Congestion Avoidance Algorithm	Queue	Policer
Voice	EF/46	Priority Queuing (PQ)	10	10	Tail	0	
Broadcast-Video	CS5/40	Weighted Round Robin Queueing (WRR)	20	60	Tail	1	Policer-HD-Camera-4MB-drop
Network-Control	CS6/48	WRR	5	5	Tail	2	
OAM	CS2/16	WRR	10	10	Tail	3	OneMB-drop
Signaling	CS3/24	WRR	5	5	Tail	4	
Scavenger	CS1/8	WRR	50	10	Random Early Drop (RED)	5	

The following table describes the policer used.

Table 5 Policer List Example

Name	Burst	Exceed	Rate
Policer-SD-Camera-1MB-drop	20000000	Drop	1000000
Policer-HD-Camera-4MB-drop	80000000	Drop	4000000
OneMB-drop	20000000	Drop	1000000

Steps to configure the policies will be described in the Localized Policies and Centralized Policy. Centralized Policy sections, and will cover the following topics:

1. Map each QoS forwarding class to an output queue (localized policy).
2. Configure the QoS scheduler, which assigns the scheduling method, bandwidth percentage, and drop algorithm for each forwarding class (localized policy).
3. Create a QoS map, where all of the QoS schedulers are grouped (localized policy).
4. Define an access list to match traffic and assign to forwarding classes (centralized policy). Apply policer if desired.
5. Apply the classification access list to an interface (localized or centralized policy). In localized policy, this is accomplished by referencing the access list in the VPN Interface template. For centralized policy, this is accomplished by applying the QoS data policy to a site and VPN list.
6. Apply the QoS map to an egress interface (configured in the VPN Interface Ethernet template).

Localized policies

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

Policies

Note that only one localized policy can be applied per device, but one policy can be shared across many devices. It is possible to create a localized policy that applies to all remote sites, or to create smaller policies and apply different ones to different site types. Localized policy is attached to a device template. Once the policy is attached to the template and deployed to the device, the route policies, access lists, and other components in the policy can be referenced in any of the feature templates attached to the device template. You will not be able to configure a feature template in a device template that contains a policy element without having a policy attached to the device template. If a device template has been attached to a device and you try to update one of the referenced feature templates with a policy element, but a policy has not yet been attached, the configuration update will fail.

In this section we will create a local policy that has the elements described in the table. Those elements are:

- QoS map to allocate bandwidth to queues. A queue is previously linked to a configured forwarding class.
- Route policy for OSPF route preference when there are redundant routers as the example shown in Remote location 3. Setting a preference is needed to guarantee traffic symmetry needed for DPI as explained later in this section.
- Route policy to track route for sites running VRRP. A prefix list containing a route in order for VRRP to track on it. When the OMP prefix route disappears, the primary router gives up VRRP primary status.
- ACLs to restrict unwanted traffic. In this implementation a policy is created to restrict traffic among IP cameras. IP cameras should only communicate with video server, so restricting IP camera to IP camera traffic could prevent a malicious device to be connected to a camera port and reach or infect other devices.
- Flow visibility.
- Application visibility, or Deep Packet Inspection (DPI) is used to classify applications and put them on different SLA classes.

Traffic Symmetry for DPI on Dual Router Scenarios

In order for DPI on a WAN Edge router to be able to classify most application traffic, it is important that the WAN Edge router sees network traffic in both directions. To ensure symmetry at dual WAN Edge router sites, traffic should prefer one router in both directions, from the LAN to the WAN and from the WAN to the LAN over the overlay.

In this implementation traffic is influenced by:

Table 6 Determining Traffic Path on Dual Router Scenario

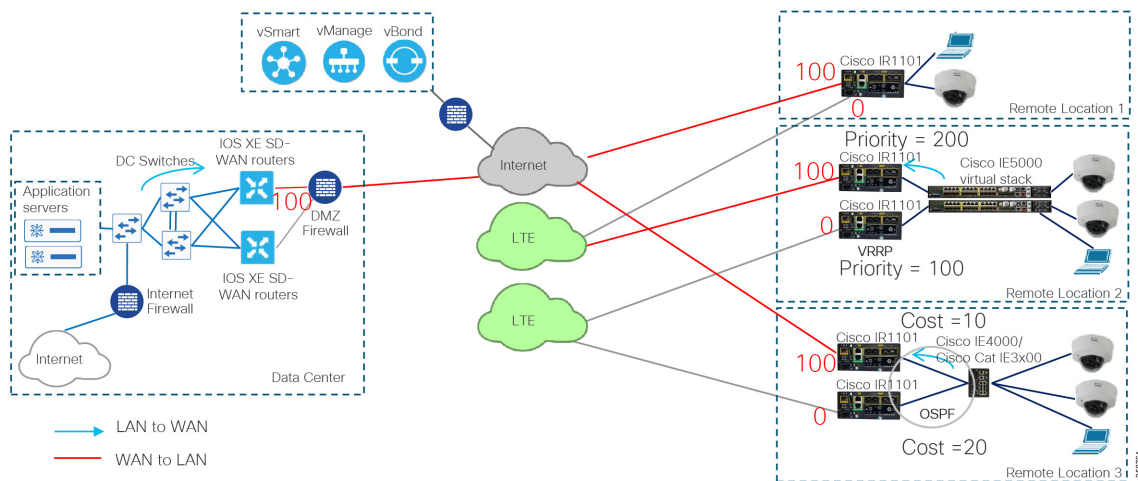
Direction	Parameter
WAN to LAN	Tunnel preference is one way to control WAN to LAN direction. This parameter is contained within the Tunnel section of the interface templates, and a variable was already created for it when the feature templates were created. When attaching a device to a template, select preference values to achieve desired topology.
LAN to WAN (applies only to redundant sites)	<p>For sites running VRRP as remote location 2 in the diagram, the preferred path is defined by VRRP priority.</p> <p>For sites running OSPF as remote location 3 shown in the diagram, route is influenced by localized route policy.</p> <p>On Data center running BGP, route is influenced by localized route policy as explained on <i>Cisco SD-WAN End-to-End Deployment Guide</i>.</p>

Note that there are other ways to influence traffic path such as application aware routing. Make sure to think about traffic symmetry for DPI on dual router scenarios when designing your network.

The following diagram shows preferred path for each router in this implementation in red, the numbers next to the tunnels indicate tunnel preference. 100 is configured for higher preference, other tunnels are configured with default value of zero.

Policies

Figure 8 Symmetric Traffic Configuration for DPI

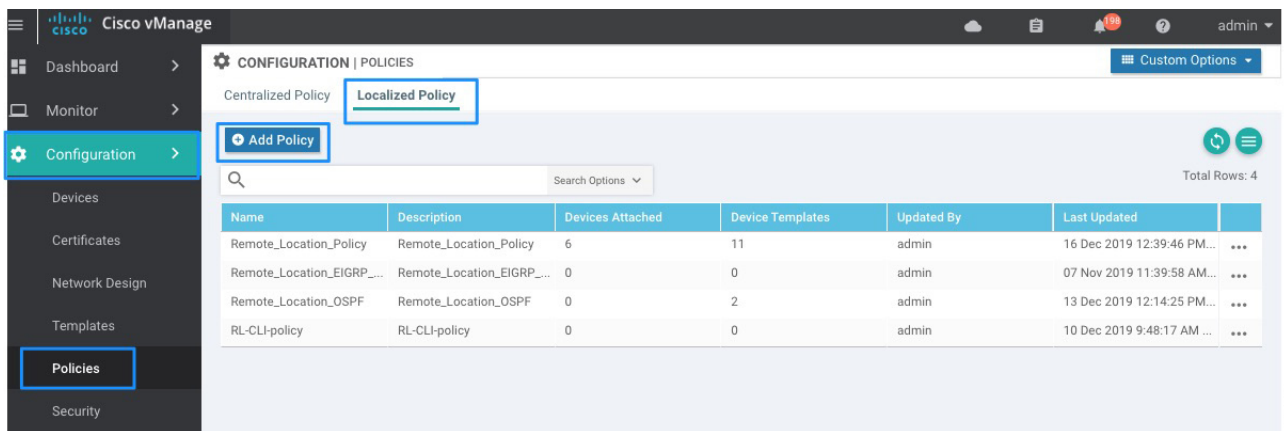


Configure Localized Policy

To configure the localized policy complete the steps below.

1. Go to **Configuration > Policies**.

Figure 9 Local Policy Creation



2. Select the **Localized Policy** tab.
3. Click on **Add Policy** to open the policy wizard.

Create Groups of Interest

The first step is to create groups of interest that will be used for matching or to perform actions later in the policy.

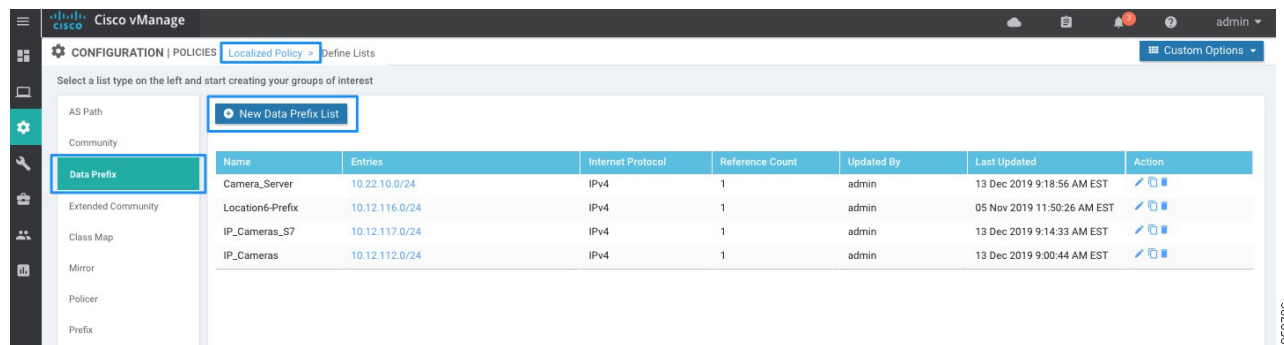
4. Select **Data Prefix** from the left panel. In this implementation data prefixes are created to use in ACLs. Click **New Data Prefix List**.

Policies

5. Enter a name, select **IPv4** radio button, and add the data prefix with network mask. Click **Add** and repeat for every data prefix. Use the following example as reference.

Table 7 Data Prefix List Example

Name	Data Prefix
IP_Cameras_S7	10.12.0.0/16
Camera Server	10.22.10.0/24

Figure 10 Define Lists Example

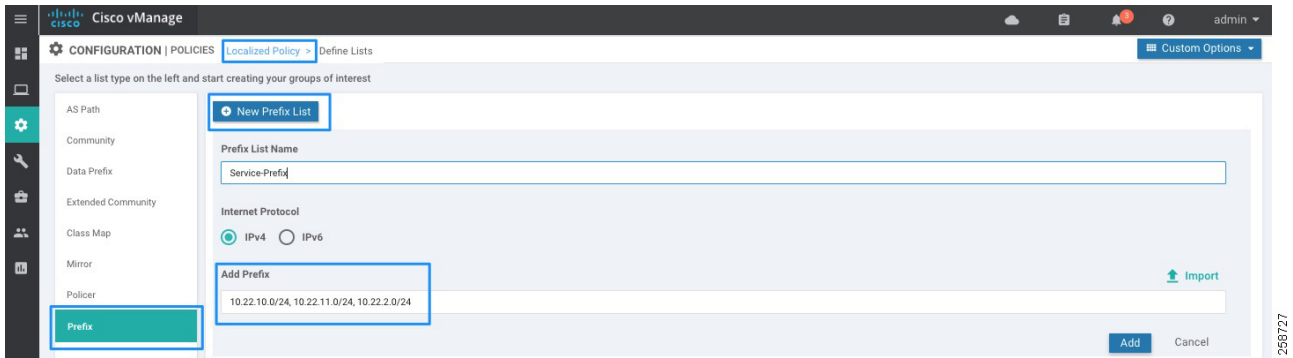
6. Another group of interest is the class map to be used for QoS scheduler. These provide a mapping from the Forwarding Class to an output queue. Select **Class Map** from the left panel.
7. To add a new entry, click **New Class List**. Enter a class name and select an option from the Queue drop-down list. Click **Save**. Table 4 QoS Deployment Example can be used as an example. Note that there is no need to create a class for queue 0 since this class is always created. Class 0 is used for Bidirectional Forwarding Detection (BFD) and SD-WAN control traffic.

Table 8 Class List Example

Class	Queue
Broadcast-Video	1
Network-Control	2
OAM	3
Signaling	4
Scavenger	5

8. Next, create prefixes. The prefix in the example will be used to track a route on a remote site for VRRP switchover when transport is unavailable on the primary router. Click **Prefix** on left panel and then click **New Prefix List**.
9. Enter a list name, click the **IPv4** radio button, and enter the prefix with network mask; make sure the prefix is available on a remote site or data center, otherwise the VRRP router will not become active. The prefix could define the default route if available. It is possible to add more than one prefix separated by comma. Click **Add**.

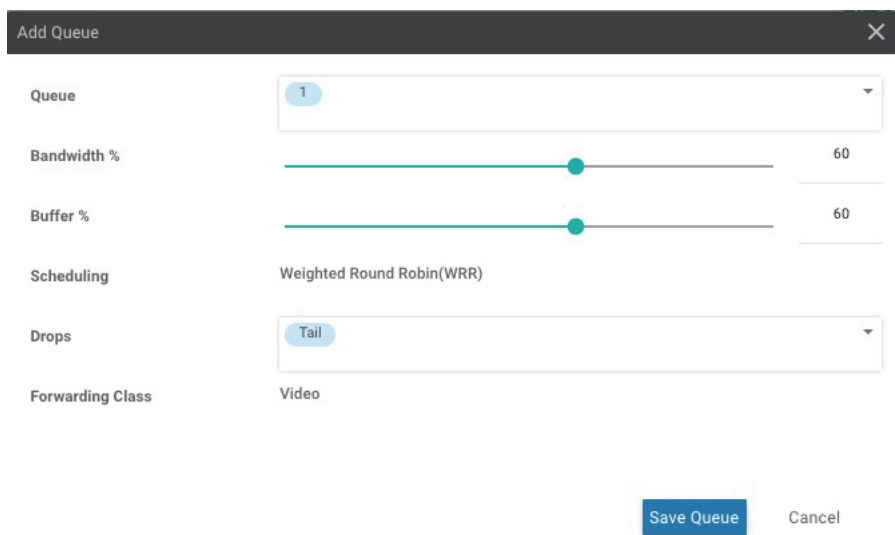
Figure 11 Add a Prefix List



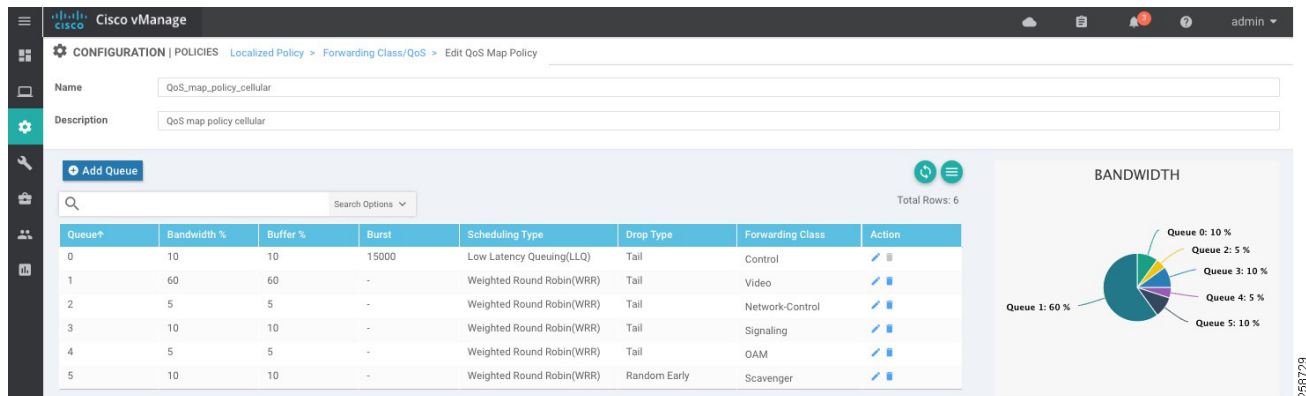
Configure Forwarding Classes/QoS

10. After all groups of interest are created, click **Next** on the wizard to move to the **Configure Forwarding Classes/QoS** step. This will define the Queue type, drop type (tail or random early), and bandwidth allocation per queue.
11. On the **QoS Map** tab, click **Add QoS Map**; a drop-down list with **Create New** or **Import Existing** appears. Choose **Create New**. Note that the **Import Existing** option could be used if a QoS Map was already created.
12. Add a name and description to the QoS map policy.
13. Click **Add Queue**.
14. Select a queue and the bandwidth percentage using the slider. Select buffer percentage, scheduling type, and drop type. Note that the buffer percentage value does not apply to IOS XE SD-WAN routers at this release. Click **Save Queue**.

Figure 12 Add Queue



15. Repeat steps 13-14 for every queue configured on Step 7. Bandwidth for Queue 0 will be calculated automatically. Use Table 4 QoS Deployment Example for reference.

Figure 13 QoS Map Policy

16. Click **Save Policy**.

17. (Optional) Create another QoS Map repeating Steps 11 to 16. This will allow you to define different scheduler for interfaces where different bandwidth is expected, for example cellular versus Internet links. Each policy will allow traffic to be treated differently as shown in Table 4 QoS Deployment Example.

Configure Access Control Lists

ACLs are created to control data traffic. In this example, traffic among IP cameras is restricted. IP cameras need to reach the camera server only, and creating the ACL will prevent a malicious endpoint being connected to a camera port and accessing or infecting IP cameras.

18. Click **Next** to configure Access Control Lists.

19. Click **Add Access Control List Policy** and then select **Add IPv4 ACL Policy** from list. Alternatively, an already existing policy can be associated by selecting **Import Existing**.

20. Add a name (Camera-To-Camera-Deny) and description to the policy.

21. Click **Add ACL Sequence** on the left panel.

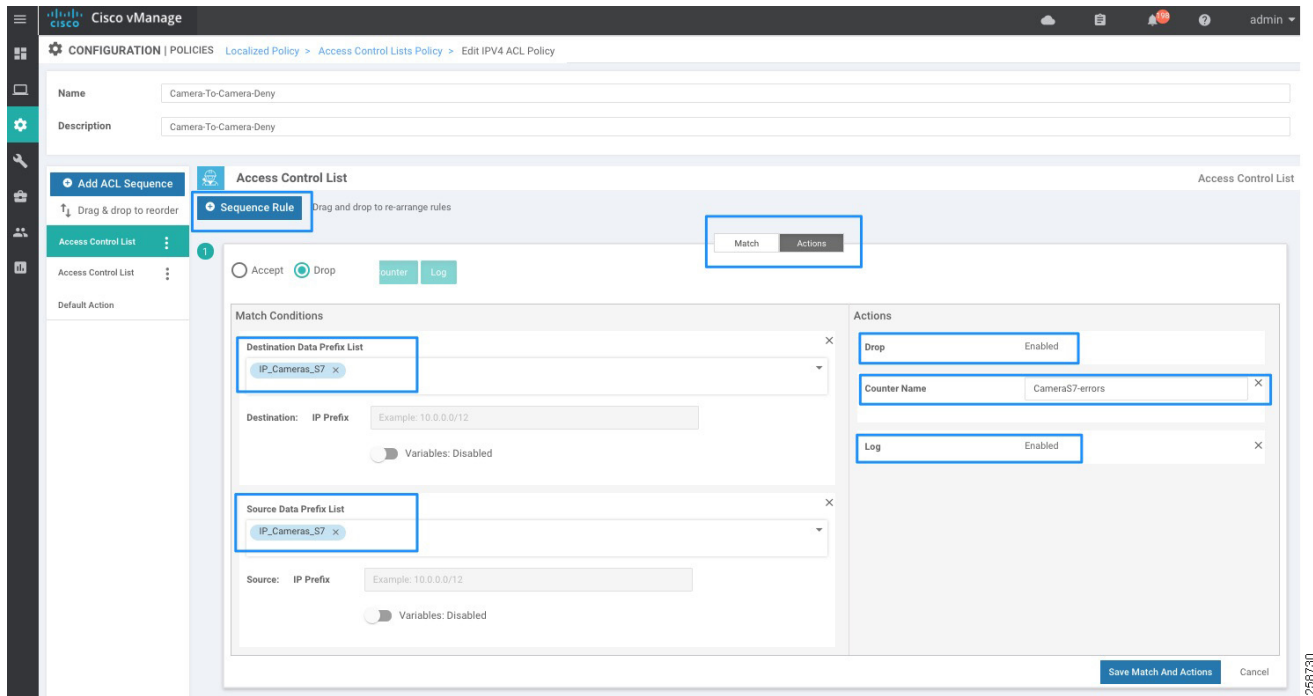
22. Click **Add Sequence Rule**. On the match tab, select **Source Data Prefix** and select a prefix from the list created at Step 5. Use Figure 9 for reference.

23. On the **Match** tab, select **Destination Data Prefix** and choose a prefix from the list created at Step 5.

24. On the **Actions** tab click the **Drop** radio button.

25. Optionally add a counter. Enter a name in the **Counter Name** field and set the **Log** field to **Enabled**.

Figure 14 Access Control List

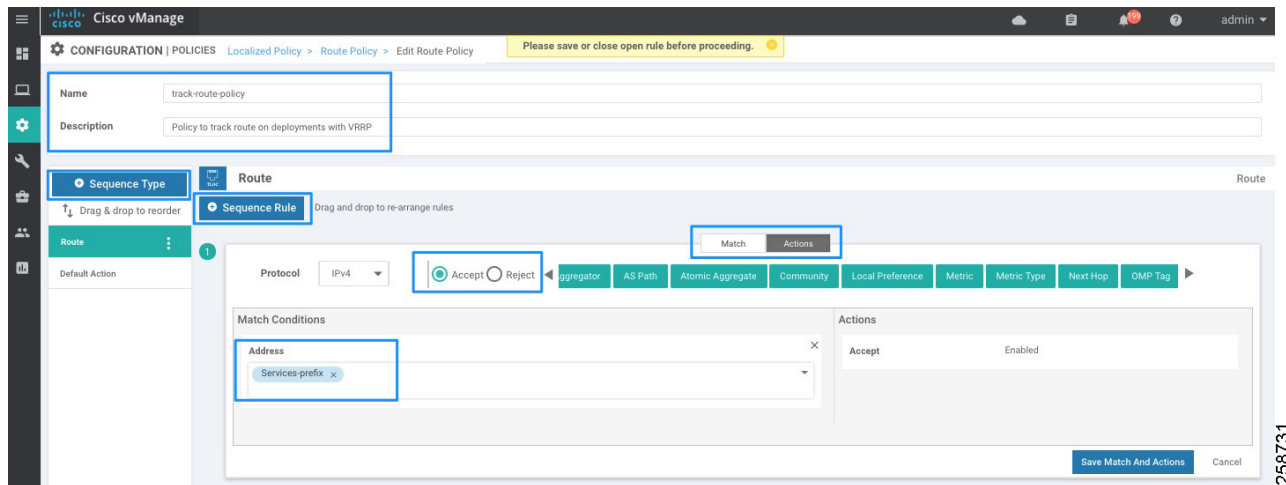


26. Click **Save Match And Actions**.
27. Repeat Steps 21 to 26 if more entries are required.
28. Click **Default Action** on the left panel. Click the pencil icon to edit and select the **Accept** action. Click **Save**.
29. Click **Save ACL Policy**.

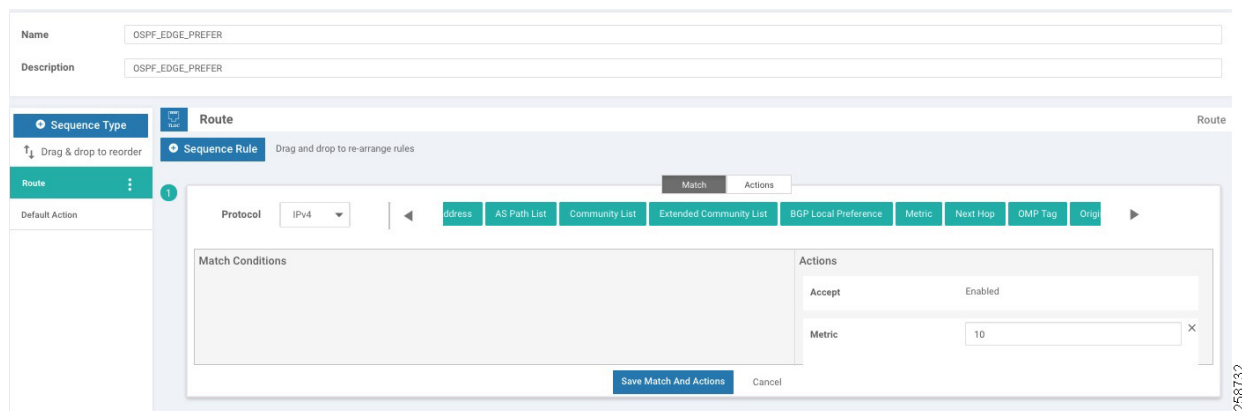
Configure Route Policy

Three policies are created as explained in the [Policy examples used in the implementation, page 15](#) table.

30. Select **Next** to move to **Configure Route Policy**. Click **Add Route Policy** and then select **Create New**.
31. Enter a name and description. For the policy used to track routes on deployments with VRRP redundant routers we are using:
 - Name: track-route-policy
 - Description: Policy to track routes on deployments with VRRP
32. Select **Sequence Type** on the left panel. Click **Sequence Rule**.
33. On the **Match** tab, select **Address**.
34. Select the prefix created on Step 9.
35. On the Actions tab, click the **Accept** radio button.
36. Click the **Save Match And Actions** button.

Figure 15 Local routing Policy Creation

37. Select **Default Action** on the left panel. Click the pencil icon to edit, then click **Accept**. Click **Save**.
38. If creating policy for OSPF preferred route, repeat Steps 30 and 31 with settings:
 - Name: OSPF_EDGE_PREFER
 - Description: Policy to set OSPF routing preference to preferred router
39. Select **Sequence Type** on the left panel. Click the **Sequence Rule** button.
40. On the Actions tab, click the **Accept** radio button.
41. On the Actions tab, click **Metric** and then enter **10** in the Metric field.

Figure 16 Route Policy for OSPF preference

42. Click **Save Match And Actions**.
43. Select **Default Action** on the left panel. Click the pencil icon to edit, then click **Accept**. Click **Save**.
44. Repeat Steps 38 to 43 with the following parameters:
 - Name: OSPF_EDGE_SEC
 - Description: Policy to set OSPF routing preference to secondary router

Policies

Metric: 20

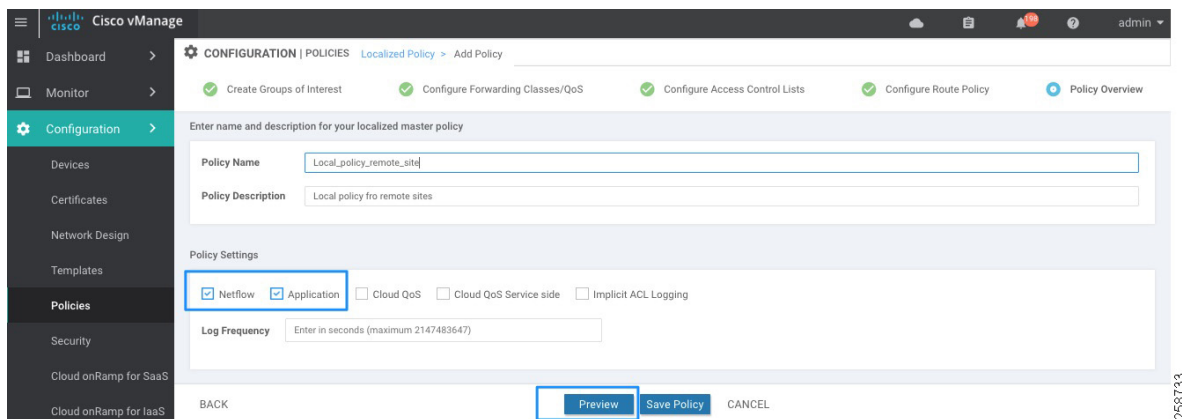
45. Click **Next** to go to Policy Overview.
46. Enter the policy name (**Remote_Location_Policy**) and description.

Enable DPI and NetFlow

In order to enable Deep Packet Inspection (DPI) and traffic monitoring follow these steps. These settings were configured but not validated as part of the scope of this CVD.

47. Check the **NetFlow** check box so the WAN Edge router can do traffic flow monitoring and send the information to vManage.
48. Check the **Application** check box to turn on DPI, or application visibility. DPI will allow a WAN Edge router to discover, monitor, and track the applications running on the LAN. This enhances the application information that appears within the vManage GUI.

Figure 17 Local Policy Preview



49. Click **Preview** to see generated CLI configuration output.
50. Click **Back** to make changes or click **Save Policy** to finish.

Tip: When saving a policy that has been already applied to devices, the wizard will continue to a Configuration Templates screen to show devices that will be updated. Click **Next** to preview changes and then click **Configure Devices** when you are ready to push the configuration. Confirm that you want to proceed.

Centralized Policy

Centralized policies are configured on vManage and downloaded to vSmart nodes. They use lists such as network prefixes, colors, and SLAs for defining targets of policy application and matching. Policy application is applied to a set of sites configured on a site list.

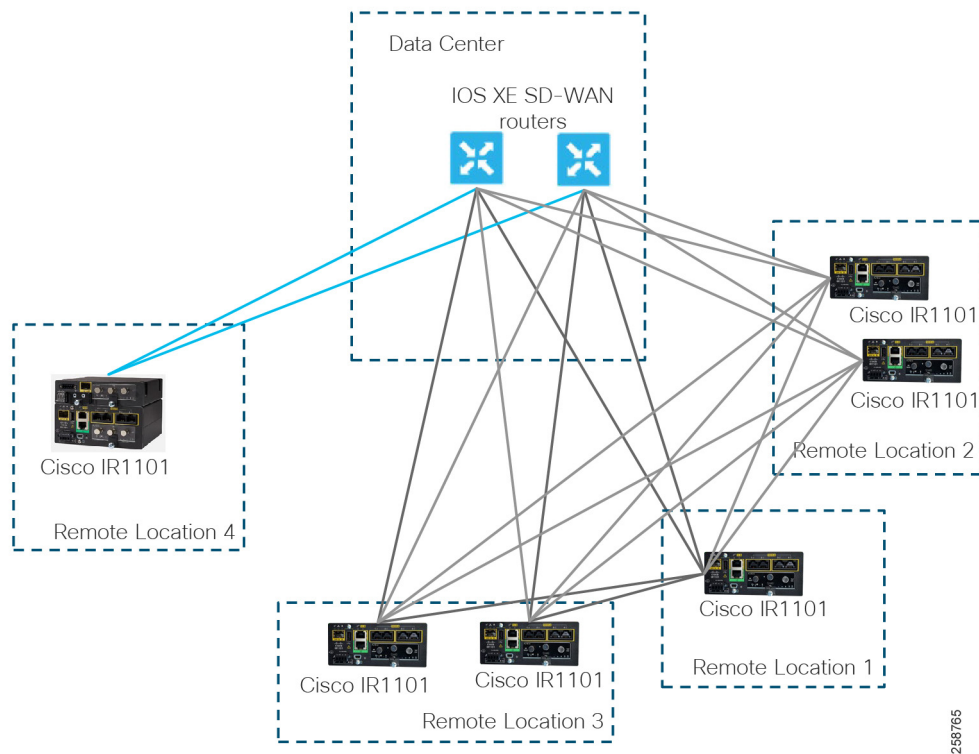
Centralized policies can be used to select the traffic path based on application SLA (application-aware routing), provide a consistent centralized data policy at the ingress on the service side (traffic policing, admission control, classification, marking and re-marking, path selection, service chaining), and affect traffic behavior for the entire SD-WAN fabric with control policies. Control policies are used for flexible VPN topology configurations, service chaining, traffic engineering, service and path affinity, and so on. Control policies act on OMP routing advertisements, whereas data policies act on application traffic characteristics.

Polcies

Only one centralized policy can be downloaded to a vSmart controller at a time. The policy contains a series of control or data policy definitions inside the centralized policy that are applied to site and VPN lists. Once saved, the centralized policy will be downloaded to the vSmart controllers.

The centralized policy showcased in this implementation has the following objectives:

- Defines overlay topology. This example uses configuration from the *Cisco SD-WAN End-to-End Deployment Guide* in which low-bandwidth sites could use a hub-and-spoke topology to save bandwidth while higher bandwidth sites use a full-mesh topology. Control connections are depicted in [Figure 18](#). Remote Site 4 is a low bandwidth site, only forming IPsec tunnels with the data center. This is accomplished by filtering routes and TLOC routes.
- Defines an application-aware routing policy. It affects traffic flowing from the service (LAN) side to the transport tunnel (WAN) side. Traffic is matched and placed into an SLA class, with certain loss, jitter, and delay values. The routing behavior is as follows:
 - Traffic will be load-balanced across all tunnels meeting the SLA class. If no tunnels meet the SLA, the traffic is sent through any available tunnel unless SLA is configured as “strict”. If the SLA is strict, traffic will only be forwarded if the SLA is met.
 - If preferred colors are specified in the policy, then traffic will be sent through the preferred color tunnels as long as the SLA is met. If no tunnels meet the SLA, the traffic is sent through any available tunnel.
 - If a backup-SLA preferred color is specified, then that tunnel is used when there are no paths that meet the SLA. Another path is used if the backup tunnel is unavailable.
 - The policy can be configured with no default action, meaning, if traffic does not match any sequence in the list, it is routed normally according to the routing protocol. Alternatively, this default traffic can be placed into an SLA class.
- Configure an access list to match traffic and assign to the forwarding class.
- Creates and applies policer for incoming traffic.

Figure 18 Customized Topology

Configuration of a Centralized Policy

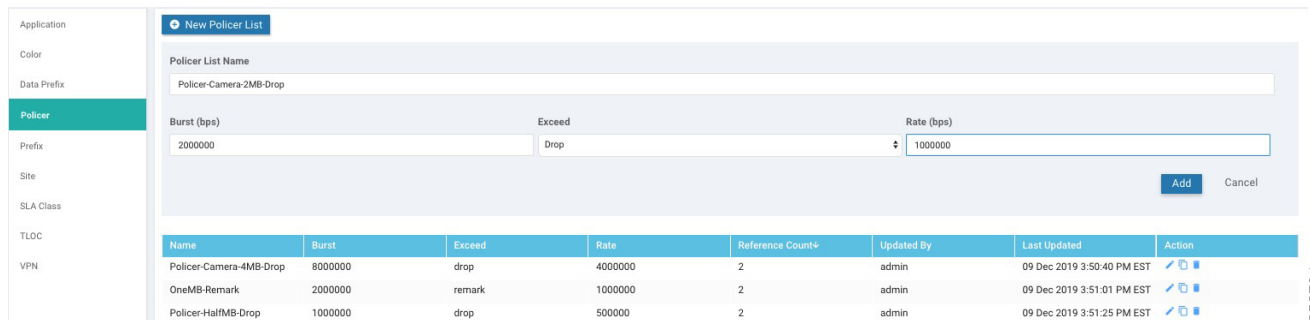
Create Groups of Interest

Similar to the local policy creation, the first step is to create lists that will be used in the policy, such as application, color, data prefixes, policer, prefix, site, SLA class, TLOC, and VPN lists. At a minimum, a list of site IDs is required to apply the individual policy definitions. Additionally, a list of the Service VPNs to which the policy may apply may be required.

1. (Optional) Create any application lists to match traffic based on application characteristics. This allows you to group applications so that you can reference the group as a whole. Refer to the [Cisco SD-WAN End-to-End Deployment Guide](#) for steps and an example.
2. Select **Policer** on the left panel to create a policer list. Use [Policer List Example, page 17](#) for reference. Click **New Policer List**.
3. Enter a name in the Policer List Name field and a bits per second (bps) value in the Burst field. In the Exceed menu, choose Drop or Remark actions. Enter a bps value in the Rate field.
4. Click **Add**.

Configuration of a Centralized Policy

Figure 19 Add New Policer List



5. Repeat Steps 2-4 as required.

6. Select **Site** on the left panel to create the site lists that will be used in the control policy. Click **New Site List**. The following lists are required for the example topology.

Table 9 Site List Example

Name	Entries	Purpose
Remote_Locations	10010200-10010400	Group all remote locations with Cisco IR1101
DC	10010100-10010199	Group all routers on data center
HB_Remote_locations	10010200-10010299	Apply a customized control policy to high bandwidth sites filtering low bandwidth sites
LB_Remote_Locations	10010300-10010399	Create hub and spoke topology for low bandwidth sites

7. Add name for the site list and sites. Click the **Add** button.

8. Select **SLA Class** on the left panel. Click **New SLA Class List** to add an SLA Class List for application-aware routing. There is a limit of four SLA classes that can be used by an application route policy. Use the following table for reference.

Table 10 SLA Class List Example

SLA Class list Name	Traffic type	Loss (%)	Latency (ms)	Jitter (ms)
SLA-Voice	Voice	1	150	30
SLA-Streaming-Video	Video	2	300	500
SLA-Operations	Network-Control	3	500	500
	Signaling			
	Network-Management			
SLA-Scavenger	Scavenger	5	500	500

9. Add an **SLA Class List Name**, and enter **Loss (%)**, **Latency (ms)** and **Jitter (ms)** values. Click the **Add** button.

10. Select **VPN** on the left panel and click the **New VPN List** button. This list will be used to define where a policy may apply. It may be useful to create separate list if you want granularity. In this example a single list is created for all the service VPNs.

11. Add a name (service_VPN_all) and a VPN list or range.

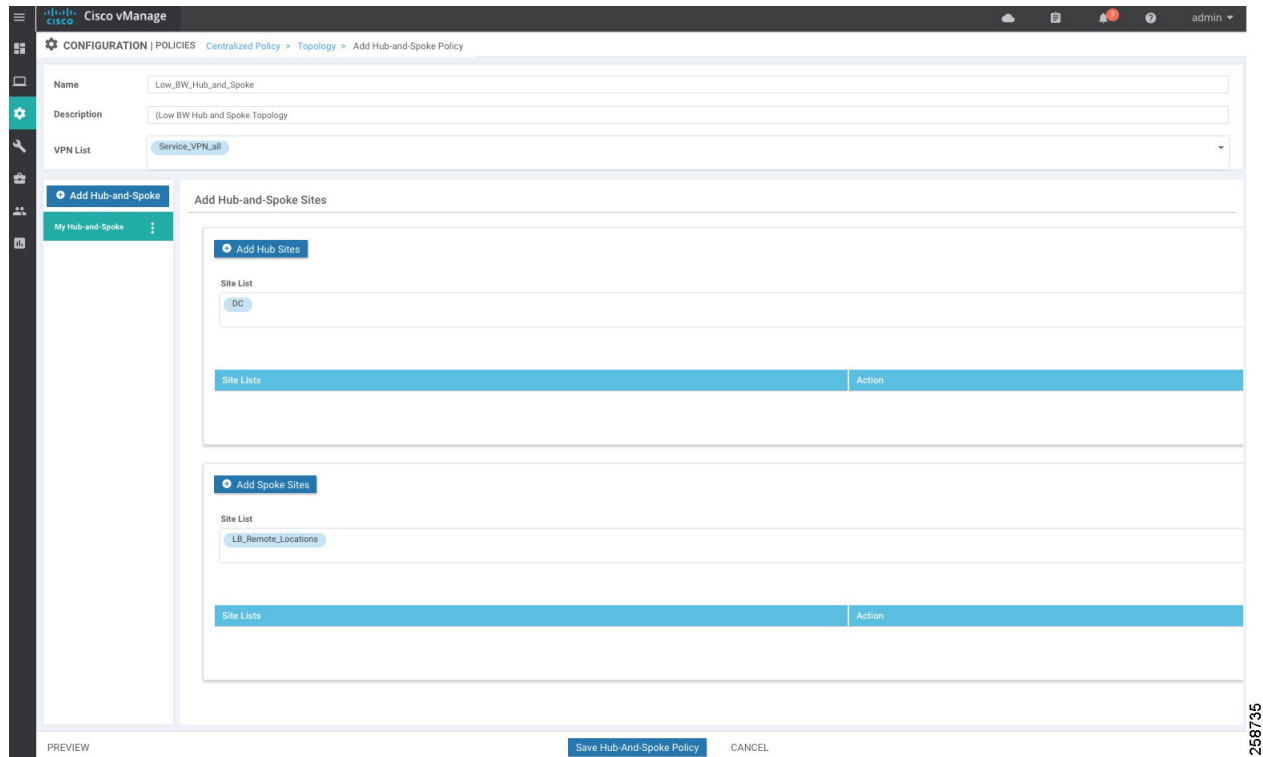
Configuration of a Centralized Policy

12. (Optional) Select **Data Prefix** on the left panel. Click **New Data Prefix List** to add a prefix to use in match conditions for policies. For example, create a prefix for IP Camera Servers to be used for traffic classification. Enter a name, select IPv4 and enter prefixes. Click the **Add** button.
13. Click **Next** to configure Topology and VPN membership.

Configure Topology and VPN Membership

This is the control policy definition; it can be a predefined full-mesh or hub-and-spoke policy, or a customized route and TLOC policy. Optionally, it is possible to allow or restrict VPNs in certain sites (not covered in this document). As depicted in Figure 18 Customized Topology, Remote Site 4 is a low bandwidth site, only forming IPSec tunnels with the data center. If no policy is applied, the default configuration is a full mesh.

14. On the Topology tab, select the **Add Topology** button. Select one of the options from the drop-down list: Hub-and-Spoke, Mesh, Custom Control or Import Existing. To create a hub-and-spoke topology for low bandwidth sites, choose **Hub-and-Spoke**.
15. Provide a name, description, and select a VPN list.
16. Click the **Add Hub Sites** button. Choose **DC**.
17. Click the **Add Spoke Sites** button. Choose **LB_Remote_Locations**.
18. Click the **Save Hub-And-Spoke Policy** button at the bottom of the page. You have just finished a policy definition that needs to be applied to a site list.

Figure 20 Hub and Spoke Topology for Low Bandwidth Sites

At this point, a hub-and-spoke topology will apply to low bandwidth sites, but high-bandwidth sites still have route and TLOC information for those sites and will attempt to form IPsec tunnels, resulting in partial WAN connectivity on the dashboard. To avoid partial connectivity an additional topology can be created to filter low bandwidth sites. Follow Steps 19 to 29 to create an additional topology.

19. On the Topology tab, click the **Add Topology** button and select **Custom Control (Route & TLOC)**.
20. Fill out name and description fields for the policy.
21. Select **Sequence Type** on the left panel. On the Add Control Policy pop-up window, select **Route**.
22. Select **Sequence Rule**.
23. Select **Match**, then select **Site** and under Site List, select **LB_Remote_Locations**. Under Actions, the default is already set to **Reject**.
24. Click the **Save Match and Actions** button.
25. Select **Sequence Type** on the left panel. On the Add Control Policy pop-up window, select **TLOC**.
26. Select **Sequence Rule**. Select **Match**, select **Site** and under Site List, select **LB_Remote_Locations**. Under Actions, the default is already set to **Reject**.
27. Click the **Save Match and Actions** button.
28. Select **Default Action** from the left panel. Click the edit symbol. Click the **Accept** radio button, then click the **Save Match and Actions** button.
29. Click the **Save Control Policy** button to save the policy definition.

Configuration of a Centralized Policy

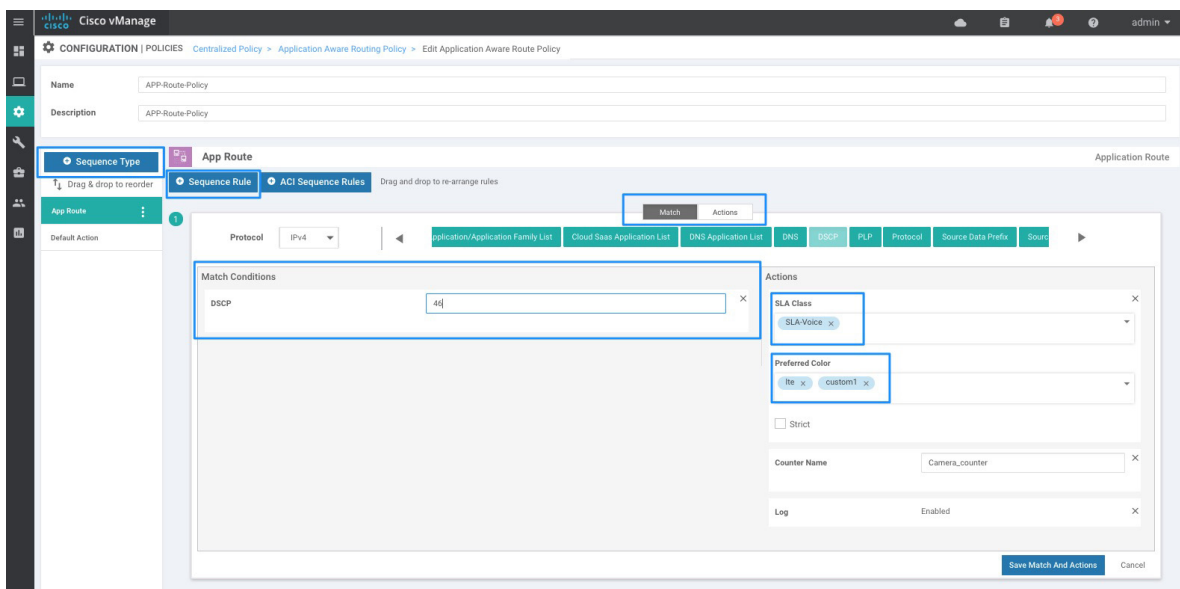
Tech tip: When you use the Predefined Hub-and-Spoke topology policy, only TLOCs and routes from the data center site are distributed to the low-bandwidth sites specified. Ensure a summary or default route is distributed from the data center if you want the low-bandwidth sites to reach other remote sites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

Configure Traffic Rules

This section is used to create the data policy. In this example we will configure application-aware routing and traffic data.

- 30. To create an application-aware routing policy click the **Add Policy** button on the Application Aware Routing tab.
- 31. Fill out the **Name** and **Description** fields.
- 32. Click the **Sequence Type** button.
- 33. Click the **Sequence Rule** button.
- 34. Under the Match tab, select the condition to be evaluated, for example DSCP.
- 35. Under the **Action** tab, select **SLA Class and Preferred Color** options. You can select a backup color, enable logs, and create a counter variable for occurrences. If the **Strict** check box is checked, the policy will restrict the traffic class to selected colors and drop the traffic if the SLA is not met. This could increase convergence times after a transport failover because a poll interval has to be completed after tunnel is back to make sure the SLA is met in strict condition.
- 36. Click the **Save and Match Actions** button.

Figure 21 Application Aware Route Policy



- 37. Repeat Steps 33 to 36 for every desired rule. The following table contains an example:

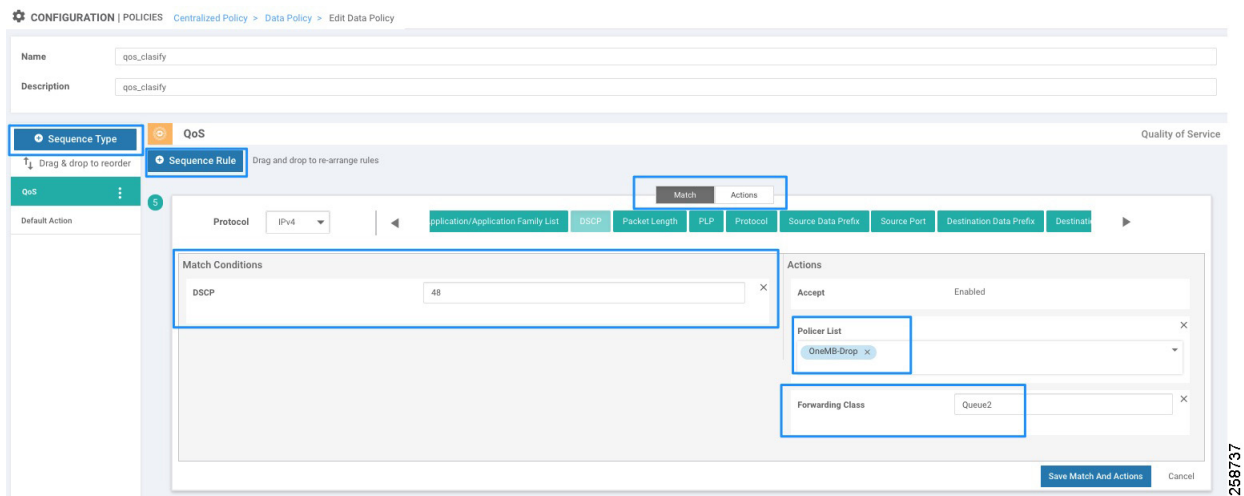
Configuration of a Centralized Policy

Table 11 Match Parameters for SLA example

Match Parameters	Application list name
DSCP: 46	SLA-Voice
DSCP: 40	SLA-Video
Destination Data Prefix: video_server	SLA-Video
DSCP: 48	SLA-Operations
DSCP: 16	SLA-Operations
DSCP: 24	SLA-Operations
DSCP: 8	SLA-Scavenger

38. Select **Default Action** in the left menu, and click the edit symbol. **None** is the default. Select the **SLA Class List** box, and select SLA-Scavenger from the SLA Class drop-down list. Click the **Save Match and Actions** button.
39. To create a Traffic Data policy to classify traffic on QoS forwarding classes, select **Traffic Data** tab and select **Add Policy > Create New**.
40. Provide a name and description.
41. Click the **Sequence Type** button on the left panel and then select **QoS**.
42. Click the **Sequence Rule** button.
43. Under the Match tab, select the condition to be evaluated, for example **DSCP**.
44. Under the Actions tab, select **Forwarding Class** and fill with values Queue0, Queue1, Queue2, Queue3, Queue4, Queue5, Queue6 or Queue 7 that matches the requirement.
45. (Optional) Select **Policer List** and apply a policer if required for specific rule.
46. Click the **Save and Match Actions** button.

Figure 22 QoS Centralized Data Policy



47. Repeat Steps 42-46 for every entry. The following table provides an example.

Table 12 Data Policy for QoS Classification and Policer Example

Traffic Type	Match Parameters	Forwarding Class	Policer
Voice	DSCP: 46	Queue0	
Voice	Destination Port:5060	Queue0	
Video	DSCP: 40	Queue1	Policer-HD-Camera-4MB-drop
Video	Destination Data Prefix: video_server	Queue1	
Network-Control	DSCP: 48	Queue2	
OAM	DSCP: 16	Queue3	OneMB-drop
Signaling	DSCP: 24	Queue4	
Scavenger	DSCP: 8	Queue5	
Scavenger	Any	Queue5	

- 48. Select **Default Action** in the left menu, then click the edit symbol. Click the **Accept** radio button. Click the **Save and Match Actions** button.
- 49. (Optional) Select **Sequence Type** on the left panel to add other data policies such as application firewall, service chaining, or traffic engineering. For more information on those policies refer to <https://www.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration-guides-list.html>
- 50. Click **Next** to continue to apply policies to sites and VPNs.

Apply policies to sites and VPNs

- 51. Fill out name and description fields for the centralized policy.
- 52. Click on the Application-Aware Routing tab. Click the **New Site List** and **VPN List** button.
- 53. In the Select Site List drop-down list choose **Remote_Locations** and **DC** sites.
- 54. Select the **VPN List** (Service_VPN_all)
- 55. Click the **Add** button.
- 56. Click on the **Traffic Data** tab.
- 57. Click the **New Site List and VPN List** button, then click the **From Service** radio button, and repeat Steps 53-55.
- 58. (Optional) Click the **Preview** button to see policy configuration.
- 59. Click the **Save Policy** button.

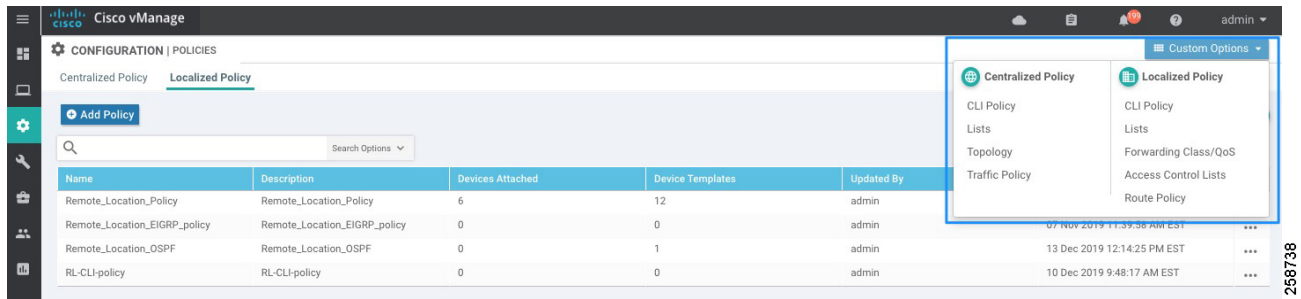
Activate Policy

- 60. Go to **Configuration > Policies**.
- 61. On the Centralized Policy tab all centralized policies are shown and the Activated column shows the active policy. Click on more actions (...) at the end of the row of the policy you want to activate and select **Activate** from the displayed options.
- 62. A dialogue box will appear and states that the policy will be applied to the reachable vSmart controllers. Click **Activate**. The policy will be pushed to the vSmart controllers and the status will indicate success.

Editing Policy Elements

The configuration steps provided in previous section show how to configure a complete policy with multiple elements in a single process. This is useful for initial implementation since it simplifies the process. If more elements need to be added or existing ones need to be modified after the policy has been created, use the **Custom Options** menu at the top right. It provides a **Lists** shortcut for both centralized and localized policies.

Figure 23 Edit Policy Elements

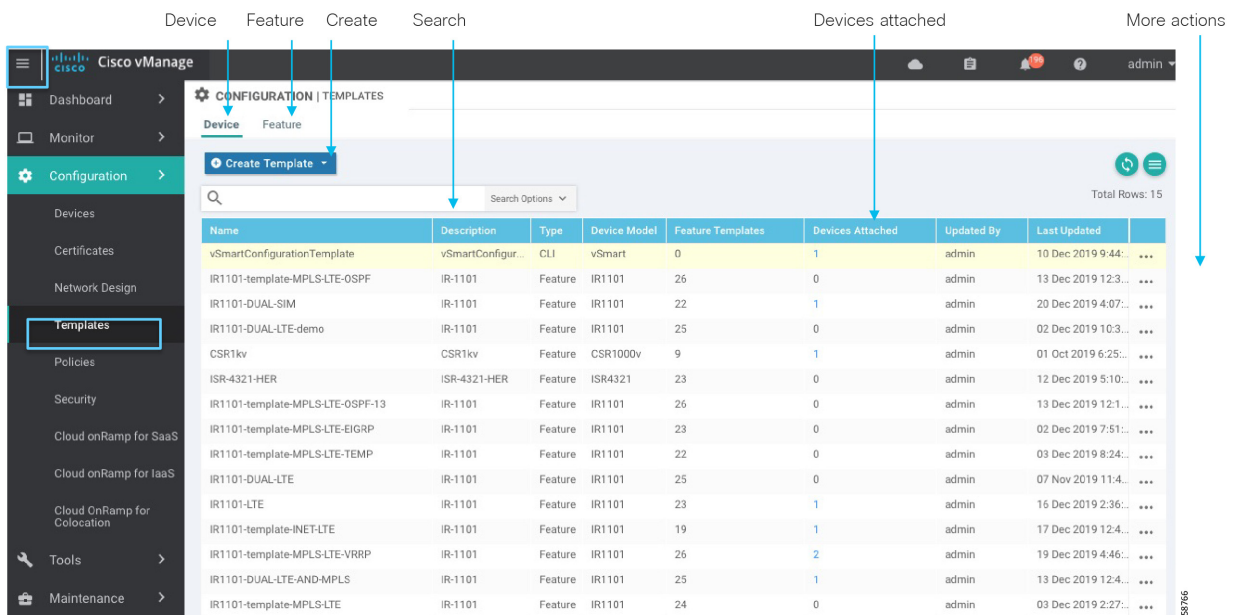


Template Configuration

The router device configuration is defined by templates created in vManage. A device template defines a device's complete operational configuration. It is possible to create device templates by consolidating together individual feature templates. Alternatively, they can be created by entering a CLI text-style configuration directly in vManage. Only feature templates are covered in this implementation guide. A feature template defines the configuration for an SD-WAN software feature; vManage comes with default feature templates but more can be created for customization.

The following image shows screen elements for template configuration that will be used in the rest of the section.

Figure 24 Template Screen Elements



Configuring Feature Templates

Before creating a device template, you must create individual feature templates that will be needed to create the device template.

Feature templates fall into three categories:

1. **Basic information:** includes settings for authentication, authorization, and accounting (AAA), BFD, global and system settings, Network Time Protocol (NTP), Overlay Management Protocol (OMP), and security.
2. **VPN:** used to create VPNs, WAN interfaces, and LAN interfaces
3. **Other templates:** includes miscellaneous templates such as banner, cellular controllers and profiles, DHCP server, routing protocols, Global Positioning System (GPS), logging, and switch ports.

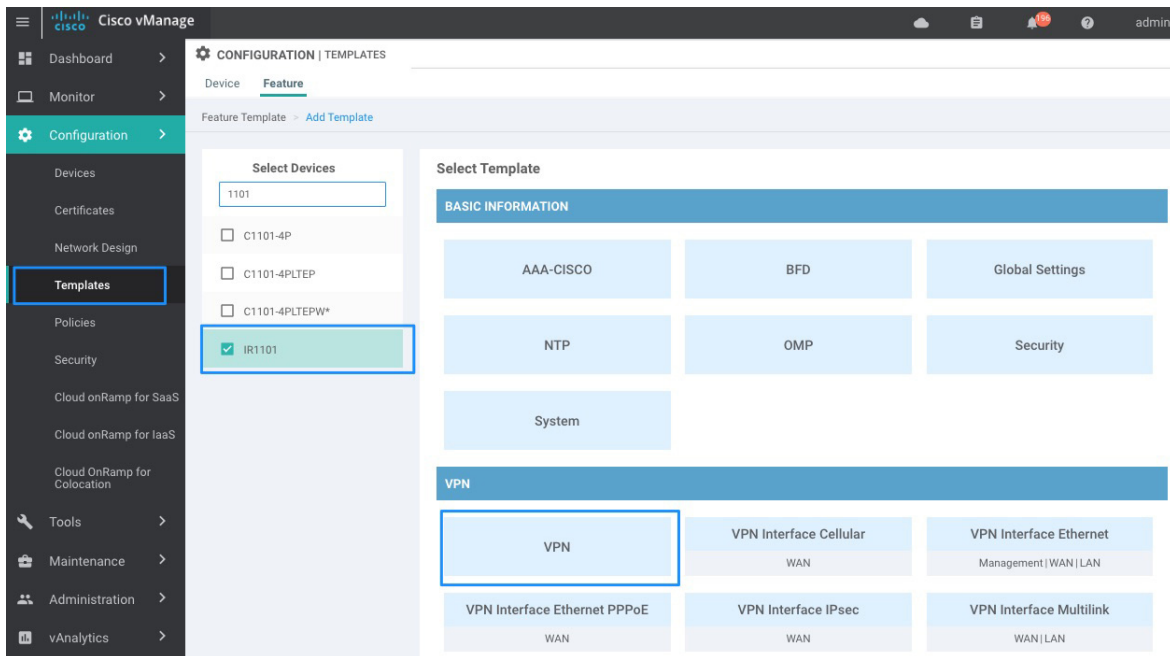
For this implementation basic information, banner, logging and SNMP templates are leveraged from the *Cisco SD-WAN End-to-End Deployment Guide*; refer to Appendix B for template values. This is to be used as an example, but it can be customized to meet specific needs. For example, BFD templates can be edited to change multiplier values for specific colors in order to reduce tunnel failover times. For more information on specific settings for a feature template refer to: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book/config-cmd.html>.

The following sections will cover the creation of templates required for extended enterprise, in addition to the ones referenced in Appendix B - Cisco SD-WAN End-to-End Deployment Guide Templates Used. First, we will explain how to create a template, and later we will provide blueprints to create specific templates needed.

Create a Feature Template

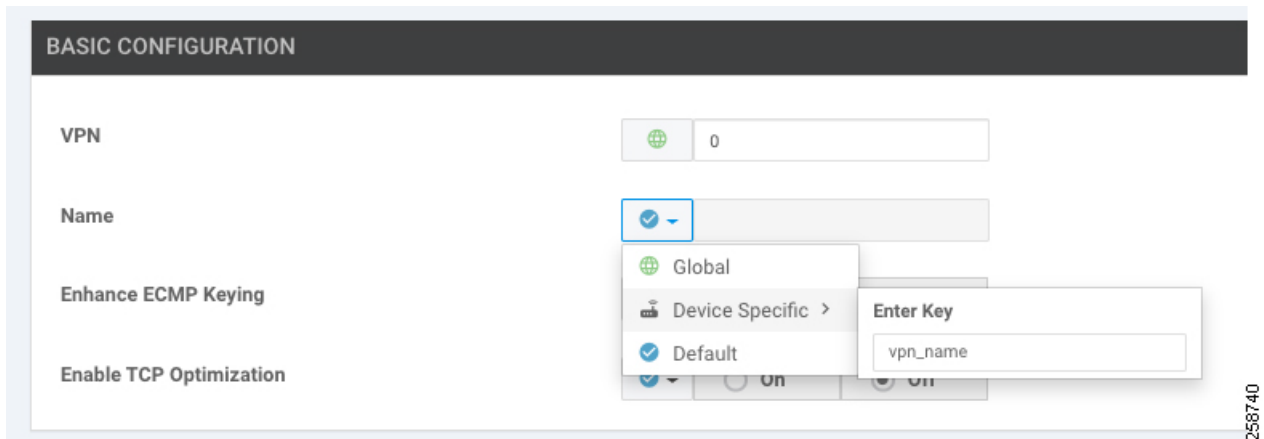
Before providing guidance to create specific feature templates for the Cisco IR1101, this section walks you through how to create a feature template.

1. In the vManage GUI, Select **Configuration > Templates**, and choose the **Feature** tab.
2. Click the **Add Template** button.
3. In the left pane, from Select Devices, select the type of device for which you are creating a template. You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.
4. In the right pane, select the feature template.

Figure 25 Feature Template Creation

5. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters. If the feature has optional parameters, the bottom of the template form shows a plus sign (+) after the required parameters.
6. In the Template Name field, enter a name for the feature template, and in the Description field, enter a description for the feature template. These fields are mandatory.
7. For each parameter that needs to be customized, choose the desired value, and if applicable, select the scope of the parameter. The scope is selected from the drop-down menu to the left of each parameter value box. The available options are:
 - a. Global parameters will apply to all devices using the template, for example VPN number.
 - b. Device-specific parameters create a variable to be set when the device is attached to the profile. An example of a device-specific parameter is static IP address. The name of the variable can be edited as shown in the following image.
 - c. Default parameters set the feature option to default configuration. When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, select global or device specific from the Scope drop-down list.

Click the plus sign (+) below the required parameters to set the values of optional parameters.

Figure 26 Scope of the Parameter

8. Click the **Save** button.

Note: Some configuration parameters can be marked as optional by checking the Mark as Optional row check box. This allows you to apply the feature template to devices with slightly different configurations. Values are entered when you attach a device to a device template. Optional values do not need to be provided.

Feature Templates for Transport VPN

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

The following steps create a feature template using the guidelines described in the Create a Feature Template section.

VPN 0 Template Reference

This template creates a VPN template for transport.

Feature Template type: VPN: VPN

Feature template name: RL_VPN0

Description: Remote Location VPN 0

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 13 VPN0 Feature Template

Section	Parameter	Type	Variable/value	Optional
Basic Configuration	VPN	Global	0	NA
	Name	Global	Transport VPN	NA
	Enhance ECMP Keying	Global	On	NA
DNS	Primary DNS Address	Global	64.102.6.247	NA
	Secondary DNS Address	Global	64.102.6.248	NA
IPv4 Route	Prefix	Global	0.0.0.0/0	No
	Gateway	Radio button	Next Hop	No
	Next Hop	Device Specific	vpn0_next_hop_ip_address_1	No
IPv4 Route (2)	Prefix	Device Specific	vpn_ipv4_ip_prefix2	Yes
	Gateway	Radio button	Next Hop	Yes
	Next Hop	Device Specific	vpn0_next_hop_ip_address_2	Yes
IPv4 Route (3)	Prefix	Device Specific	vpn_ipv4_ip_prefix3	Yes
	Gateway	Radio button	Next Hop	Yes
	Next Hop	Device Specific	vpn0_next_hop_ip_address_3	Yes

Note that IPv4 Route is repeated three times, the purpose of this is to allow a static route per transport interface. For a Cisco IR1101, three transport interfaces can be created—two cellular and one wired interface. In the suggested configuration, only one route is mandatory since at least one connection to transport is required.

To add each route:

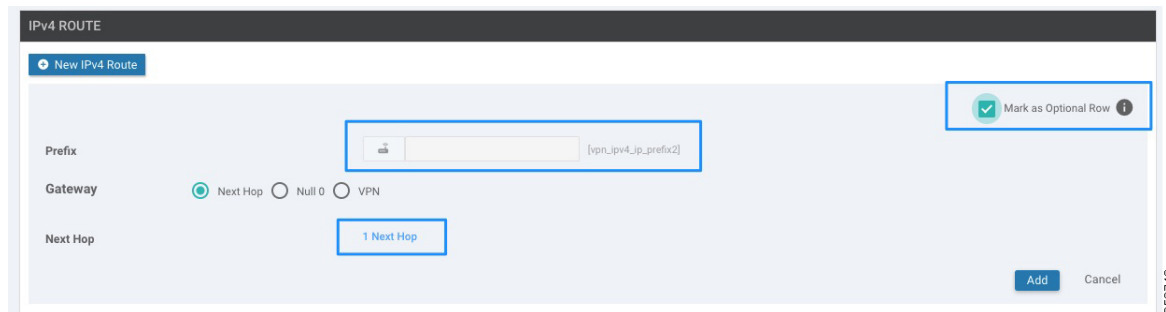
1. Click the **New IPv4 Route** button as shown in the figure.

Figure 27 New IPv4 Route

2. If adding one of the optional routes, change the prefix to device specific and provide a variable name; otherwise, select **Global**.
3. If adding an optional route, check the **Mark as Optional Row** check box. See figure below.
4. Click **Add Next Hop**, then in the dialog box click **Add Next Hop**.
5. Change the address to device specific and provide the variable name.

Click the **Add** button and the dialog box will close. The Next Hop field will show 1 Next Hop, as shown in figure below.

Figure 28 New IPv4 Route Details



6. Click the **Add** button.
7. If all other fields on the feature template are configured, click **Update**.

VPN Internet Interface Template Reference

This template is used to associate the interface to the VPN 0 template. Its purpose is to define interface settings for the wired transport. This template allows for dynamic IP address assignment for WAN interface GigabitEthernet0/0/0. Additionally, an IPSec tunnel is defined with color biz-internet for control and transport connections. The Restrict setting on the tunnel is disabled to allow inter-color communication. Finally, this template defines a preference variable that will determine if the interface is selected for directing traffic to the tunnel. A higher value is preferred over a lower one, and when two or more tunnels to the destination have the same preference value, the traffic is distributed among them.

Feature Template type: VPN: VPN interface Ethernet

Feature template name: RL_INET_INT

Description: Default DHCP interface for Internet connection

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 14 Interface Ethernet Feature Template for Internet Transport

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Global	GigabitEthernet0/0/0
	Description	Global	Internet Interface
IPv4 Configuration	IPv4 Address	Radio button	Dynamic
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
	Restrict	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced Options>Encapsulation	IPsec	Global	On

Template Configuration

	Preference	Device Specific	vpn0_inet_tunnel_ipsec_preference
ACL/QoS	Shaping Rate (Kbps)	Device Specific	vpn_inet_qos_shaping-rate
	QoS Map	Global	qos_class_wired

Note: If a static IP address assignment is desired, the following IPv4 configuration can be used.

Table 15 Interface Ethernet Additional Settings for Static IP Address

Section	Parameter	Type	Variable/value
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device specific	vpn0_inet_int_ip_addr maskbits

VPN Cellular Interface Template Reference

This template is used to associate the interface to the VPN 0 template. Its purpose is to define interface settings for the cellular interface 0/1/0. This template allows for dynamic IP address assignment and defines an IPsec tunnel with color lte for control and transport connections. The Restrict setting on the tunnel is disabled to allow inter-color communication. It also defines a preference variable that will determine if the interface is selected for directing traffic to the tunnel as explained in [VPN Internet Interface Template Reference, page 39](#).

Feature Template type: VPN: VPN interface Cellular

Feature template name: RL_CELL_INT

Description: Default cellular interface 0/1/0

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 16 Interface Cellular Feature Template for LTE Transport on Expansion Module

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_cell1_int_shutdown
	Interface Name	Global	Cellular0/1/0
	Description	Global	Cellular interface
IPv4 Configuration	IPv4 Address	Radio button	Dynamic
Tunnel	Tunnel Interface	Global	On
	Color	Global	lte
	Restrict	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced Options>Encapsulation	IPsec	Global	On

Template Configuration

	Preference	Device Specific	vpn0_cell0_1_0_tunnel_ipsec_preference
ACL	Shaping Rate (Kbps)	Device Specific	vpn_cell1_qos_shaping-rate
	QoS Map	Global	qos_class_cellular

VPN Cellular Interface for Expansion Module Template Reference

This template is used to associate the expansion module cellular interface to the VPN 0 template. This template is needed for dual LTE since the same interface template cannot be attached twice to the same VPN. Parameters are similar to the ones described in VPN Cellular Interface Template Reference but it applies to a different cellular interface and associates the tunnel to a different color custom1 as shown in Figure 2 Validation Topology.

Feature Template type: VPN: VPN interface

Cellular Feature template name: RL_CELL_INT_EM

Description: Default cellular interface 0/3/0

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 17 Interface Cellular Feature Template for LTE Transport on Expansion Module

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	vpn0_cell3_int_shutdown
	Interface Name	Global	Cellular0/3/0
	Description	Global	Cellular interface EM
IPv4 Configuration	IPv4 Address	Radio button	Dynamic
Tunnel	Tunnel Interface	Global	On
	Color	Global	Custom1
	Restrict	Global	Off
	Allow Service>NTP	Global	On
Tunnel>Advanced Options>Encapsulation	IPsec	Global	On
	Preference	Device Specific	vpn0_cell0_3_0_tunnel_ipsec_preference
ACL	Shaping Rate (Kbps)	Device Specific	vpn_cell3_qos_shaping-rate
	QoS Map	Global	qos_class_cellular

Feature Templates for Service VPN

These templates configure the local service-side, or LAN-facing, network. This network will be used by the endpoints to access services in the data center or establish endpoint-to-endpoint connectivity. In the extended enterprise example deployment multiple service VPNs are created: shared services (VPN 1), IoT devices (VPN 10), and employee (VPN 11). One template is required for each. Services VPNs have to be created also on the data center side; for specific steps refer to the Cisco SD-WAN End-to-End Deployment Guide.

On the IR110, service-side interfaces are configured using SVIs. In the following example two SVI templates are created to be used on a single VPN (VPN 11) because you cannot use the identical feature template under a single VPN more than once. These templates can be reused in the different VPNs; for example, a single SVI template can be used for VPN 10 and VPN 11.

For the service-side a loopback0 interface template is created. The loopback interface is used for logging and SNMP it is referenced on corresponding feature templates. An OSPF template is also required to connect to the access switch in the remote location 3 example as shown in Validation Topology.

Follow the steps described in the Create a Feature Template section to create the required feature templates for the Extended Enterprise deployment.

Service VPN 1 Template Reference

This template creates service VPN 1 template.

Feature Template type: VPN: VPN

Feature template name: RL_VPN1

Description: Remote Location VPN 1 shared services

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 18 Service-Side VPN1 Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	VPN 1 shared services
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	10.22.2.4

Service VPN 10 Template Reference

This template creates service VPN 10 template.

Feature Template type: VPN: VPN

Feature template name: RL_VPN10

Description: Remote Location VPN 10 IoT devices

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 19 Service-Side VPN10 Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	10
	Name	Global	VPN 10 IoT devices
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	10.22.2.4

Service VPN 11 Template Reference

This template creates service VPN 11 template.

Feature Template type: VPN: VPN

Feature template name: RL_VPN11

Description: Remote Location VPN 11 Employee

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 20 Service-Side VPN11 Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	11
	Name	Global	VPN 11 Employee
	Enhance ECMP Keying	Global	On
DNS	Primary DNS Address	Global	10.22.2.4

Service VPN Interface SVI 1

This template is for the SVI, which will be reused on every service VPN. In this template VRRP is set as optional; if VRRP is not required do not include VRRP settings on the template, but if VRRP could potentially be used on any remote location the VRRP configuration can be added as optional so it can be used by sites with and without VRRP configuration.

One of the VRRP settings is called “Track Prefix List”; this list contains a prefix to a remote service route learned through OMP (default route if available). When the OMP prefix route disappears, the router gives up VRRP primary status. This is to guarantee VRRP failover in the case the primary router loses WAN connectivity. The prefix will be created in the policy section and referenced by the variable.

Most sites use DHCP relay to the data center, so an IP DHCP helper address is configured. If you want to use the router as the DHCP server, an optional DHCP template can be created as shown later.

Feature Template type: VPN: VPN Interface SVI

Feature template name: RL_SVI-SERVICE-VPN-1

Description: Remote Location service VPN SVI 1

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Template Configuration

Use the following settings, any value not mentioned in the list leave it as default.

Table 21 Service-Side SVI Feature Template

Section	Parameter	Type	Variable/value	Optional
Basic Configuration	Shutdown	Device Specific	vpn_service_svi_shutdown_1	NA
	VLAN Interface Name	Device Specific	vpn_svi_if_name_SVI_1	NA
	Description	Device Specific	vpn_svi_if_description_SVI_1	NA
IPv4 Configuration	IPv4 Address	Device Specific	vpn_if_svi_if_ipv4_prefix_SVI_1	NA
	DHCP Helper	Device Specific	vpn_svi_dhcp_helper_SVI_1	NA
ACL	Ingress ACL - IPv4*	Global	On	NA
	IPv4 Ingress Access* List	Global	Camera-To-Camera-Deny	NA
VRRP	Group ID	Device Specific	vpn_if_vrrp_grpid_1	Yes
	Priority	Device Specific	vpn_if_vrrp_priority_1	Yes
	Track Prefix List**	Device Specific	vpn_if_vrrp_track_prefix_list_1	Yes
	IP Address	Device Specific	vpn_if_vrrp_vrrp_ipaddress_1	Yes

*Shows where to apply an ACL created on Localized Policy

**Variable that will point to localized policy to track on a route for VRRP switchover when transport is unavailable.

Service VPN Interface SVI 2 (Optional)

In some instances, more than one SVI is required per VPN. For example, on the employee VPN one SVI is required for data and a separate VPN is required for voice. This template creates a template for an additional interface SVI. This template may be reused on more than one service VPN. In this template VRRP is set as optional; if VRRP is not required don't include VRRP settings on the template, but if VRRP could potentially be used on any remote location the VRRP configuration can be added as optional so it can be used by sites with and without VRRP configuration.

Feature Template type: VPN Interface SVI

Feature template name: RL_ SVI-SERVICE-VPN-2

Description: Remote Location service VPN SVI 2

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 22 Service-Side Secondary SVI Feature Template

Section	Parameter	Type	Variable/value	Optional
Basic Configuration	Shutdown	Device Specific	vpn_service_svi_shutdown_2	NA
	VLAN Interface Name	Device Specific	vpn_svi_if_name_SVI_2	NA
	Description	Device Specific	vpn_svi_if_description_SVI_2	NA
IPv4 Configuration	IPv4 Address	Device Specific	vpn_if_svi_if_ipv4_prefix_SVI_2	NA
	DHCP Helper	Device Specific	vpn_svi_dhcp_helper_SVI_2	NA
VRRP	Group ID	Device Specific	vpn_if_vrrp_grpid_2	Yes
	Priority	Device Specific	vpn_if_vrrp_priority_2	Yes
	Track Prefix List**	Device Specific	vpn_if_vrrp_track_prefix_list_2	Yes
	IP Address	Device Specific	vpn_if_vrrp_vrrp_ipaddress_2	Yes

**Variable that will point to localized policy to track on a route for VRRP switchover when transport is unavailable

Switchport Template

The switchport template configures the switchport settings on the router. The following tables contain three examples.

Example 1: Cisco IR1101 with four access ports to connect 4 endpoints directly to the switch.

Feature Template type: Switch Port

Feature template name: RL_SW_Ports_4_access

Description: Remote Location switchport 4 access ports

Device type: IR1101.

Use the following settings, any value not mentioned in the list leave it as default.

Table 23 Switchport Feature Template for Access Ports

Section	Parameter	Type	Variable/value
Basic Configuration	Slot	Global	0
	Sub-Slot	Global	0
	Module	Global	4 Port
Interface 1	Interface Name	Global	FastEthernet0/0/1
	Shutdown	Device Specific	switchport_1_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_1_if_access_vlan
Interface 2	Interface Name	Global	FastEthernet0/0/2
	Shutdown	Device Specific	switchport_2_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_2_if_access_vlan
Interface 3	Interface Name	Global	FastEthernet0/0/3
	Shutdown	Device Specific	switchport_3_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_3_if_access_vlan
Interface 4	Interface Name	Global	FastEthernet0/0/4
	Shutdown	Device Specific	switchport_4_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_4_if_access_vlan

Example 2: Cisco IR1101 with three access ports to connect three endpoints directly to the switch and a trunk to be connected to an access switch.

This template is shown below.

Feature Template type: Switch Port

Feature template name: RL_SW_Ports_4_Trunk

Description: Remote Location switchport 3 access ports and a trunk

Device type: IR1101.

Use the following settings, any value not mentioned in the list leave it as default.

Table 24 Switchport Feature Template with Trunk Port

Section	Parameter	Type	Variable/value
Basic Configuration	Slot	Global	0
	Sub-Slot	Global	0
	Module	Global	4 Port
Interface 1	Interface Name	Global	FastEthernet0/0/1
	Shutdown	Device Specific	switchport_1_if_shutdown
	Switch Port	Radio button	Trunk
	Allowed VLANS	Device Specific	switchport_1_if_trunk_allowed_vlans
Interface 2	Interface Name	Global	FastEthernet0/0/2
	Shutdown	Device Specific	switchport_2_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_2_if_access_vlan
Interface 3	Interface Name	Global	FastEthernet0/0/3
	Shutdown	Device Specific	switchport_3_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_3_if_access_vlan
Interface 4	Interface Name	Global	FastEthernet0/0/4
	Shutdown	Device Specific	switchport_4_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_4_if_access_vlan

Example 3: Cisco IR1101 with expansion module

Gigabit Ethernet ports in expansion module are configured as trunk ports to be connected to the access switch. Fast Ethernet ports are configured for access ports to connect to end devices directly.

Feature Template type: Switch Port

Feature template name: RL_SW_Ports_5_EM

Description: Remote Location switchport 4 access ports and a trunk on EM

Device type: IR1101

Use the following settings, any value not mentioned in the list leave it as default.

Table 25 Switchport Feature Template for Expansion Module

Section	Parameter	Type	Variable/value
Basic Configuration	Slot	Global	0
	Sub-Slot	Global	0
	Module	Global	8 Port
Interface 1	Interface Name	Global	FastEthernet0/0/1
	Shutdown	Device Specific	switchport_1_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_1_if_access_vlan
Interface 2	Interface Name	Global	FastEthernet0/0/2
	Shutdown	Device Specific	switchport_2_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_2_if_access_vlan
Interface 3	Interface Name	Global	FastEthernet0/0/3
	Shutdown	Device Specific	switchport_3_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_3_if_access_vlan
Interface 4	Interface Name	Global	FastEthernet0/0/4
	Shutdown	Device Specific	switchport_4_if_shutdown
	Switch Port	Radio button	Access
	VLAN ID	Device Specific	switchport_4_if_access_vlan
Interface 5	Interface Name	Global	GigabitEthernet0/0/5
	Shutdown	Device Specific	switchport_5_if_shutdown
	Switch Port	Radio button	Trunk
	Allowed VLANS	Device Specific	switchport_5_if_trunk_allowed_vlans

VPN Interface Ethernet Loopback0

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

Feature Template type: VPN Interface Ethernet

Feature template name: Loopback0

Description: Interface Loopback0

Device type: all IOS XE SD-WAN routers

Use the following settings, any value not mentioned in the list leave it as default.

Template Configuration

Table 26 Loopback Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	No
IPv4 Configuration	IPv4 Address	Radio button	Static
	DHCP Helper	Device Specific	lo0_int_ip_addr maskbits

OSPF Template

The OSPF template is used on sites that require OSPF connectivity to the access switch. The router interfaces are configured for OSPF network point to point. A route policy was configured as part of the localized policy as an example. It defines the OSPF routing behavior on the local site network and affect routing into or out of that specific site. A variable is created to reference the local route policy.

Feature Template type: OSPF

Feature template name: RL_OSPF

Description: Remote location OSPF

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 27 OSPF Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	Router ID	Device Specific	ospf_router_id
Redistribute	Protocol	Global	OMP
	Route Policy*	Device Specific	ospf_redistribute_route_policy
Area	Area Number	Device Specific	ospf_area_a_num
	Interface>Interface Name	Device Specific	ospf_name_iface
	Interface>Advanced Options>OSPF Network Type	Global	point-to-point
	Range>Address	Device Specific	ospf_area_range_address_0
Advanced	Reference Bandwidth (Mbps)	Global	1000000
	Originate	Global	On

*Variable pointing to localized policy to control OSPF path metric

DHCP Template (Optional)

A DHCP server pool template is created to add DHCP server functionality to the IR1101. Once created, the template is associated under an interface template.

Feature Template type: DHCP Template

Feature template name: RL_DHCP_template

Template Configuration

Description: Remote location DHCP server

Device type: IR1101. Optionally, include more IOS XE SD-WAN routers for remote locations if template is to be reused.

Use the following settings, any value not mentioned in the list leave it as default.

Table 28 DHCP Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	Address Pool	Device Specific	voice_dhcp_addr_pool maskbits
	Exclude Addresses	Device Specific	voice_dhcp_addr_exclude_range
Advanced	Domain Name	Global	cisco.local
	Default Gateway	Device Specific	dhcp_default_gateway
	DNS Servers	Global	10.22.2.4

Note: TFTP Server option can be also added to the template.

4G LTE Configuration

The Cisco IR1101 offers LTE support through the use of Pluggable Modules. Cisco LTE Pluggable Module support can be found on datasheet:

<https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html>.

The following table shows the relationship between Modems, SIMs, Interface, and Controller. For 4G-LTE-Advanced, the numbering on the Cisco IR1101 for slot 0, module 0, and port 0 is 0/1/0 for all commands on the base unit. On the Expansion Module, the numbering for slot 0, module 0, and port 0 is 0/3/0 for all commands.

Table 29 LTE Module Details

Router	Controller	SIM	Modem Sub Slot	PDN Interface
IR1101	0/1/0	0 1	0/1	Cellular 0/1/0 Cellular 0/1/1
IR1101 with Expansion Module	0/3/0	0 1	0/3	Cellular 0/3/0 Cellular 0/3/1

Cisco pluggable modules ship with a specific carrier provisioning file that can be found using the show cellular slot hardware command. Default profiles for the carrier are already populated and can be deployed readily. If using default profiles, such as AT&T, Sprint, and Verizon, there is no need to make any profile-related changes. In this case the router receives its IP address dynamically and is ready for PnP discovery. No feature templates are required to support default profiles.

Tip: Use the show cellular unit profile command to view the data profile. An asterisk(*) symbol is displayed against the data profile. A double asterisk(**) symbol is displayed against the attach profile.

Although profiles can be created, modified, and deleted, current versions of vManage don't allow you to change the profile attachment. For example, the P-LTE-US module comes with seven pre-configured profiles and default profile used for attach and data is 1. Even when you could create an additional eighth profile, vManage lacks the capability to select it to be used for attach and data. Therefore, if you need to use customized profiles (for example, Access Point

Template Configuration

Name (APN) in mobile networks), you need to overwrite the default profile. In the example, you would need to overwrite profile 1 with customized value. Default profiles are shown in the table. To customize profile, use feature template cellular profile.

Table 30 LTE Default Profiles

Modem	Profile Number
P-LTE-GB (Global)	Profile 1
P-LTE-VZ (Verizon)	Both Profile 1 and Profile 3
P-LTE-US (AT&T or other SPs)	Profile 1
P-LTEA-EA	Profile 1 and Profile 3 when using Verizon SIM Profile 1 when using AT&T SIM

Tip: When using the cellular interface for router onboarding using customized cellular profiles (nondefault APNs), device onboarding has to be done using the bootstrap method. More information can be found in the Device Onboarding section.

Warning: Dual SIM cards with different APNs is not possible when using customized profiles due to a current vManage limitation. Using vManage version 19.2 (and older) it is not possible to associate a specific APN per slot using feature templates.

Cellular Controller

When a cellular interface is added to a device template, a cellular controller template is required. We will create two feature templates, one for controller 0/1/0 and one for controller 0/3/0 used for the expansion module.

Feature Template type: Cellular controller

Feature template name: RL_CELL_CONTROLLER_0_1_0

Description: Remote location cellular controller 0/1/0

Device type: Device type: IR1101.

Use the following settings, any value not mentioned in the list leave it as default.

Table 31 Cellular Controller Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	Cellular ID	Global	0/1/0

Feature Template type: Cellular controller

Feature template name: RL_CELL_CONTROLLER_0_3_0

Description: Remote location cellular controller 0/3/0 Expansion module

Device type: IR1101.

Use the following settings, any value not mentioned in the list leave it as default.

Table 32 Cellular Controller Feature Template for Expansion Module

Section	Parameter	Type	Variable/value
Basic Configuration	Cellular ID	Global	0/3/0

Cellular Profile (Optional)

This configuration is only needed if using a customized APN. Be sure to understand limitations mentioned in Caveats and Limitations before using this template.

Feature Template type: Cellular profile

Feature template name: RL_CELL_PROFILE_CUST

Description: Remote location cellular profile for customized APN

Device type: IR1101.

Use the following settings, any value not mentioned in the list leave it as default.

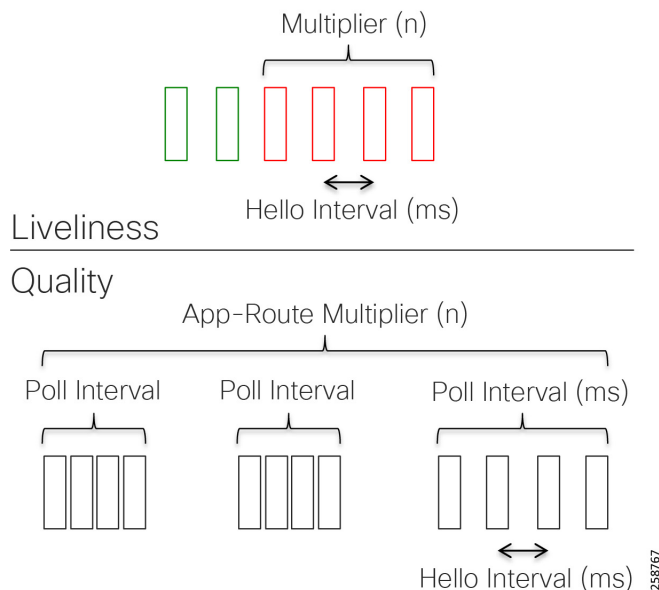
Table 33 Cellular Profile Feature Template

Section	Parameter	Type	Variable/value
Basic Configuration	Profile ID	Device Specific	cellular_profile_profile_id
	Access Point Name	Device Specific	cellular_profile_apn

A Note on BFD Timers and Application-Aware Routing

The BFD feature template allows for the configuration of two timers (hello interval and poll interval) that are used for application-aware routing to determine the availability of the tunnel.

- Each IOS XE SD-WAN router sends BFD hello packets using the hello interval for path quality and availability detection, and those packets are echoed back by the remote site. The hello interval and multiplier determine how many BFD packets need to be lost to declare the IPSec tunnel down. The hello interval and multiplier can be customized per color and applied per device. The default value for the hello interval is 1 sec, and in general is not recommended to edit this value. If desired, the multiplier value can be decremented to decrease the time that takes to detect a failure in the tunnel.
- The number of hello intervals that fit inside the poll interval determines the number of BFD packets considered for establishing the poll interval average path quality. The app-route multiplier determines number of poll intervals for establishing overall average path quality. The poll interval and multiplier are configured at the device level.

Figure 29 Understanding BFD Timers

To determine the SLA classification of a tunnel, application-aware routing uses the loss, latency, and jitter information from the latest poll intervals. The number of poll intervals used is determined by a multiplier. These default values have to be chosen to provide damping of sorts, as a way to prevent frequent reclassification (flapping) of the tunnel. The multiplier is user-configurable per IOS XE SD-WAN router; that is, it applies to all tunnels originating on a router. If there is a need to react quickly to changes in tunnel characteristics, you can reduce the multiplier all the way down to 1. With a multiplier of 1, only the latest poll interval loss and latency values are used to determine whether this tunnel can satisfy one or more SLA criteria. Regardless of how quickly a tunnel is reclassified, the loss, latency, and jitter information are measured and calculated continuously.

Warning: Changing the BFD timers is not recommended because it changes the scalability of tunnels that the device can provide. Timers should stay conservative if possible and if changed from the defaults, should be tested thoroughly in the customer environment.

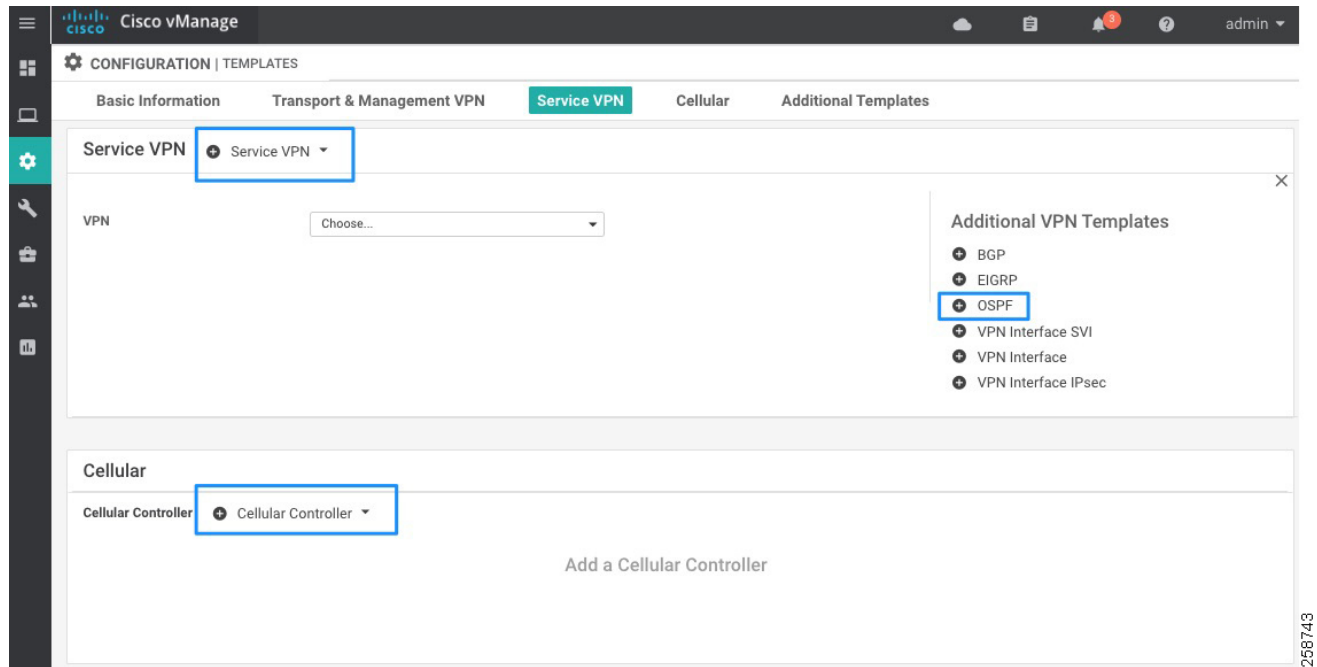
Device Templates

A device template contains a set of configurations to be applied to a device type. In this section we will explain how to create a device template, followed by some examples used during validation.

1. From the vManage GUI, go to **Configuration > Templates** and click the **Device** tab.
2. Click **Create Template** and choose **From Feature Template** from the options.
3. From the Device Model drop-down list choose the type of device for which you are creating the template. vManage displays all the feature templates for that device type. The required feature templates are indicated with an asterisk and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. Enter information in the Template Name and Description fields.
5. To view the factory-default configuration for a feature template, select the desired feature template and click **View Template** text. Click the **Cancel** button to return to the Configuration Template screen. The drop-down list on each template option will show available templates for specific feature, and if templates were created previously before they will show in the list.
6. Select the desired feature template for each setting.

7. (Optional) A (+) sign indicates it is possible to add elements to the device template. The figure below illustrates options to add a service VPN, a Cellular Controller, and Additional VPN templates such as OSPF.

Figure 30 Adding Optional Elements to Device Template



8. Click the **Create** button to save the template. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

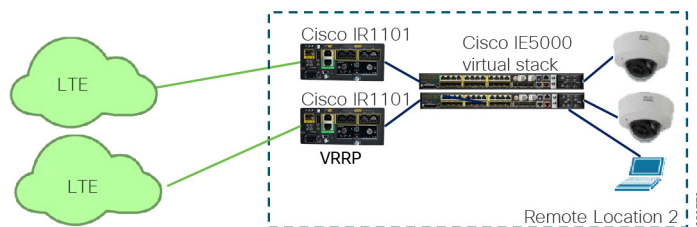
Device Templates for Extended Enterprise Remote Sites

In this guide we are creating four different device templates that match different device configurations. Note that those device templates are provided as guidance but they should be modified to match specific requirements.

IOS XE SD-WAN router with LTE Transport

Remote Location 2 on Figure 2 Validation Topology shows two routers with one cellular transport each. On the service side they are connected to a switch stack using trunk ports, and other ports are access ports to connect end devices. Note that no special device template considerations are done to support VRRP on the site because VRRP settings are added as optional parameters in the common service VPN feature templates.

Figure 31 Remote Location 2



To create a profile that matches this deployment follow steps in the Device Templates section using the following values.

Name: IR1101_CELL_with_TRUNK

Description: Template for single router with cellular connection and switchport on service side

Device Type: IR1101

Table 34 Device Template IR1101_CELL_with_TRUNK

Section	Template sub-type	Template name	Note
Basic Information	System	System_Template	Blueprint on Appendix B
	Logging	Logging_Template	Blueprint on Appendix B
	NTP	NTP_Template	Blueprint on Appendix B
	AAA		Blueprint on Appendix B
	AAA-Cisco	AAA_Template	Blueprint on Appendix B
	BFD	BFD_Template	Blueprint on Appendix B
	OMP	OMP_Template	Blueprint on Appendix B
	Security	Security_Template	Blueprint on Appendix B
Transport & Management VPN (VPN0)	VPN0	RL_VPN0	
	VPN interface Cellular	RL_CELL_INT	
Service VPN (VPN1)	VPN	RL_VPN1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
Service VPN (VPN10)	VPN	RL_VPN10	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
Service VPN (VPN11)	VPN	RL_VPN11	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-2	Optional if a second interface in same VPN is required
Cellular	Cellular Controller	RL_CELL_CONTROLLER_0_1_0	
Additional Templates	Banner	Banner_Template	Blueprint on Appendix B

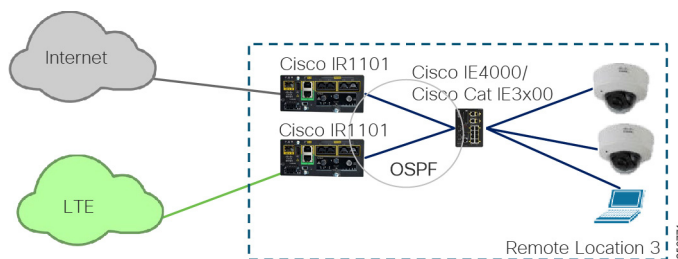
Template Configuration

	Policy	Remote_Location_Policy	Local policy
	SNMP	SNMP_Template	Blueprint on Appendix B
Switch Portxxx	Switch Port	RL_SW_Ports_4_Trunk	

IOS XE SD-WAN router with LTE Transport and OSPF

Remote location 3 on Figure 2 Validation Topology shows one router with an LTE transport and one router with an Internet transport. This section shows device template parameters for a router with LTE transport. This location has the OSPF configuration on the service side and is connected to a switch using a trunk port.

Figure 32 Remote Location 3



To create a profile that suits this deployment, follow steps in the Device Templates section using the following values.

Name: IR1101_CELL_OSPF_with_TRUNK

Description: Template for single router with cellular connection, OSPF and switchport on service side

Device Type: IR1101

Table 35 Device Template IR1101_CELL_OSPF_with_TRUNK

Section	Template sub-type	Template name	Note
Basic Information	System	System_Template	Blueprint on Appendix B
	Logging	Logging_Template	Blueprint on Appendix B
	NTP	NTP_Template	Blueprint on Appendix B
	AAA		Blueprint on Appendix B
	AAA-Cisco	AAA_Template	Blueprint on Appendix B
	BFD	BFD_Template	Blueprint on Appendix B
	OMP	OMP_Template	Blueprint on Appendix B
	Security	Security_Template	Blueprint on Appendix B
Transport & Management VPN (VPN0)	VPN0	RL_VPN0	
	VPN interface Cellular	RL_CELL_INT	
Service VPN (VPN1)	VPN	RL_VPN1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	VPN Interface Ethernet	Loopback0	
	OSPF	RL_OSPF	

Template Configuration

Service VPN (VPN10)	VPN	RL_VPN10	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	OSPF	RL_OSPF	
Service VPN (VPN11)	VPN	RL_VPN11	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	OSPF	RL_OSPF	
Cellular	Cellular Controller	RL_CELL_CONTROLLER_0_1_0	
Additional Templates	Banner	Banner_Template	Blueprint on Appendix B
	Policy	Remote_Location_Policy	Local policy
	SNMP	SNMP_Template	Blueprint on Appendix B
Switch Portxxx	Switch Port	RL_SW_Ports_4_Trunk	

IOS XE SD-WAN router with Internet Transport and OSPF

Remote location 3 on Figure 2 Validation Topology shows one router with an LTE transport and one router with an Internet transport. This section shows device template parameters for router with Internet transport. This location has the OSPF configuration on the service side and is connected to a switch using a trunk port. To create a profile that suits this deployment, follow steps in the Device Templates section using the following values.

Name: IR1101_INET_OSPF_with_TRUNK

Description: Template for single router with Internet connection, OSPF and switchport on service side

Device Type: IR1101

Table 36 Table 35 Device Template IR1101_INET_OSPF_with_TRUNK

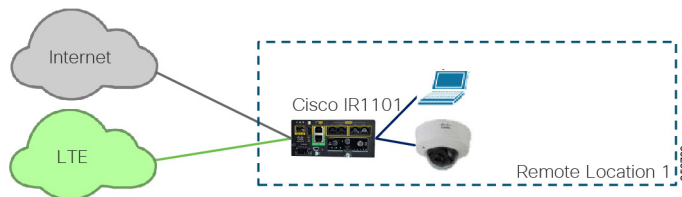
Section	Template sub-type	Template name	Note
Basic Information	System	System_Template	Blueprint on Appendix B
	Logging	Logging_Template	Blueprint on Appendix B
	NTP	NTP_Template	Blueprint on Appendix B
	AAA		Blueprint on Appendix B
	AAA-Cisco	AAA_Template	Blueprint on Appendix B
	BFD	BFD_Template	Blueprint on Appendix B
	OMP	OMP_Template	Blueprint on Appendix B
	Security	Security_Template	Blueprint on Appendix B
Transport & Management VPN (VPN0)	VPN0	RL_VPN0	
	VPN Interface	RL_INET_INT	
Service VPN (VPN1)	VPN	RL_VPN1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	VPN Interface Ethernet	Loopback0	

	OSPF	RL_OSPF	
Service VPN (VPN10)	VPN	RL_VPN10	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	OSPF	RL_OSPF	
Service VPN (VPN11)	VPN	RL_VPN11	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	OSPF	RL_OSPF	
Additional Templates	Banner	Banner_Template	Blueprint on Appendix B
	Policy	Remote_Location_Policy	Local policy
	SNMP	SNMP_Template	Blueprint on Appendix B
Switch Portxxx	Switch Port	RL_SW_Ports_4_Trunk	

IOS XE SD-WAN router with Cellular and Internet Transport

Remote Location 1 on Figure 2 Validation Topology shows a single router with one wired transport and one cellular transport.

Figure 33 Remote Location 1



On the service side, all switch ports are access ports. To create a profile that suits this deployment follow steps in the Device Templates section using the following values.

Name: IR1101_INET_and_CELL

Description: Template for single router with Internet and cellular transport

Device Type: IR1101

Table 37 Table 36 Device Template IR1101_INET_and_CELL

Section	Template sub-type	Template name	Note
Basic Information	System	System_Template	Blueprint on Appendix B
	Logging	Logging_Template	Blueprint on Appendix B
	NTP	NTP_Template	Blueprint on Appendix B
	AAA		Blueprint on Appendix B
	AAA-Cisco	AAA_Template	Blueprint on Appendix B
	BFD	BFD_Template	Blueprint on Appendix B
	OMP	OMP_Template	Blueprint on Appendix B

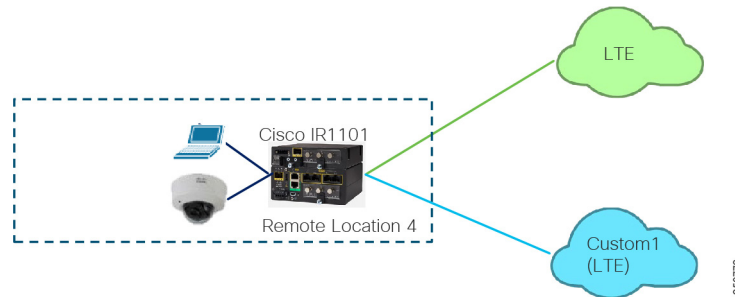
Template Configuration

	Security	Security_Template	Blueprint on Appendix B
Transport & Management VPN (VPN0)	VPN0	RL_VPN0	
	VPN Interface	RL_INET_INT	
	VPN interface Cellular	RL_CELL_INT	
Service VPN (VPN1)	VPN	RL_VPN1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	DHCP	RL_DHCP_template	Optional if DHCP server functionality is required
	VPN Interface Ethernet	Loopback0	
Service VPN (VPN10)	VPN	RL_VPN10	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	DHCP	RL_DHCP_template	Optional if DHCP server functionality is required
Service VPN (VPN11)	VPN	RL_VPN11	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-2	Optional if a second interface in same VPN is required
Cellular	Cellular Controller	RL_CELL_CONTROLLER_0_1_0	
	Cellular profile	RL_CELL_PROFILE_CUST	Optional if non default cellular profile required**
Additional Templates	Banner	Banner_Template	Blueprint on Appendix B
	Policy	Remote_Location_Policy	Local policy
	SNMP	SNMP_Template	Blueprint on Appendix B
Switch Portxxx	Switch Port	RL_SW_Ports_4_access	

IOS XE SD-WAN router with Dual LTE

Remote Location 4 on Figure 2 Validation Topology shows a single router with an expansion module and two cellular interfaces.

Figure 34 Remote Location 4



To create a profile that suits this deployment follow steps in the Device Templates section using the following values:

Name: IR1101_DUAL_CELL_EM

Description: Template for single router with expansion module and two cellular transports

Device Type: IR1101

Table 38 Table 37 Device Template IR1101_DUAL_CELL_EM

Section	Template sub-type	Template name	Note
Basic Information	System	System_Template	Blueprint on Appendix B
	Logging	Logging_Template	Blueprint on Appendix B
	NTP	NTP_Template	Blueprint on Appendix B
	AAA		Blueprint on Appendix B
	AAA-Cisco	AAA_Template	Blueprint on Appendix B
	BFD	BFD_Template	Blueprint on Appendix B
	OMP	OMP_Template	Blueprint on Appendix B
	Security	Security_Template	Blueprint on Appendix B
	Transport & Management VPN (VPN0)	VPN0	RL_VPN0
VPN interface Cellular		RL_CELL_INT	
VPN interface Cellular		RL_CELL_INT_EM	
Service VPN (VPN1)	VPN	RL_VPN1	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
	VPN Interface Ethernet	Loopback0	
Service VPN (VPN10)	VPN	RL_VPN10	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	
Service VPN (VPN11)	VPN	RL_VPN11	
	VPN Interface SVI	RL_SVI-SERVICE-VPN-1	

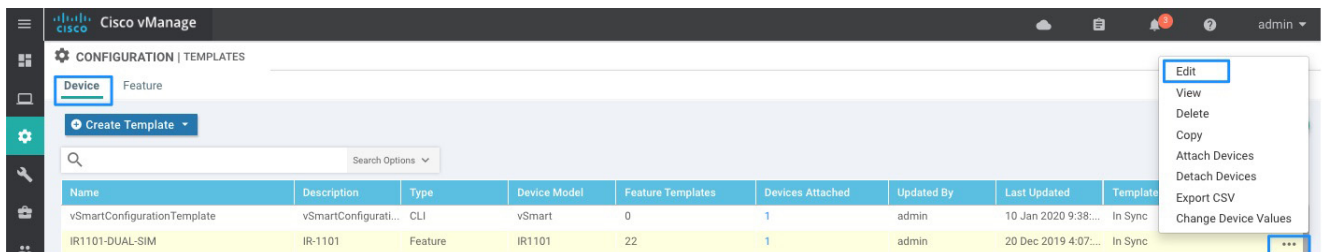
Template Configuration

	VPN Interface SVI	RL_ SVI-SERVICE-VPN-2	Optional if a second interface in same VPN is required
Cellular	Cellular Controller	RL_CELL_CONTROLLER_0_1_0	
	Cellular Controller	RL_CELL_CONTROLLER_0_3_0	
Additional Templates	Banner	Banner_Template	Blueprint on Appendix B
	Policy	Remote_Location_Policy	Local policy
	SNMP	SNMP_Template	Blueprint on Appendix B
Switch Portxxx	Switch Port	RL_SW_Ports_5_EM	

Modifying Templates

1. To modify device templates to add localized policy, go to **Configuration>Templates**.
2. Select the **Device** tab.
3. The page will show device templates that have already been configured. Click on the ellipses (...) at the end of the row for a specific device template. Choose **Edit** from the menu.

Figure 35 Edit a Template



4. Modify any settings, if desired.
5. Click **Update**. If the template is already attached to devices the wizard will continue to a configuration templates screen to show devices that will be updated. Click **Next** to preview changes and then click **Configure Devices** when you are ready to push configuration. Confirm that you want to proceed. Policy elements are now ready to be used on feature templates.

Device Onboarding

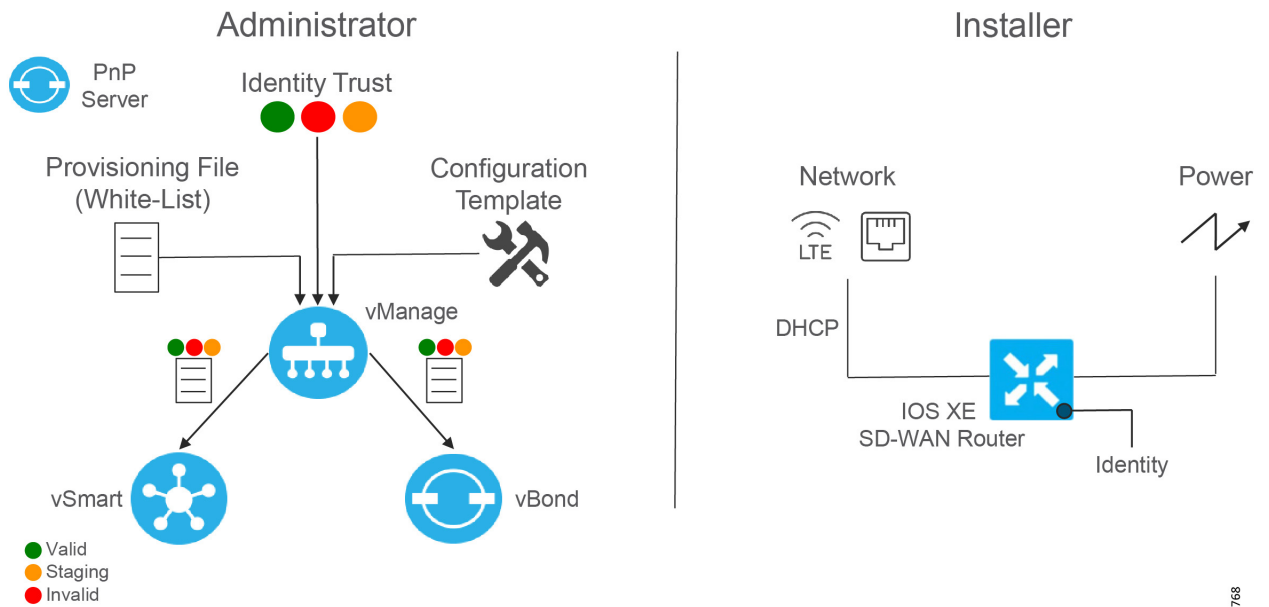
Device onboarding is a process initiated by the network administrator by completing the following tasks:

- Load device(s) on Plug and Play Connect if not added during procurement process
- Load device(s) on vManage, push them to vSmart and vBond, and declare the device(s) as valid or staging device(s).
- Attach the device to a template

After the steps are completed, an installer on the remote site could connect the device to the network, after which the device will reach vBond, establish DTLS connectivity with controllers, and download the configuration defined on the template.

The following graph illustrates the device onboarding activities. Detailed steps are provided in this chapter.

Figure 28 Device Onboarding



Cisco Plug and Play Connect

In order for the WAN Edge devices to join and be active in the overlay, a valid, authorized serial number file has to be uploaded to vManage. This authorized serial number file lists the serial and chassis numbers for all WAN Edge routers allowed in the network. vManage will send this file to the controllers, and only devices that match serial numbers on this list will be validated and authenticated successfully by the controllers. The authorized serial number for IOS XE SD-WAN routers is obtained from Plug and Play (PnP) Connect portal. PnP Connect portal is also used to automate onboarding of network devices and apply configuration settings without manual intervention. This guide will provide required steps to

add a device on PnP Connect using a smart account and associate it to a vBond profile. Refer to the following link for deeper understanding on PnP connect
<https://www.cisco.com/c/en/us/products/collateral/software/smart-accounts/guide-c07-744931.html#4DeploymentOptions>.

Prerequisites

- Smart account and virtual account
- If the deployment is on premises, vBond has to be defined in PnP connect. Refer to https://www.cisco.com/c/dam/en_us/services/downloads/SD-WAN_pnp_support_guide.pdf for specific steps. Note that for cloud deployments, controller information is reflected automatically on the PnP portal.

Adding a device on PnP Connect

A device can be added to PnP Connect automatically if the smart account and virtual account are added to the order on Cisco Commerce Workspace.

If the device is not added through the procurement process, follow these steps:

1. Get serial number and certificate serial number from the device using the *show crypto pki certificates CISCO_IDEVID_SUDI* command:

```
Router#show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
Status: Available
Certificate Serial Number (hex): XXXXXXXXX
Certificate Usage: General Purpose
Issuer:
cn=ACT2 SUDI CA
o=Cisco
Subject:
Name: IR1101-K9
Serial Number: PID:IR1101-K9 SN:XXXXXXXXXXXX
cn=IR1101-K9
ou=ACT-2 Lite SUDI
o=Cisco
serialNumber=PID:IR1101-K9 SN: XXXXXXXXXXXX
Validity Date:
start date: 07:49:10 UTC Mar 9 2019
end date: 20:25:41 UTC May 14 2029
Associated Trustpoints: CISCO_IDEVID_SUDI
```

2. Navigate to <https://software.cisco.com>.
3. Under the Network Plug and Play section, click the **Plug and Play Connect** link.
4. Ensure the correct virtual account is chosen in the top right corner.
5. Click **Add Devices** button.
6. Select **Enter Device Info Manually** radio button. Alternatively, you could upload a Comma Separated Values (CSV) file.
7. Click **Next**.
8. Click **Identify Device** button.
9. Fill out the serial number obtained in Step 1, base PID (IR1101-K9), and the selected vBond controller profile.

Figure 29 Connect - Identify Device

Identify Device ✕

* Serial Number

* Base PID

Controller Profile

Description

Cancel
Save

258746

10. Click **Save**. On the wizard screen, click **Next**.
11. On Review & Submit, click **Submit**.
12. Click **Done**.
13. After the router is added, a list of devices is displayed. Select the recently added device and then click **Edit Selected**.
14. Click the space under the Certificate Serial Number column for the device and enter the information from Step 1.

Figure 30 Add Certificate Serial Number

Selected Devices
Product Group : Router

Serial Number	Base PID	Certificate Serial Number	Controller	Description	Actions
AAAAAAAAAAAA	IR1101-K9	ABCDER	VBOND-EE-TEST-PROFILE	--	✎ 🗑

🔍 double click to edit certificate serial number

Showing 1 Record

Cancel
Submit

258746

15. Click **Submit**.
16. The device will show with yellow status showing Pending (Redirection). If the device is onboarded using the PnP automatic onboarding process, this state will change to Redirect Successful; otherwise it will stay in current state.

Load authorized WAN edge serial numbers to vManage

There are two methods to upload the authorized devices to vManage.

Method 1: Sync to the Smart Account

1. In the vManage GUI, go to **Configuration > Devices**.
2. Ensure that **WAN Edge List tab** is selected.
3. Click **Sync Smart Account** and a window pops up which prompts you for your Username and Password.
4. Enter your username and password for the Cisco website. The check box which validates the uploaded list is checked by default.
5. Click **Sync**. Wait for status to show success.

Tip: You must re-sync vManage with the Smart Account/Virtual Account for any new devices added to the PNP portal.

Method 2: Upload File Manually

1. Navigate to <https://software.cisco.com>.
2. Under the Network Plug and Play section, click the **Plug and Play Connect** link.
3. Ensure the correct virtual account is chosen in the top right corner.
4. Click **Controller Profiles** text.
5. Next to the correct controller profile, click **Provisioning File** text.
6. In the pop-up window, select the controller versions from the drop-down list. Choose **18.3 and newer**. Click **Download** button and save the file to your computer.
7. In the vManage GUI, go to **Configuration > Devices** on the left panel.
8. Ensure that WAN Edge List tab is selected.
9. Click the **Upload WAN Edge List** button. A pop-up window appears. Choose **file**.
10. Check the check box in order to validate the list and send it to the controllers. Click **Upload**. If you do not select **Validate**, then all the devices will show up as invalid, and you will need to individually change them to valid if you want to bring them up on the network and participate in the overlay.
11. Select **OK** in the confirmation box that appears.
12. A pop-up window appears to inform you that the list uploaded successfully and informs you of the number of routers that were uploaded successfully. Select **OK**. A page will indicate that the list has been successfully pushed out to the vBond and vSmart controllers.

Stage Devices (Optional)

Optionally, it is possible to put the devices in a staging state. In this state the control plane could be initialized but they will not join the overlay and forward traffic until they are put into a valid state. The WAN Edge routers will become OMP peers with the vSmart controllers, but no OMP routes will be sent, nor will any local routes be redistributed into OMP.

1. From the vManage GUI, go to **Configuration > Certificates**. Find the appropriate device by matching the chassis serial number.
2. To the right of the targeted router, select **Staging**. A pop-up window will ask for confirmation. Select **OK**.

3. Repeat for any number of routers.
4. Click the **Send to Controllers** button in the upper left portion of the screen when finished.

Attach device to template

Attaching the device to a device template will associate the configuration to the device. During this process, all variables on the templates need to be assigned to a value.

1. Go to **Configuration > Templates**.
2. In the **Device** tab, identify the template you want to use.
3. Click the more actions (...) icon to the right of the row and then click **Attach Devices**. The **Attach Devices** dialog box opens.
4. In the **Available Devices** column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column on the right.
6. Click **Attach**.
7. Before the full configurations can be built and pushed out, you need to first define all variables associated with the feature templates attached to the device template. There are two ways to do this: either by entering the values of the variables manually within the GUI, or by uploading a CSV file with a list of the variables and their values. Detailed steps for each option will be provided at the end of this section. The variables used for each device in this deployment are documented in [Appendix D Device Template Values](#).
8. Click the **Next** button. The next screen will indicate that the configure action will be applied to the devices being attached to the template.
9. (Optional) Select a device on the left side to show the configuration that will be pushed to the IOS XE SD-WAN router on the **Config Preview** tab.
10. (Optional) Select the **Config Diff** tab at the top of the screen to see the difference in the current local configuration versus the new configuration which is about to be pushed.
11. (Optional) You may select the **Configure Device Rollback Timer** text in the lower left corner to view or change the rollback timer. Rollback timer is a protection mechanism; if the router is unreachable after a configuration change it rolls back to the previous configuration. You can configure the timer to any value between 6 and 15 minutes. It is not recommended to disable it. Click **Save** or **Cancel** to go back to main window.
12. Select **Configure Devices**. If configuring more than one device, a pop-up window warns of committing changes to multiple devices. Check the check box to Confirm configuration changes on the devices. Select **OK**. The configuration then gets pushed out to the devices. When complete, vManage should show the **Done-Scheduled** status, indicating the device is offline but template is scheduled to be pushed when connectivity is established.
13. (Optional) To view devices attached to a device template, go to **Configuration > Templates**. From the **Device** tab, identify the template and click the **Device Attached** column that indicates how many devices are attached. The pop out window will show attached devices.

Add Variables with a File

1. Download the .csv file by clicking the download arrow symbol in the upper right corner.
2. Fill out variables on the file and click **Save**.
3. Click the upload arrow in the top right corner of the screen to upload the .csv file.

4. A window will pop up. Choose the file and click the **Upload** button. The message “File Uploaded Successfully” should appear in green at the top of the screen.
5. (Optional) Scroll to the right and view or modify the values of the variables that have been used for input.

Tip: Adding variables with a file is the preferred method when you have used a feature template multiple times. In this scenario same variable name will appear more than once in the screen without context. On the other hand, The CSV file provides variable parent context in addition to variable name. As an example, when using same SVI template for VPN10 and VPN11, CSV file header will show VPN context in the header like this:

```
/11/vpn_if_svi_if_name_SVI_2/interface/if-name
```

Add Variables Manually

To add values manually, enter the values of the variables in the text boxes. There may also be variables with check boxes for enabling them; if the check box is checked, the variable will be included. If you leave a non-optional text field empty, the text box will be highlighted red when you try to move to the next page. Optionally, you can click the more actions icon (...) at the end of the row and fill out the variables on the pop-out window. Click the **Update** button when finished.

Tip: When you are finished filling out the variables and before moving further, download the .csv file by clicking the download arrow symbol in the upper right corner. The .csv file will be populated with the values you have filled in so far. If you deploy the configuration, and for any reason there is an error in one of the input variables and the configuration fails to deploy, when you come back to this page, all the values you entered earlier will not be available and you will need to enter them again. If you downloaded the populated .csv file, just upload it by clicking the up arrow. Then you can click **Edit Device Template** to the right of the desired device, and all of your latest values will be populated in the text boxes. Modify any input values and try to deploy again.

Modify Variables

To modify variables even after the device has been provisioned, follow the following steps.

1. Go to **Configuration > Devices**.
2. Identify the device you want to update and click more actions (...) at the end of the row.
3. Choose **Change Device Values** from the list.
4. Use the manual or file method to update variables.

Generate Bootstrap Configuration File

This step is only needed if onboarding devices using the bootstrap method described in the next section.

1. On vManage, navigate to **Configuration > Devices**.
2. Click the More Actions icon (...) to the right of the row for the applicable device and choose **Generate Bootstrap Configuration**.
3. In the dialog box that opens, make sure that the **Cloud-init** radio button is selected, and then click **OK**.
4. The system generates a file and displays its contents in a pop-up window.
5. Click **Download**.
6. Rename the file to **ciscosdwan.cfg** (case sensitive).
7. Copy the ciscosdwan.cfg file to a bootable USB drive or to the bootflash of the device. The file must be named exactly as shown or the device will not read it.

Bring up Devices

Bringing up a router to connect to SD-WAN network can be done by three methods:

- PnP for zero touch deployment.
- Bootstrap, for devices that cannot get Internet connectivity without additional configuration, such as devices connected to transport with a static IP configuration or non-default cellular profiles.
- CLI, adding manual configuration via the console.

This guide focuses on PnP and bootstrap methods since they don't require network administration expertise to bring up the device. These methods are explained below.

Plug and Play

When a device meets the requirements stated below, it boots and reaches PnP Connect portal to get the vBond IP address. The router establishes a secure tunnel to vBond, and after authentication vBond sends the vManage IP address to the Cisco IOS XE router. The router contacts vManage over a secure tunnel and vManage sends the full configuration to the Cisco IOS XE router. Finally, the router contacts vSmart over a secure tunnel; after authentication, it will join the SD-WAN fabric. This process does not require any manual intervention or configuration.

Prerequisites

- IR1101 has IOS XE SD-WAN Release 16.12.1b or newer. For image installation refer to Appendix A - Upgrade Cisco IR1101 with IOS XE SD-WAN Image.
- Device is connected to a network.
- Device can get a DHCP IP address and reach PnP portal and vBond.
- Device does not have any configuration.
- Device is imported to vManage as valid or staging.
- Device is assigned to a device template.

Bootstrap

If the device meets prerequisites mentioned below, when the device boots, it reads the configuration file from the USB drive from or the bootflash and uses the configuration information to join the network. The configuration will enable network connectivity as well as provide system parameters and vBond address. Once the device is authenticated by vBond, it gets vManage information. The router establishes communication with vManage and joins the overlay network.

Tip: it is recommended to copy the configuration file on bootflash before performing IOS XE SD-WAN installation. After IOS XE SD-WAN installation is completed the default one-time user admin is deleted, and the default password can be used once and then must be changed. If the initial configuration session times out or if the session is interrupted or terminated before the password is changed and saved, subsequent login attempts fail. To avoid this situation when using bootstrap configuration, copy the configuration file before upgrading; the bootstrap configuration will contain configured user information that can be used for subsequent login.

- If using enterprise root certificate, issue the following command to install the certificates after the switch is configured:

```
Router# request platform software sdwan root-cert-chain install bootflash: certificate
```

Prerequisites

- IR1101 has IOS XE SD-WAN Release 16.12.1b or newer. For image installation refer to Appendix A - Upgrade Cisco IR1101 with IOS XE SD-WAN Image.
- Device is connected to a network.
- SD-WAN controllers should be reachable on the network.
- Bootstrap configuration is loaded on bootflash of the device or on a bootable USB drive plugged to the device.
- Device is imported to vManage as valid or staging.
- Device is assigned to a device template.
- If using your enterprise root certificate to authenticate the router, copy the certificate on bootflash.

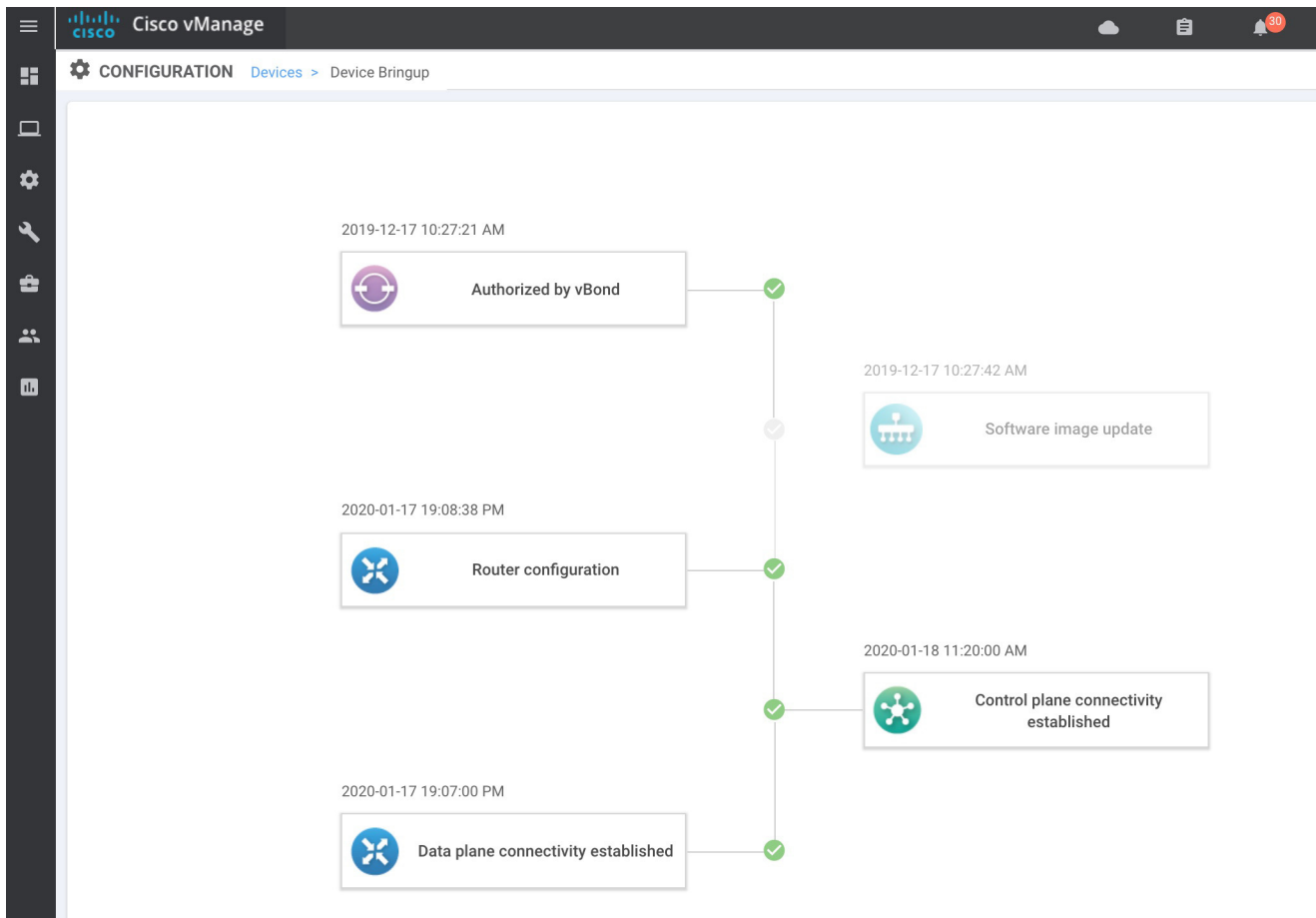
Activate Devices in Staging State

If IOS XE SD-WAN routers are in staging mode, the status won't be seen from the vManage dashboard and they won't be able to establish data plane connectivity. To move those devices into a valid state, go to **Configuration > Certificates**. If device is in Staging mode, switch to **Active** and click **Send to Controllers** at the top of the page.

Device Onboarding Troubleshooting

To check device onboarding status, go to **Configuration > Devices**. Click on more actions (...) at the end of the row and choose **Device Bring up** to see status of onboarding process. All stages should be passed with a green check mark. The only exception is the Software Image Update that may be grayed out. If there are any issues or the device is not found on the device list use this troubleshooting section.

Figure 31 Device Bring up



Device is Not Authorized by vBond

- Check the device is in the staging or valid state. Go to **Configuration > Certificates** and confirm the status of the device. If device is not in the list, make sure is added on PnP Connect portal and imported into vManage. If device is in invalid state, change to **Valid** or **Staging** and then click **Send to Controllers** at the top of the page.
- Make sure the device is associated to a template on vManage. Go to **Configuration > Devices**. Click more actions (...) at the end of the row and choose **Template Log**. If logs show “No logs available”, associate to a template by following the **Attach Device to Template** section.
- If using PnP make sure the device got its IP configuration using DHCP, and check that the device is able to reach `devicehelper.cisco.com`. If the device is not getting an IP address, check physical connectivity and contact the service provider. If using cellular interfaces refer to **Troubleshooting LTE Connectivity**.
- The following is expected in the logs when doing PnP:

```
*Jan 17 20:12:18.433: %PNP-6-HTTP_CONNECTING: PnP Discovery trying to connect to PnP server
https://devicehelper.cisco.com.:443/pnp/HELLO
*Jan 17 20:12:18.658: %PNP-6-HTTP_CONNECTED: PnP Discovery connected to PnP server
https://devicehelper.cisco.com.:443/pnp/HELLO
.....
*Jan 17 20:12:49.322: SDWAN INFO: SDWAN pnp send vbond info: Org name iot-ee Host x.x.x.x port 12346
intf Cellular0/1/0
*Jan 17 20:12:50.313: %PNP-6-PNP_REDIRECTION_DONE: PnP Redirection Done successfully
```

- Successful communication with the PnP server is shown on PnP Connect portal on the Devices tab as shown in the image below. The device Status column will show Redirect Successful instead of Pending Redirection. Click the Show Log link for more information, it will show timestamps, if the device contacted the server, and authentication results.

Figure 32 PnP Connect Device Redirected

Cisco Software Central > Plug and Play Connect InternalTestDemoAccount11.cisco.com ConnectedAutomation

Plug and Play Connect Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions

<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input type="checkbox"/>	<input type="text" value=""/>	<input type="text" value=""/>	Any	Any	Select Range	Any	Clear Filters
<input type="checkbox"/>		IR1101-K9	Router	VBOND-EE-TEST-PROFI...	2020-Jan-17, 20:30:29	Redirect Successful	Show Log...
<input type="checkbox"/>	BBBBBBCCCC	IR1101-K9	Router	VBOND-EE-TEST-PROFI...	2020-Jan-16, 22:01:44	Pending (Redirection)	Show Log...

259748

- If device is onboarded using bootstrap, PnP Connect portal does not show any updates. Instead check if the configuration was loaded to the device with the **show sdwan running-config** command. If the configuration is not present, check that the configuration file **ciscosdwan.cfg** is present on bootflash or the bootable USB as described in the Bootstrap section.
- If the device is successfully redirected in the case of PnP or has the right configuration in the case of bootstrap, confirm the device is able to reach vBond. If using a domain name instead of IP address, check that the DNS server IP address is configured on the VPN0 feature template attached to the device and reachable from the router.
- The command **show sdwan control connections** shows control connections, and if the device is not authenticated by vBond, use the **show sdwan control connection-history** command to see attempts to connect with code for failure. Common errors are:
 - DCONFAL: DTLS Connection Failure. Check connectivity, firewall or NAT configuration
 - CRTREJSER/BIDNTVRFD: Serial Number(s) Not Present.
 - The serial number is not present on the controllers for a given device, you will see that control connections fail.
 - VSCRTREV/CRTVERFL: Certificate Revoked/Invalidated
 - In cases when the certificate is revoked on controllers or WAN Edge serial number is invalidated.
 - For more information on control connections troubleshooting refer to

<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html>

- The command **show sdwan control statistics** shows if control packets are being transmitted and received. If packets are sent but not received check connectivity.

Router Configuration Failure

vManage was not able to push configuration to the device. Go to **Configuration > Devices**. Click more actions (...) at the end of the row and choose **Template Log**. There are also options to review the configuration by selecting **Running Configuration (on device)** or **Local Configuration (on vManage)**.

The Status column on **Configuration > Devices** will show Out of Sync if the template is not attached successfully to device. It is possible to click the **Out of Sync** link to view configuration differences.

Figure 33 Device Out of Sync with Template

Serial	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status*	Validity
ISR4321-K9-FD0210708TQ		01553C70	NA	NA	ISR4321-1	2.2.0.11	100	vManage	DC_RTP_Template	In Sync	valid
IR1101-K9-FCW225190A9		03558887	NA	NA	IR1101-EFA	2.2.0.12	212	vManage	IR1101-DUAL-LTE-AND...	In Sync	valid
IR1101-K9-FCW23110H97		03CF40F1	NA	NA	IR1101-3-NET	2.2.0.13	203	CLI	-	In Sync	valid
IR1101-K9-FCW23100HTE		03973469	NA	NA	IR1101-Lab-N13	2.2.0.15	205	vManage	IR1101-template-MPLS-L...	In Sync	valid
IR1101-K9-FCW2336GHEN		0448CC25	NA	NA	IR-1101-6	2.2.0.16	206	vManage	IR1101-template-MPLS-L...	In Sync	valid
CSR-2568717C-8791-90F3-6V6V-CWE40...		FD6684F7	NA	NA	car1kv-wedge1	2.2.0.100	1000	CLI	-	In Sync	valid
IR1101-K9-FCW23270HYY		04097F71	NA	NA	IR-1101-7	2.2.0.17	217	vManage	IR1101-LTE	Out of Sync - Device L... staging	File Upload ...
ISR4321-K9-FD0210708VL		01552386	NA	NA	-	-	-	vManage	DC_RTP_Template	Sync Pending - Device...	valid
CSR-56721764-A515-8527-718D-C7C4...		Token - c96ea83bb8ad...	NA	NA	-	-	-	vManage	CSR1kv	Sync Pending - Device...	valid
IR1101-K9-FCW2336DH7J		044757A3	NA	NA	IR-1101-2-EFA	2.2.0.22	212	vManage	IR1101-DUAL-SIM	Sync Pending - Device...	valid

Control Plane Connectivity Not Established

Go to **Monitor > Network** and select the device. Select **Control Connections** from the left panel to view connectivity to vManage and vSmart. If connectivity is not established, use the **ping** command to check connectivity.

Data Plane Connectivity Not Established

Check that the device is not in staging mode by going to **Configuration > Certificates**. If device is in **Staging** mode, switch to **Active** and click **Send to Controllers** at the top of the page.

Refer to the following link for more tips on data plane connectivity:

<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214510-troubleshoot-bidirectional-forwarding-de.html>

Configuration Reset

Clearing the configuration of the router may be needed in order to restart the PnP process. To clear the SD-WAN configuration from a router take either of the following actions.

```
Device# request platform software sdwan config reset
```

```
Device# reload
```

Or:

```
Device# request platform software sdwan software reset
```

Troubleshooting LTE Connectivity

Make sure the following requirements are addressed:

- If the signal is not good at the router, use the Cisco offered antenna accessories and extension cables to place the antenna away from router in a better coverage area.
- You must have 4G LTE network coverage where your router is physically placed.
- You must subscribe to a service plan with a wireless service provider and obtain a Subscriber Identity Module (SIM) card. Only micro SIM is supported. The SIM cards are usually provided in an unlocked state so that it can be used without a Personal Identification Number (PIN). If the SIM is unlocked, it can be inserted into a 4G LTE-Advanced module and used without an authorization code.
- You must install the SIM card before configuring the 4G LTE or router.

- Make sure APN is configured per provider instructions. The **show cellular unit profile** command shows information about the modem data profiles created and attached. The *unit* argument identifies the router slot, module slot, and port separated by slashes (i.e. 0/1/0).

```
Router# show cellular 0/1/0 profile
```

- The **show cellular unit network** command displays information about the carrier network, cell site, and available service.
- The **show cellular unit radio** command shows the radio signal strength.
- Note that cellular networks have higher latency compared to wired networks. Latency rates depend on the technology and carrier. Latency also depends on the signal conditions and can be higher because of network congestion.

Device Management

Software Upgrade

When upgrading using vManage, you can upgrade using a code image that is directly loaded onto vManage or a remote vManage, and you can also upgrade using a code image located on a remote file server. In this procedure, software for any device is uploaded to the vManage software repository.

Uploading Images on vManage

1. Go to **Maintenance > Software Repository**. The repository stores the image locally on vManage, a remote file server, or remote vManage.
2. Click **Add New Software** and choose **vManage** from the drop-down list.
3. A dialog box will appear prompting you to drop an image file or browse for an image on the local computer.
4. Load the desired images and click the **Upload** button. A window will indicate that the images are being loaded to the vManage. Once completed, a message will indicate the images were uploaded successfully, and the version, software location (vManage), and available files will be added to the repository.

Device Upgrade

1. Confirm there is enough space on the device for an image download using the **dir bootflash:** command. Free space is shown at the bottom. Remove files if needed.
2. Go to **Maintenance > Software Upgrade** to check the code versions under the **Current Version** column.

Figure 34 Device Upgrade

Device Group	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability*	Current Version	Available Versions	Default Version
IRL	IR-1101-6	2.2.0.16	IR1101-K9-FCW23360HEN	206	IR1101	reachable	16.12.1b.0.4		16.12.1b.0.4
	IR-1101-EFA	2.2.0.12	IR1101-K9-FCW225100A9	212	IR1101	reachable	16.12.1d.0.32	16.12.1b.0.4	16.12.1b.0.4
	IR-1101-Lab-N13	2.2.0.15	IR1101-K9-FCW23100HTF	205	IR1101	reachable	16.12.1d.0.32		16.12.1d.0.32
	IR1101-3-INET	2.2.0.13	IR1101-K9-FCW23110H97	203	IR1101	reachable	16.12.1d.0.32		16.12.1d.0.32

3. If an upgrade is needed, check the check boxes next to the routers you want to upgrade and click the **Upgrade** button. A dialog box will appear.

4. Verify **vManage** is selected. Choose the new code version from the drop-down list.
5. Check the **Activate and Reboot** check box and then click **Upgrade**. The device will retrieve the software, install it, and then reboot in order to activate it. Optionally you can leave the box unchecked and activate the image later.

Warning: upgrade may fail if there is insufficient disk space (CSCvq13666). Check release notes for more information. Make sure you check disk space before starting the upgrade on the device.

Activate an Image

For images already installed but not activated follow the steps:

1. Go to **Maintenance > Software Upgrade** to check the code versions under the **Current Version** column.
2. Check the check boxes next to the routers you want to activate and click **Activate**. A dialog box will appear.
3. If there is an image installed ready to activate it will show in the **Version** drop-down menu. Select the version and click **Activate**. The router will reboot with the new version.

Best Practices

- Break up the routers into different upgrade groups. You can identify them with a tag in the device-groups field in the system template. Target a test site or multiple test sites and put those routers into the first upgrade group.
- In dual-router sites, put each router into a different upgrade group and do not upgrade both of them at the same time.
- All routers in an upgrade group can be upgraded in parallel (up to 32 WAN Edge routers), however, take into account the ability for vManage or a remote file server to be able to handle the concurrent file transfers to the routers.
- Upgrade the first upgrade group and let the code run stable for a predetermined amount of time, then proceed to upgrade the additional upgrade groups.
- To keep the disk from getting full, clean up older versions using vManage. To delete older versions, go to **Maintenance > Software Upgrade**, select the device you want to clear and select **Delete Available Software**. On the dialog box select the images you want to delete and then click **Delete**.

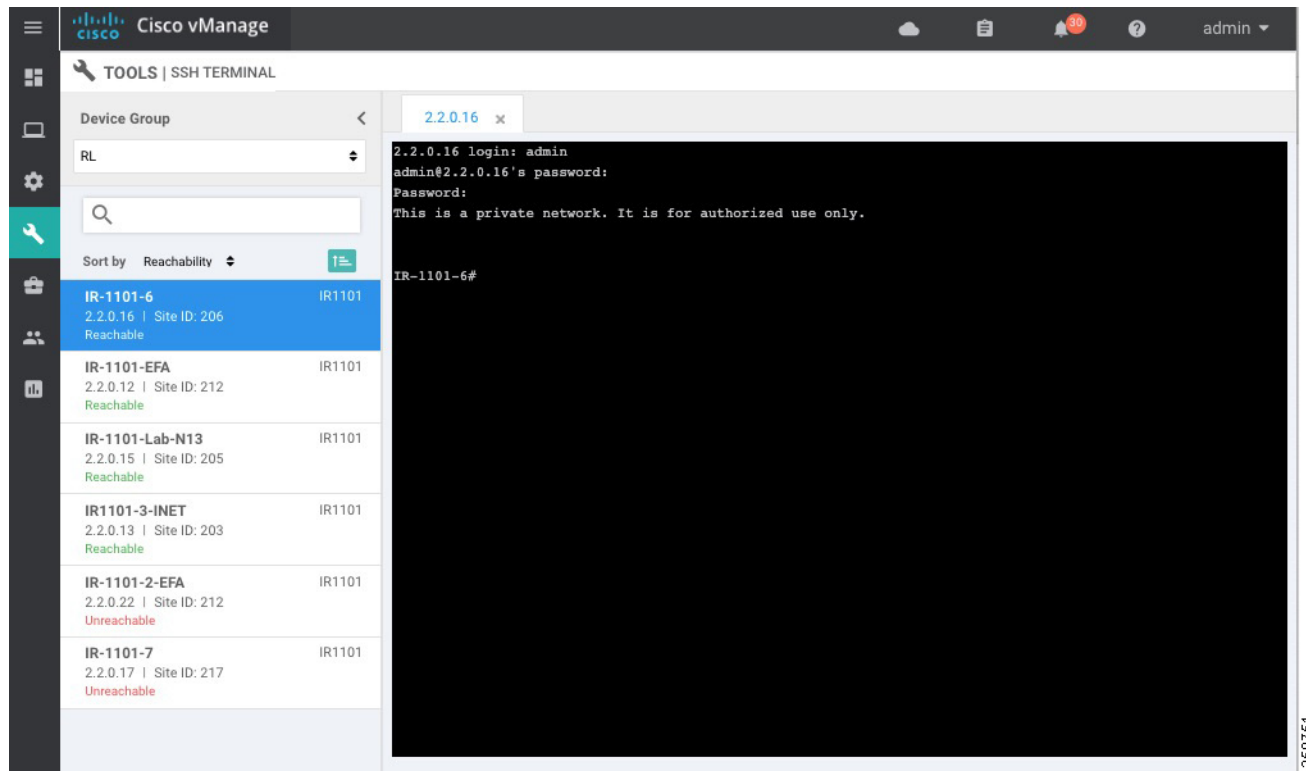
Reboot a Device

Reboot a router by going into **Maintenance > Device Reboot**. Make sure you are on the **WAN Edge** tab. Select the device to reboot and click **Reboot**. Confirm the action on the pop out window.

Connect to the Device Terminal

Go to **Tools > SSH terminal**. Choose the device you want to connect on the left panel. A terminal window to the device will be displayed. Provide device credentials.

Figure 35 Device Terminal



Generate Admin Tech

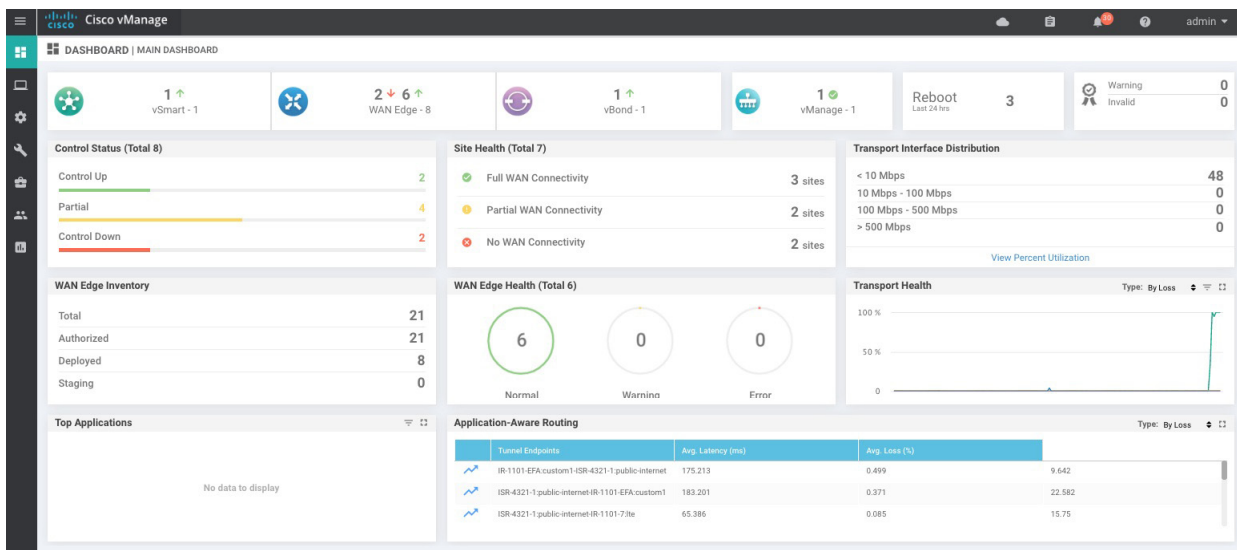
Go to **Tools > Operational Commands**. Choose the router and click on more actions (...) at the end of the row. Click **Admin Tech**. Select the information you want to collect and click **Generate**. Wait until the file is generated and then click **Download**.

Monitor

Main Dashboard

Use the dashboard screen to monitor, at a glance, the overall health of the SD-WAN overlay network.

Figure 36 Dashboard



The top bar shows tasks and alarms on the system. The dashboard also displays all control connections from vManage to the vSmart controllers, WAN Edge routers, and vBond orchestrators in the overlay network as well as the status of the vManage NMSes in the network. You can click on the number or the Up or Down arrow to display a table with detailed information for each connection.

The dashboard displays the total number of reboots in the last 24 hours for all devices in the network. Click the **Reboot pane** for more information.

The **Control Status** pane displays whether vSmart and WAN Edge routers are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each WAN Edge router must connect to the configured maximum number of vSmart controllers. The **Control Status** pane shows three counts:

- **Control Up:** Total number of devices with the required number of operational control plane connections to a vSmart controller.
- **Partial:** Total number of devices with some, but not all, operational control plane connections to vSmart controllers.
- **Control Down:** Total number of devices with no control plane connection to a vSmart controller.

Click any row to display a table with device details.

The **Site Health View** pane displays the state of a site data connections. When a site has multiple WAN edge routers, this pane displays the state for the entire site, not for individual devices. The pane displays three states:

- **Full WAN Connectivity:** Total number of sites where all BFD sessions on all WAN edge routers are in the up state.
- **Partial WAN Connectivity:** Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- **No WAN Connectivity:** Total number of sites where all BFD sessions on all WAN edge are in the down state. These sites have no data plane connectivity.

Click a row to display a pop-up window with detailed information on each site, node, or tunnel.

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

The **WAN Edge Inventory** pane provides four counts:

- **Total:** Total number of WAN Edge routers whose authorized serial number has been uploaded on the vManage server.
- **Authorized:** Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid.
- **Deployed:** Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.
- **Staging:** Total number of WAN Edge routers in staging state.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

The **WAN Edge Health** pane displays an aggregated view for each router state according to resource utilization and a count of how many WAN Edge routers are in that state

The **Transport Health** pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors. From the Type drop-down, select loss, latency, or jitter. Click the **Expand** icon to open the **Transport Health** window. This full-screen window displays a more detailed view of the same information.

The **Application-Aware Routing** pane displays the 10 worst tunnels over the last 24 hours based on criteria specified from the **Type** drop-down list, including loss, latency, and jitter.

Geography

Use the **Geography** page (**Monitor > Geography**) to view information about the Cisco SD-WAN devices and links in the overlay management network. The Geography page provides a map displaying the geographic location of the Cisco SD-WAN devices. It is possible to filter by tag.

To choose the devices you want to display on the map use the Filter button, and the map is dynamically updated to reflect your selections. Also, as you make the device group, device type, and link selections, the tabs next to the **Filter** button are updated.

To display basic information for a device, hover over the device icon. A window displays the system IP address, hostname, site ID, device type, and device status.

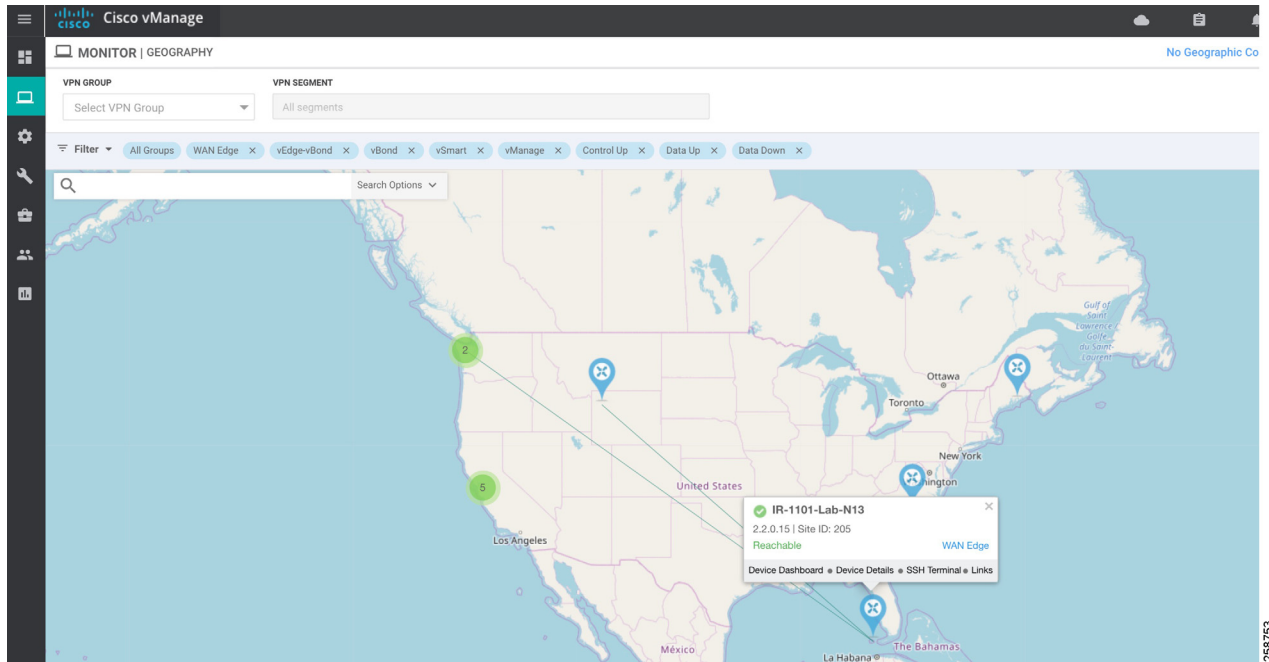
By default, control and data connections are not displayed on the map. To see control and data connections for a device double-click the device icon to open a window with details about the device. Click **Links**.

- An active control connection between two devices is displayed on the map as a thin blue line. Multiple active connections between devices are displayed by a bold blue line. A control connection that is down is displayed on the map as a dotted red line. Multiple control connections that are down are displayed by a bold dotted red line. If you hover over the line, the connection status (up or down) is shown.
- An active data connection between two devices is displayed on the map as a thin green line. Multiple active data connections are displayed by a bold green line. A data connection that is down is displayed on the map as a dotted red line. Multiple data connections that are down are displayed by a bold dotted red line. If you hover over the line, the connection status (up or down) is shown.
- An active consolidated control and data connection between two devices is displayed on the map as a thick gray line.

Similarly, it is possible to double-click on the device to go to **Device Dashboard**, **Device Details**, or **SSH terminal**.

Tip: Device location and device groups are configured using System Feature Template.

Figure 37 Monitor Geography



Network

Use the **Network** page (**Monitor > Network**) to display a list of Cisco SD-WAN devices in the overlay network and to display detailed information about individual devices. The device list can be filtered by group, reachability, hostname, system IP address, site ID, and device model. Choose options from the **Sort** drop-down list or enter a string in the **Search** box.

The following image shows how to use the Network page to view devices in Staging state. Sort or filter by reachability. Note that this view also shows BFD and control connections. Devices in Staging will show control connections, but BFD will be 0. Information can be downloaded to a CSV file using the arrow at the top right of the table.

Figure 38 Monitor Network Reachability

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability↑	Site ID	BFD	Control	Version	Up Since	Device Groups
vmanage	2.2.0.1	vManage	90ccf5c9-200a-478b-9028-975a5...	✓	reachable	100	--	7	19.2.0	09 Jan 2020 6:13:00 PM EST	"No groups"
vsmart	2.2.0.2	vSmart	f2fd3bb0-adaa-4c64-862b-aba120...	✓	reachable	100	--	9	19.2.0	02 Oct 2019 10:31:00 AM EDT	"No groups"
vBond	2.2.0.3	vEdge Cloud (vBo...	c1dffe1-ed8c-439d-9467-da5e67...	✓	reachable	100	--	--	19.2.0	23 Aug 2019 12:14:00 PM EDT	"No groups"
IR-1101-2-EFA	2.2.0.22	IR1101	IR1101-K9-FCW23360H7J	✓	reachable	212	1	2	16.12.1b.0.4	17 Jan 2020 6:52:00 PM EST	"IR1101" "RL" "US"
IR-1101-6	2.2.0.16	IR1101	IR1101-K9-FCW23360HEN	✓	reachable	206	3	2	16.12.1b.0.4	05 Dec 2019 1:58:00 PM EST	"IR1101" "RL" "US"
IR-1101-EFA	2.2.0.12	IR1101	IR1101-K9-FCW225100A9	✓	reachable	212	4	3	16.12.1d.0.32	05 Dec 2019 4:23:00 PM EST	"IR1101" "RL" "US"
IR-1101-Lab-N13	2.2.0.15	IR1101	IR1101-K9-FCW23100HTF	✓	reachable	205	3	2	16.12.1d.0.32	18 Dec 2019 6:06:00 PM EST	"IR1101" "RL" "US"
IR1101-3-INET	2.2.0.13	IR1101	IR1101-K9-FCW23110H97	✓	reachable staging	203	0	2	16.12.1d.0.32	14 Jan 2020 2:41:00 AM EST	"IR1101" "RL" "US"
ISR-4321-1	2.2.0.11	ISR4321	ISR4321/K9-FD0210708TQ	✓	reachable	100	6	3	16.12.1b.0.4	02 Dec 2019 4:06:00 PM EST	"DC" "EAST" "ISR" "...
IR-1101-7	2.2.0.17	IR1101	IR1101-K9-FCW23270HY	✗	unreachable	217	--	--	16.12.1d.0.32	17 Jan 2020 3:26:00 PM EST	"IR1101" "RL" "US"
csr1kv-vedge1	2.2.0.100	CSR1000v	CSR-25E6717C-B791-90F3-E9E9-C...	✗	unreachable	1000	--	--	16.12.1b.0.4	02 Oct 2019 2:42:00 PM EDT	"No groups"

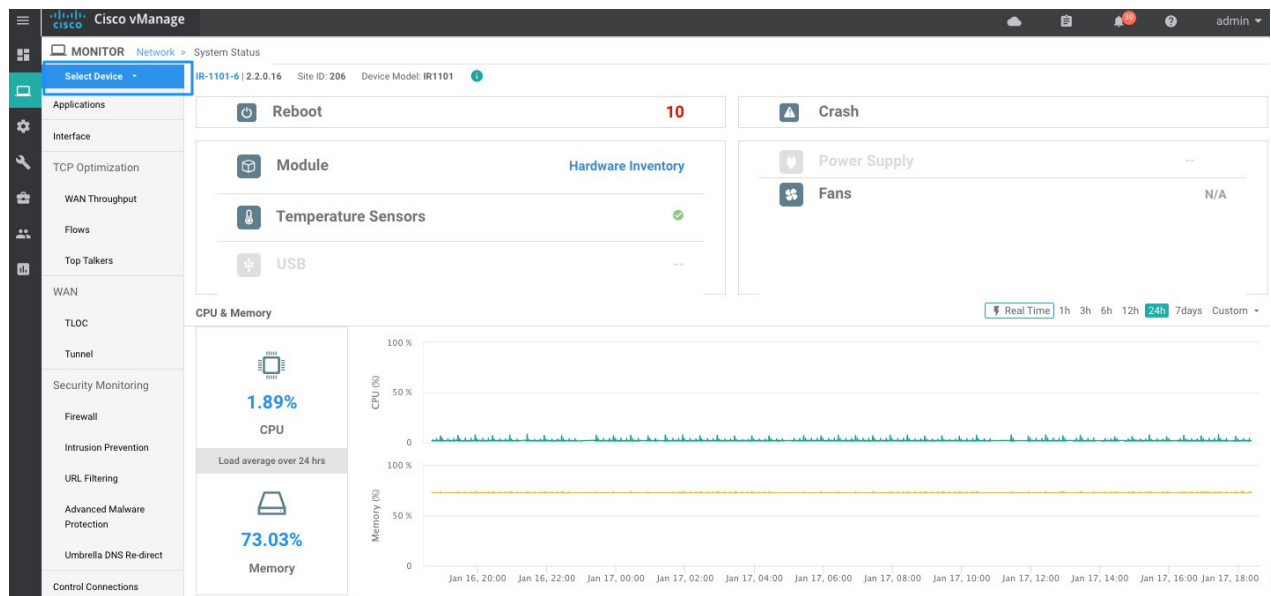
To display information about an individual device, click the device hostname. The left pane lists the information categories about the device. In the right pane, the **System Status** category is selected, which displays status information about the device.

To select a different device, either choose a device from the **Select Device** drop-down list located at the top of the left pane or click **Network** in the title bar and then click a device hostname.

System Status

To view system status for a device, go to **Monitor > Network**, then click a device hostname. The **System Status** page shows information such as CPU, memory, hardware inventory and number of times the device has rebooted.

Figure 39 System Status

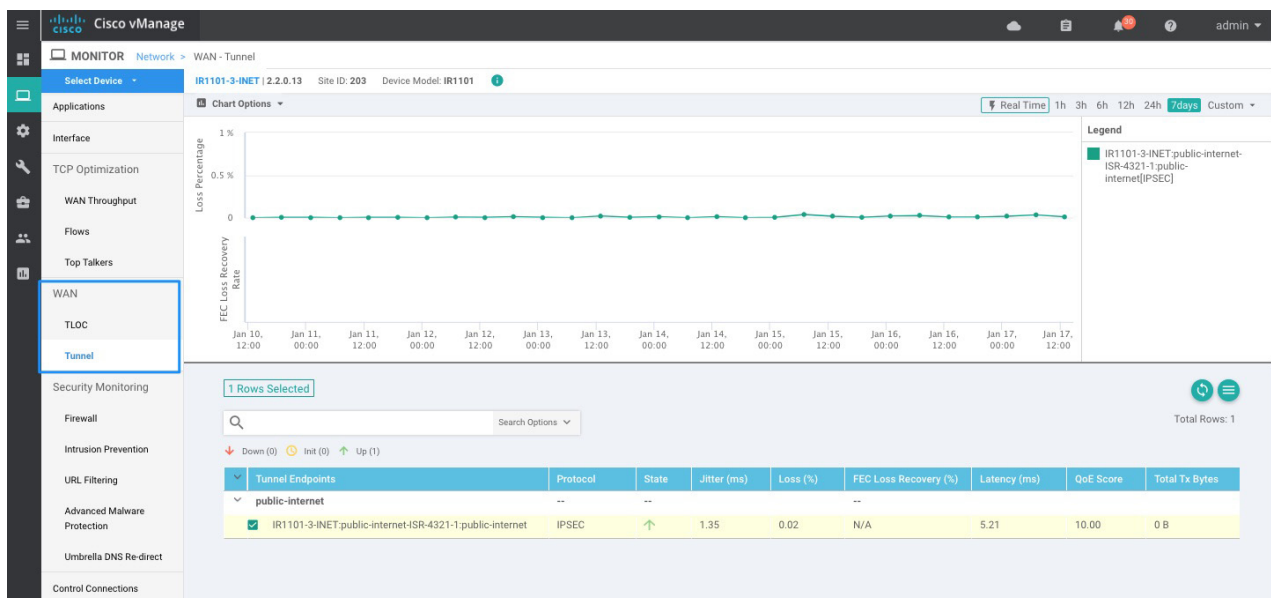


WAN Information

Go to **Monitor > Network** and then click a device hostname.

- **WAN >TLOC** on the left panel shows information about TLOC loss, latency, and jitter.
- **WAN > Tunnel** on the left panel displays information about all data plane tunnels, you can easily see if you are sending or receiving packets for a particular tunnel. This can help you understand if packets are making it on each end, and isolate connectivity issues between the nodes.

Figure 40 Monitor Device WAN Information



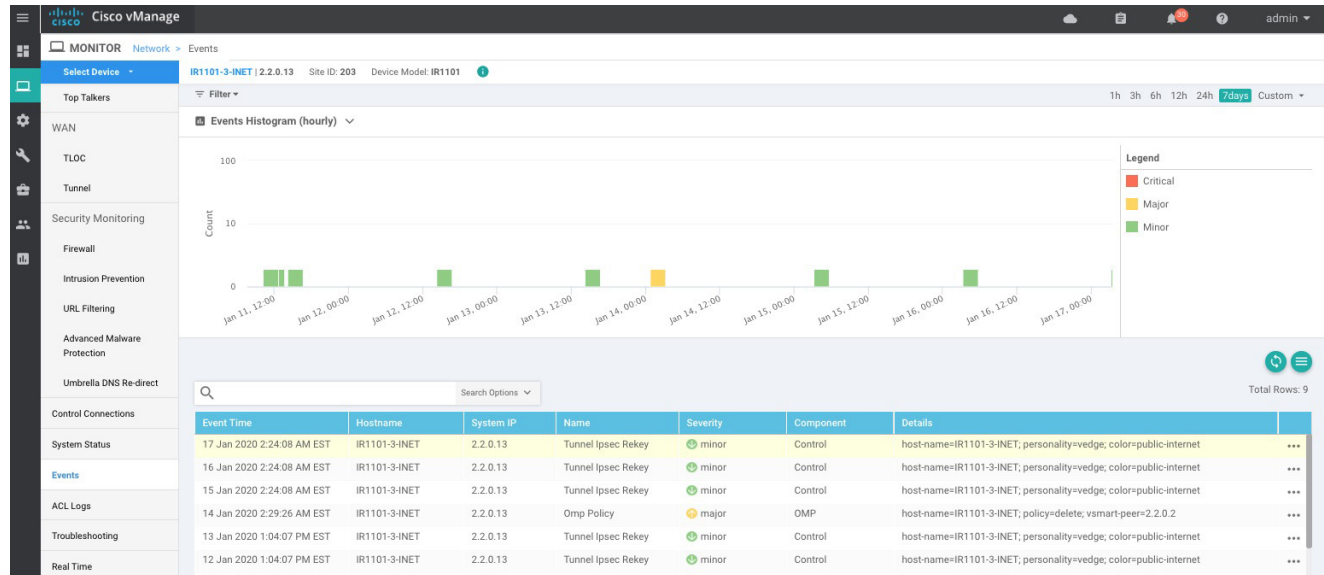
Control Connections

Go to **Monitor > Network** and click a device hostname, then choose **Control Connections** on the left panel. It shows the expected and actual number of connections and the control connections data in graphical and tabular format.

Events

To view the number of critical, major, or minor events on a device go to **Monitor > Network** and click a device hostname, then choose Events on the left panel. It shows a list of the events and a histogram.

Figure 41 Events



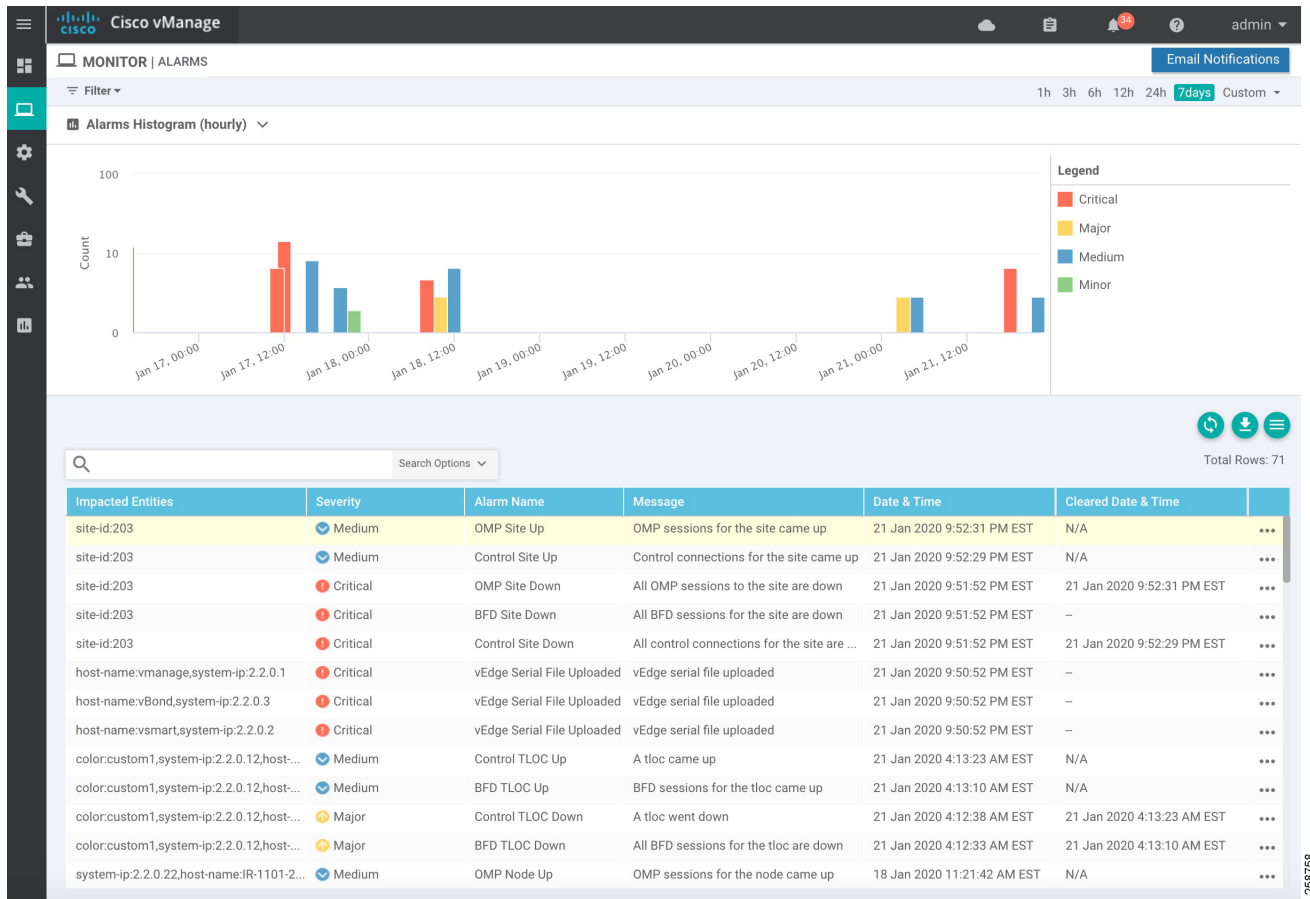
Tip: Events can be useful to troubleshoot a device that went offline. Choose **Events** from the left panel to display events from the device before it went down, such as `bfd-state-change`, `omp-state-change`, or `control-connection-state-change`.

Alarms

Use the Alarms (**Monitor > Alarms**) page to display detailed information about alarms generated by controllers and routers in the overlay network.

To set filters for searching alarms generated by one or more Cisco SD-WAN devices click the Filter drop-down menu. You can filter by severity, status, alarm name, severity and impacted entity. To view detailed information about any alarm, click the table row and click the More Actions icon (...) to the right of the row, then choose **Alarm Details**. The Alarms Details window opens, displaying the possible cause of the alarm, impacted entities, and other details.

Figure 42 Alarms



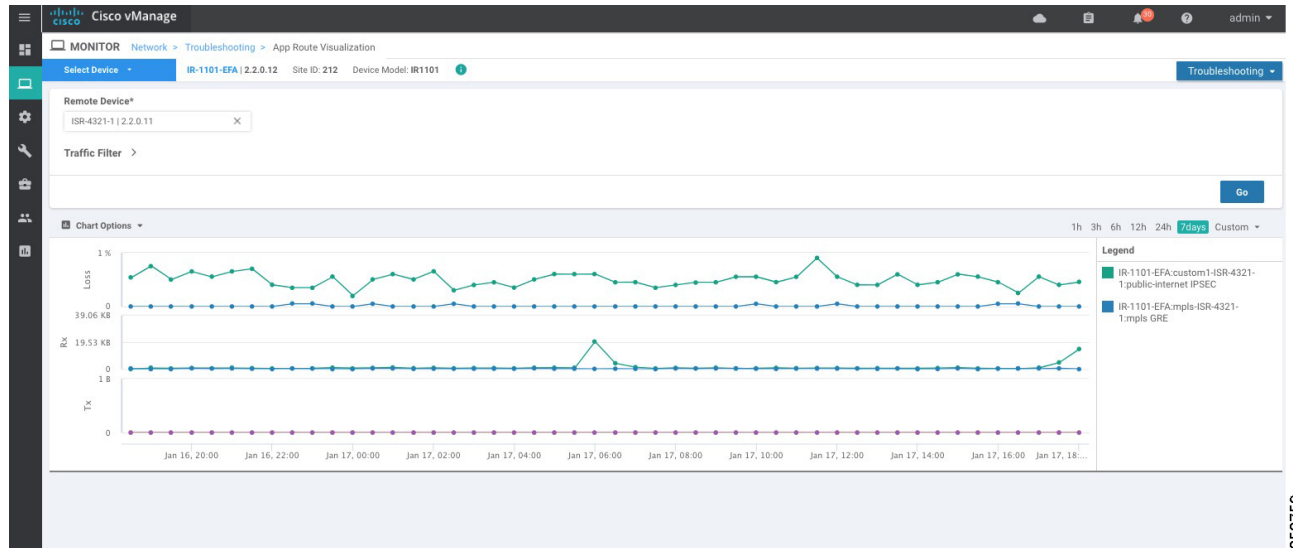
The software generates alarms when a state or condition changes, such as when a software component starts, transitions from down to up, or transitions from up to down. Refer to https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/monitor.html#c_Alarms_12333.xml for available alarms.

Troubleshooting

You can troubleshoot connectivity or traffic health for all devices in the overlay network. Go to **Monitor > Network**, click a device hostname, then choose **Troubleshooting** on the left panel. Some troubleshooting features are grayed out because they do not apply to IOS XE SD-WAN routers in this release.

- Device Bring up is used to verify the status of device onboarding up as explained in Device Onboarding Troubleshooting.
- Control Connections (Live View) shows Control Connections in Real Time. This view not only shows actual connections but detail on expected connections color and current status.
- Tunnel Health displays either loss, latency, or jitter in graphical format for all tunnels between the two devices in each direction.
- App route visualization is useful to check application-aware routing traffic from the source device to the destination device

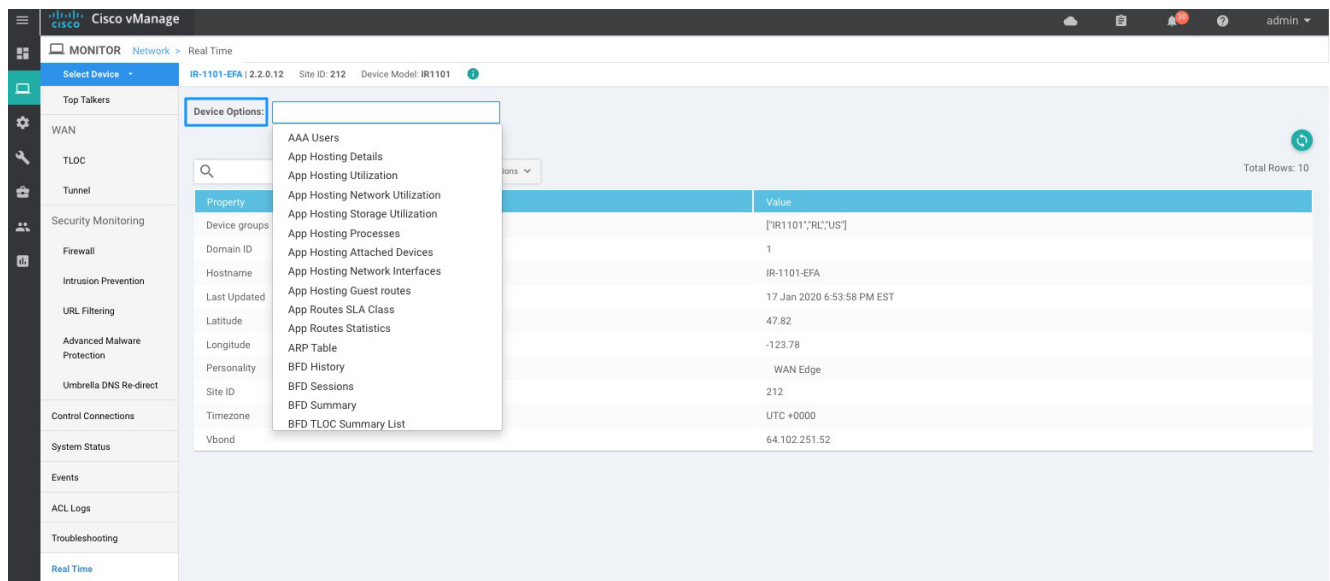
Figure 43 App Route Visualization



Real Time

To see device information in real time, go to **Monitor > Network**, click a device hostname, then choose **Real Time**. You will see the **Device Options** drop-down list located directly under the device name, from which you can choose a feature-specific operational command to display real-time device information for the selected command. The commands in the drop-down are listed alphabetically. The commands available vary depending on the device selected. When you first choose **Real Time**, the **System Information** command is selected, and real-time system information about the device is displayed in tabular format. For some commands, you can add filters to speed up the display of information.

Figure 44 Real Time



Some useful options are included in the table that follows.

BFD commands are useful to troubleshoot data plane connectivity. If BFD tunnels are flapping or down, then there may be packet loss, latency, or NAT issues. You can check which tunnels are up and down with the **show bfd sessions** and **show bfd history** commands. If too many BFD packets are dropped, the tunnel will go down.

OMP commands are useful to troubleshoot centralized control policy and tunnel preferences.

Table 38 Real Time Commands

Device Options	Description
App Routes SLA Class	Displays information on SLA classes on the device
App Routes Statistics	Display statistics about data traffic, jitter, loss, and latency and other interface characteristics for all operational data plane tunnels
bfd history	Display the history of the BFD sessions
bfd sessions	<p>Display information about the BFD sessions running on the local router. The following information is displayed:</p> <ul style="list-style-type: none"> ■ System IP: Peers system-ip ■ Source and Remote TLOC Color: This is useful to know what TLOC you are expecting to receive and send. ■ Source IP: It is the private source IP. ■ DST public IP: It is the destination that the router is using to form the Data Plane tunnel. ■ DST public PORT: Public NAT-ed port that the router uses in order to form the Data Plane tunnel to the remote WAN Edge. ■ Transitions: Number of times the BFD session has changed its status, from NA to UP and vice versa.
bfd summary	Display summary information about the BFD sessions running
bfd tloc summary list	Display BFD session summary information per TLOC
cellular connection	Display cellular connection stats, active profile, IP address and DNS
cellular network	Display information about cellular network
cellular radio	Displays cellular radio status and details
control connections	Display information about active control plane connections
control connections history	Display information about control plane connection attempts initiated by the local device.
control local properties	Display the basic configuration parameters and local properties related to the control plane and certificates
control statistics	Display statistics about the packets that router has transmitted and received in the process of establishing and maintaining secure DTLS connections
interface detail	Display information about IPv4 interfaces on the router
omp services	Display the services learned from OMP peering sessions.
omp peers	Display information about the OMP peering sessions that are active

omp received routes	Display routes received from vSmart. Use the following reference for status Codes: C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Inv -> invalid
omp received TLOCs	Display information learned from the TLOC routes advertised over the OMP sessions running between vSmart controllers and routers. You can also run this command on vSmart to check if the vSmart Receives TLOCs sent by router
policy access list associations	Display the IPv4 access lists that are operating on each interface.
policy access list counters	Display the number of packets counted by IPv4 access lists configured on the router. Counters are defined on the policy creation
policy access list names	Display the names of the IPv4 access lists configured on the router

Additional Command Line Interface Commands

You can use SSH connection from vManage to run any CLI command. Some useful commands are described in the following sections.

Check Connectivity

Use the ping and traceroute commands to check connectivity. Make sure you are pinging from the right VPN; VPN 0 is default. Use VRF keyword to select VPN.

```
ROUTER#traceroute vrf 1 10.2.1.1
```

Check Template Attachment

If a template is not attaching, or if the configuration of the device is not changing, you can check the status of the template with the **show sdwan system** command. It will show vManage: true, Commit Pending: false and display configuration template name when template is attached successfully.

```
IR-1101-2-EFA#show sdwan system
Viptela (tm) vedgeOperatingSystemSoftware
.....
Personality:          vedge
Model name:           vedge-IR-1101
Services:              None
vManage:              true
Commit pending:       false
Configuration template: IR1101-DUAL-SIM
Chassis serial number: FFFFFXXXXAB
```

Check QoS Scheduler

Use the show policy-map interface int command to check stats for scheduler on the WAN interface. It will display the service policy name and statistics for rate and packets.

```
IR-1101-EFA#show policy-map interface gi 0/0/0
GigabitEthernet0/0/0

Service-policy output: shape_GigabitEthernet0/0/0
```

Caveats and Limitations

```

...

Service-policy : qos_class

...

Class-map: Queue0 (match-any)
6727731 packets, 3111326413 bytes
5 minute offered rate 28190000 bps, drop rate 0000 bps
Match: qos-group 0
Priority: 30% (30000 kbps) , burst bytes 750000, b/w exceed drops: 2328

Class-map: Queue3 (match-any)
5 minute offered rate 683000 bps, drop rate 0000 bps

Match: qos-group 3
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/27/0
(pkts output/bytes output) 785297/73853878
bandwidth 5% (5000 kbps)

```

Check if Tunnel Meets SLA

Display statistics about jitter, loss, and latency and other interface characteristics for all operational data plane tunnels using the `show sdwan app-route stats` command. `sla-class-index` line in the output displays SLA classes for which the tunnel meets SLA criteria.

```

IR-1101-EFA#show sdwan app-route stats remote-system-ip 2.2.0.11
app-route statistics 10.12.255.10 10.22.255.2 gre 0 0
remote-system-ip 2.2.0.11
local-color    public-internet
remote-color   public-internet
mean-loss      0
mean-latency   123
mean-jitter    6
sla-class-index 0,1,2,3,4

```

	TOTAL	AVERAGE	AVERAGE	TX DATA	RX DATA	DATA	DATA	
INDEX	PACKETS	LOSS	LATENCY	JITTER	PKTS	PKTS	PKTS	PKTS
0	132	01	0	6035	1	0	0	
1	133	01		0	0	0	0	

Check Policy from vSmart

Display a centralized data policy, an application-aware policy, or a cflowd policy that a vSmart controller has pushed to the router with the command `show sdwan policy from-vsmart`.

Caveats and Limitations

- Although profiles can be created, modified and deleted, current versions of vManage do not allow you to select the default profiles. If you need to use customized profiles (for example, Access Point Name (APN) in mobile networks), you must overwrite the selected default profile as explained in 4G LTE Configuration.

Caveats and Limitations

- The rollback feature does not support restoring changes to default APN configuration. If there is not an APN profile explicitly provisioned with a feature template before applying a template that overwrites the APN and control connection is lost due to that change, the rollback feature will not restore default APN configuration.
- Dual SIM cards with different APNs is not possible when using customized profiles due to a current vManage limitation. Using vManage version 19.2 (and older) it is not possible to associate a specific APN per slot using feature templates. Because of that any customization applied to a cellular unit will apply to all SIM slots on the module.
- An upgrade may fail if there is insufficient disk space (CSCvq13666). Check release notes for more information. Make sure you check disk space before starting the upgrade on the device.



Appendix A – Upgrade Cisco IR1101 with IOS XE SD-WAN Image

1. Use the console port to connect to the router. Check available space in bootflash; a minimum of 1.5 GB space is needed for the image. Delete old files if necessary, using the **delete** command.

```
Router#delete /force /recursive tracelogs
```

2. Download the Cisco IOS XE SD-WAN software image from the Cisco site.
3. Upload the Cisco IOS XE SD-WAN software image from the file server to the router bootflash. In this case the image is loaded on a USB flash drive and copied to the device.

```
Router#copy usbflash0:ir1101-ucmk9.16.12.1d.SPA.bin bootflash:
```

4. If using bootstrap method, copy the configuration file to bootflash

```
Router#copy usbflash0:ciscosdwan.cfg bootflash:
```

5. If using bootstrap method and the enterprise root certificate, copy the certificate to bootflash

```
Router#copy usbflash0:certificate bootflash:
```

6. Remove all existing boot statements and save the configuration. You can check for existing statements using the command `show run | i boot`. If there is any statement, go to configuration mode and delete it using the `no boot system` command.

```
Router#config t  
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no boot system flash bootflash:IR1101-universalk9.16.03.07.SPA.bin
```

7. Add a boot variable that points to the Cisco IOS XE SD-WAN image:

```
Router# (config)# boot system flash bootflash:SDWAN-image
```

8. Write the configuration to memory

```
Router# wr mem
```

9. Verify that the BOOT variable shows only the IOS XE SD-WAN image:

```
Router# show bootvar  
BOOT variable = bootflash:ir1101-ucmk9.16.12.1d.SPA.bin,1;  
CONFIG_FILE variable does not exist  
BOOTLDR variable does not exist  
Configuration register is 0x2102
```

10. Remove all existing configuration from the router:

```
Router# write erase
```

11. Set the config-register to 0x2102:

```
Router# config t
```

```
Router(config)# config-register 0x2102  
Router(config)# end
```

12. Reload the router

```
Router# reload
```

13. The router reboots with the IOS XE SD-WAN image. If the initial configuration dialog is presented, enter **No**. When prompted to terminate auto install, enter **yes**.

```
System configuration has been modified. Save? [yes/no]:  
% Please answer 'yes' or 'no'.
```

```
System configuration has been modified. Save? [yes/no]: no  
Proceed with reload? [confirm]
```

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

15. Stop PnP and allow the Cisco IOS XE SD-WAN packages to install:

```
Router# pnpa service discovery stop
```

16. Wait until the router has completed expanding the SD-WAN package. You should see the following line on the console.

```
Jan 17 22:33:33.900: %INSTALL-5-OPERATION_COMPLETED_INFO: R0/0: packtool: Completed expand package running
```

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

```
Router#request platform software sdwan software reset
```

```
*Jan 17 20:00:04.302: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install activate  
bootflash:ir1101-ucmk9.16.12.1d.SPA.bin  
*Jan 17 20:00:18.139: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram  
Router#
```

18. The router will either start the PNP process or boot with bootstrap configuration if the file was copied on to the device.

19. If using bootstrap method and If using a certificate signed by your enterprise root certificate authority (CA), install the certificate. When using PnP this step is not required.

```
Router# request platform software sdwan root-cert-chain install bootflash: certificate
```

20. To verify that the control connections are up and the device is validated, enter the following command at the system prompt:

```
Device# show sdwan control connections
```



Appendix B – Cisco SD-WAN End-to-End Deployment Guide Templates Used

System feature template settings

Table 39 System feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_hostname
	Device Groups	Device Specific	system_device_groups
	Console Baud Rate (bps)	Device Specific	system_console_baud_rate
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset

Logging feature template settings

Table 40 Logging feature template settings

Section	Parameter	Type	Variable/value
Server	Hostname/IP Address	Global	10.22.2.4
	VPN ID	Global	1
	Source Interface	Global	loopback0

NTP feature template settings

NTP feature template settings

Table 41 NTP feature template settings

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

AAA feature template settings

Table 42 Table 42 AAA feature template settings

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

OMP feature template settings

Table 43 OMP feature template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Number of Paths Advertised per Prefix	Global	16
	ECMP Limit	Global	16
Advertise	Connected	Global	Off
	Static	Global	Off

Table 44 BFD feature template settings

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

Security feature template settings

Table 45 Security feature template settings

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

Banner template settings

Banner template settings

Table 46 Banner template settings

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

SNMP template settings

Table 47 SNMP template settings

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Device Specific	snmp_shutdown
	Name of Device for SNMP	Device Specific	snmp_device_name
	Location of Device	Device Specific	snmp_device_location
SNMP Version	SNMP Version	Radio button	V2
SNMP Version/View & Community	View/Name	Global	isoALL
	View/Object Identifiers	Global	1.3.6.1
	Community/Name	Global	c1sco123
	Community/Authorization	Global/Drop-down	read-only
SNMP Version/Trap	Community/View	Global	isoALL
	Trap Group/Group Name	Global	SNMP-GRP
	Trap Group/Trap Type Modules/Module Name	Global	all
	Trap Group/Trap Type Modules/Severity Levels	Global	critical, major, minor
	Trap Target Server/VPN	Global	1
	Trap Target Server/IP Address	Global	10.22.2.6
	Trap Target Server/UDP Port	Global	162
	Trap Target Server/Trap Group Name	Global	SNMP-GRP
Trap Target Server/Community Name	Global	c1sco123	
Trap Target Server/Source Interface		loopback0	

SNMP template settings



Appendix C – Cisco IE Switches configuration

OSPF Configuration on Industrial Ethernet Switch

```
vrf definition employee
 rd 11:11
 !
 address-family ipv4
  route-target export 11:11
  route-target import 11:11
 exit-address-family
 !
vrf definition video
 rd 10:10
 !
 address-family ipv4
  route-target export 10:10
  route-target import 10:10
 exit-address-family
 !
 !
 !
spanning-tree mode rapid-pvst
spanning-tree extend system-id
no spanning-tree vlan 1,16-17,116,130-250,253-255,1006

interface GigabitEthernet1/1
 switchport mode trunk
 load-interval 30
 !
 !
interface Vlan15
 ip address 10.12.15.1 255.255.255.252
 ip ospf network point-to-point
 !
interface Vlan16
 ip address 10.12.16.1 255.255.255.252
 ip ospf network point-to-point
 !
interface Vlan17
 ip address 10.12.17.1 255.255.255.0
 !
interface Vlan115
 vrf forwarding video
 ip address 10.12.115.1 255.255.255.252
 ip ospf network point-to-point
 !
interface Vlan116
 vrf forwarding video
 ip address 10.12.116.1 255.255.255.252
```

Configuration on Industrial Ethernet Switch Connected to Routers Running VRRP

```
ip ospf network point-to-point
!
interface Vlan117
vrf forwarding video
ip address 10.12.117.1 255.255.255.0
!
interface Vlan215
vrf forwarding employee
ip address 10.12.215.1 255.255.255.252
ip ospf network point-to-point
!
interface Vlan216
vrf forwarding employee
ip address 10.12.216.1 255.255.255.252
ip ospf network point-to-point
!
interface Vlan217
vrf forwarding employee
ip address 10.12.217.1 255.255.255.0
!
router ospf 1
router-id 10.12.16.1
auto-cost reference-bandwidth 100000
network 10.0.0.0 0.255.255.255 area 1
!
router ospf 10 vrf video
router-id 10.12.115.1
auto-cost reference-bandwidth 100000
capability vrf-lite
network 10.12.115.0 0.0.0.255 area 10
network 10.12.116.0 0.0.0.255 area 10
network 10.12.117.0 0.0.0.255 area 10
!
router ospf 11 vrf employee
router-id 10.12.217.1
auto-cost reference-bandwidth 100000
capability vrf-lite
network 10.12.215.0 0.0.0.255 area 11
network 10.12.216.0 0.0.0.255 area 11
network 10.12.217.0 0.0.0.255 area 11
```

Configuration on Industrial Ethernet Switch Connected to Routers Running VRRP

```
no spanning-tree vlan 1,16,116,130-250,1006

interface GigabitEthernet1/1
switchport trunk allowed vlan 2-300
switchport mode trunk
!
interface GigabitEthernet1/3
switchport trunk allowed vlan 2-300
switchport mode trunk
!
```



Appendix D – Device Template Values

Device Template Values for IR1101_CELL_with_TRUNK

Devices on Remote Location 2 use device template Name: IR1101_CELL_with_TRUNK, the following table contains a list of variables on the template and some example values used on the implementation.

Table 48 Device Template Values for IR1101_CELL_with_TRUNK

Section	Variable/value	IR-1101-Location2-1	IR-1101-Location2-2
System: variables contain device specific settings. From this template, it is possible to configure baud rate for console connection.			
Basic Configuration	system_site_id	10010206	10010206
	system_system_ip	2.2.0.16	2.2.0.15
	system_hostname	IR-1101-Loc2-1	IR-1101-Loc2-2
	system_device_groups	RL,IR1101,US	RL,IR1101,US
	system_console_baud_rate	9600	9600
GPS	system_latitude	44	44
	system_longitude	-110	-110
Advanced	system_port_hop	FALSE	FALSE
	system_port_offset	0	0
VPN0: Only one default route is defined since there is only one tunnel interface. Other fields are left blank since they are optional.			
IPv4 Route (1)	vpn0_next_hop_ip_address_1	Cellular0/1/0	Cellular0/1/0
IPv4 Route (2)	vpn_ipv4_ip_prefix2		
	vpn0_next_hop_ip_address_2		
IPv4 Route (3)	vpn_ipv4_ip_prefix3		
	vpn0_next_hop_ip_address_3		
VPN0 interface Cellular: Note IPSec preference value is higher for the device with higher VRRP priority in order to have traffic symmetry for DPI. Shaping rate for QoS is defined in this section, this value should be configured according to service provider offered upstream bandwidth.			
Basic Configuration	vpn0_cell1_int_shutdown	FALSE	FALSE
Tunnel>Advanced Options>Encapsulation	vpn0_cell0_1_0_tunnel_ipsec_preference	100	0
ACL	vpn_cell1_qos_shaping-rate	10000	10000
VPN Interface SVI 1(VPN 1): VRRP optional values are used on this location. VRRP tracks prefix list created on localized policy.			

Device Template Values for IR1101_CELL_with_TRUNK

Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan16	vlan16
	vpn_svi_if_description_SVI_1	Shared Services	Shared Services
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.16.2/24	10.12.16.3/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	1	1
	vpn_if_vrrp_priority_1	200	100
	vpn_if_vrrp_track_prefix_list_1	Services-prefix	Services-prefix
	vpn_if_vrrp_vrrp_ipaddress_1	10.12.16.1	10.12.16.1
VPN Interface SVI 1 (VPN 10)			
Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan116	vlan116
	vpn_svi_if_description_SVI_1	Video	Video
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.116.2/24	10.12.116.3/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	1	1
	vpn_if_vrrp_priority_1	200	100
	vpn_if_vrrp_track_prefix_list_1	Services-prefix	Services-prefix
	vpn_if_vrrp_vrrp_ipaddress_1	10.12.116.1	10.12.116.1
VPN Interface SVI 1 (VPN 11)			
Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan216	vlan216
	vpn_svi_if_description_SVI_1	Employee voice	Employee voice
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.216.2/24	10.12.216.3/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	1	1
	vpn_if_vrrp_priority_1	200	100
	vpn_if_vrrp_track_prefix_list_1	Services-prefix	Services-prefix
	vpn_if_vrrp_vrrp_ipaddress_1	10.12.216.1	10.12.216.1
VPN Interface Ethernet (Loopback0)			
IPv4 Configuration	lo0_int_ip_addr maskbits	2.2.0.16/32	2.2.0.15/32
Switchport: FastEthernet0/0/1 is configured as a port in both routers to connect to Industrial Ethernet switch			
Interface 1 (FE0/0/1)	switchport_1_if_shutdown	FALSE	FALSE
	switchport_1_if_trunk_allowed_vlans	1,16,116,216,236	1,16,116,216,236
Interface 2 (FE0/0/2)	switchport_2_if_shutdown	FALSE	FALSE
	switchport_2_if_access_vlan	16	16
Interface 3 (FE0/0/3)	switchport_3_if_shutdown	FALSE	FALSE
	switchport_3_if_access_vlan	116	116
Interface 4 (FE0/0/4)	switchport_4_if_shutdown	FALSE	FALSE
	switchport_4_if_access_vlan	216	216

Device Template Values for IR1101_CELL_with_TRUNK

SNMP			
Basic Configuration	snmp_shutdown	FALSE	FALSE
	snmp_device_name	IR-1101-Loc2-1	IR-1101-Loc2-2
	snmp_device_location	Yellowstone	Yellowstone

Device Template Values for IR1101_INET_and_CELL

IR1101 on Remote Location 1 uses device template Name: IR1101_INET_and_CELL, the following table contains a list of variables on the template and some example values used on the implementation.

Table 49 Device Template Values for IR1101_INET_and_CELL

Section	Variable	IR1101-Location-1
System: variables contain device specific settings. From this template, it is possible to configure baud rate for console connection.		
Basic Configuration	system_site_id	10010213
	system_system_ip	2.2.0.13
	system_hostname	IR1101-Location-1
	system_device_groups	RL,IR1101,US,L1
	system_console_baud_rate	9600
GPS	system_latitude	44.34
	system_longitude	-68.27
Advanced	system_port_hop	FALSE
	system_port_offset	0
VPN0: two default routes are defined, one for each WAN interface		
IPv4 Route (1)	vpn0_next_hop_ip_address_1	GigabitEthernet0/0/0
IPv4 Route (2)	vpn_ipv4_ip_prefix2	0.0.0.0/0
	vpn0_next_hop_ip_address_2	Cellular0/1/0
IPv4 Route (3)	vpn_ipv4_ip_prefix3	
	vpn0_next_hop_ip_address_3	
VPN0 interface Cellular: IPSec preference is set to default value 0, while wired interface preference is set higher. Internet tunnel will be preferred. Shaping rate is defined as 10Mbps for this interface. This value should be configured according to service provider offered upstream bandwidth.		
Basic Configuration	vpn0_cell1_int_shutdown	FALSE
Tunnel>Advanced Options>Encapsulation	vpn0_cell0_1_0_tunnel_ipsec_preference	0
ACL	vpn_cell1_qos_shaping-rate	10000
VPN0 interface INET: IPSec preference set to 100, Internet will be the preferred transport. Shaping rate is defined as 100Mbps for this interface. This value should be configured according to service provider offered upstream bandwidth.		
Basic Configuration	vpn0_inet_int_shutdown	FALSE
Device Specific	vpn0_inet_tunnel_ipsec_preference	100
ACL/QoS	vpn_inet_qos_shaping-rate	100000
VPN Interface SVI 1(VPN 1): VRRP values are left blank since there is no VRRP on this location		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	Vlan13
	vpn_svi_if_description_SVI_1	Shared Services
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.13.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4

Device Template Values for IR1101_INET_and_CELL

VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
DHCP (VPN1-SVI1): DHCP server for VPN1 SVI1 network		
Basic Configuration	voice_dhcp_addr_pool maskbits	10.12.13.0/24
Basic Configuration	voice_dhcp_addr_exclude_range	10.12.13.1-10.12.13.20,10.12.13.100-10.12.13.155
Advanced	dhcp_default_gateway	10.12.13.1
VPN Interface SVI 1 (VPN 10): VRRP values are left blank since there is no VRRP on this location		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	vlan113
	vpn_svi_if_description_SVI_1	Video
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.113.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
DHCP (VPN10-SVI1): DHCP server for VPN10 SVI1 network		
Basic Configuration	voice_dhcp_addr_pool maskbits	10.12.113.0/24
Basic Configuration	voice_dhcp_addr_exclude_range	10.12.113.1-10.12.113.20,10.12.113.100-10.12.113.155
Advanced	dhcp_default_gateway	10.12.113.1
VPN Interface SVI 1 (VPN 11): VRRP values are left blank since there is no VRRP on this location		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	vlan213
	vpn_svi_if_description_SVI_1	Employee voice
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.213.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
VPN Interface SVI 2(VPN 11): Second SVI for a service VPN is created in this template. VRRP values are left blank since there is no VRRP on this location.		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_2	vlan233
	vpn_svi_if_description_SVI_2	Employee Data
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_2	10.12.233.1/24
	vpn_svi_dhcp_helper_SVI_2	10.22.2.4

Device Template Values for IR1101_DUAL_CELL_EM

VRRP	vpn_if_vrrp_grpid_2	
	vpn_if_vrrp_priority_2	
	vpn_if_vrrp_track_prefix_list_2	
	vpn_if_vrrp_vrrp_ipaddress_2	
VPN Interface Ethernet (Loopback0)		
IPv4 Configuration	lo0_int_ip_addr maskbits	2.2.0.13/32
Switchport		
Interface 1 (FE0/0/1)	switchport_1_if_shutdown	FALSE
	switchport_1_if_access_vlan	13
Interface 2 (FE0/0/2)	switchport_2_if_shutdown	FALSE
	switchport_2_if_access_vlan	113
Interface 3 (FE0/0/3)	switchport_3_if_shutdown	FALSE
	switchport_3_if_access_vlan	213
Interface 4 (FE0/0/4)	switchport_4_if_shutdown	FALSE
	switchport_4_if_access_vlan	233
SNMP		
Basic Configuration	snmp_shutdown	FALSE
	snmp_device_name	IR1101-Location-1
	snmp_device_location	Acadia
Cellular Profile: required for non-default APNs. Original profile 1 is overwritten with new APN value.		
Basic Configuration	cellular_profile_profile_id	1
	cellular_profile_apn	globaldata.net

Device Template Values for IR1101_DUAL_CELL_EM

IR1101 on Remote Location 4 uses device template Name: IR1101_DUAL_CELL_EM, the following table contains a list of variables on the template and some example values used on the implementation.

Table 50 Device Template Values for IR1101_DUAL_CELL_EM

Section	Variable	IR1101-Location-1
System: variables contain device specific settings. From this template, it is possible to configure baud rate for console connection.		
Basic Configuration	system_site_id	10010212
	system_system_ip	2.2.0.12
	system_hostname	IR1101-Location-4
	system_device_groups	RL,IR1101,US,L4
	system_console_baud_rate	9600
GPS	system_latitude	47.82
	system_longitude	-123.78
Advanced	system_port_hop	FALSE

Device Template Values for IR1101_DUAL_CELL_EM

	system_port_offset	0
VPN0: two default routes are defined, one for each WAN interface		
IPv4 Route (1)	vpn0_next_hop_ip_address_1	Cellular0/1/0
IPv4 Route (2)	vpn_ipv4_ip_prefix2	0.0.0.0/0
	vpn0_next_hop_ip_address_2	Cellular0/3/0
IPv4 Route (3)	vpn_ipv4_ip_prefix3	
	vpn0_next_hop_ip_address_3	
VPN0 interface Cellular: IPSec preference is set to default value 0 on both cellular interfaces, in this case load will be shared on both tunnels. Shaping rate is defined as 10Mbps for this interface, this value should be configured according to service provider offered upstream bandwidth.		
Basic Configuration	vpn0_cell1_int_shutdown	FALSE
Tunnel>Advanced Options>Encapsulation	vpn0_cell0_3_0_tunnel_ipsec_preference	0
ACL	vpn_cell3_qos_shaping-rate	10000
VPN0 interface Cellular Expansion Module: IPSec preference is set to default value 0 on both cellular interfaces, in this case load will be shared on both tunnels. Shaping rate is defined as 10Mbps for this interface, this value should be configured according to service provider offered upstream bandwidth.		
Basic Configuration	vpn0_cell3_int_shutdown	FALSE
Tunnel>Advanced Options>Encapsulation	vpn0_cell0_1_0_tunnel_ipsec_preference	0
ACL	vpn_cell1_qos_shaping-rate	10000
VPN Interface SVI 1 (VPN 1): VRRP values are left blank since there is no VRRP on this location		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	vlan12
	vpn_svi_if_description_SVI_1	Shared Services
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.12.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
VPN Interface SVI 1 (VPN 10): VRRP values are left blank since there is no VRRP on this location		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	vlan112
	vpn_svi_if_description_SVI_1	security
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.112.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
VPN Interface SVI 1 (VPN 11): VRRP values are left blank since there is no VRRP on this location		

Device Template Values for IR1101_DUAL_CELL_EM

Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_1	vlan212
	vpn_svi_if_description_SVI_1	employee data
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.212.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1	
	vpn_if_vrrp_priority_1	
	vpn_if_vrrp_track_prefix_list_1	
	vpn_if_vrrp_vrrp_ipaddress_1	
VPN Interface SVI 2(VPN 11): Second SVI for a service VPN is created in this template. VRRP values are left blank since there is no VRRP on this location.		
Basic Configuration	vpn_service_svi_shutdown	FALSE
	vpn_svi_if_name_SVI_2	vlan232
	vpn_svi_if_description_SVI_2	employee voice
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_2	10.12.232.1/24
	vpn_svi_dhcp_helper_SVI_2	10.22.2.4
VRRP	vpn_if_vrrp_grpid_2	
	vpn_if_vrrp_priority_2	
	vpn_if_vrrp_track_prefix_list_2	
	vpn_if_vrrp_vrrp_ipaddress_2	
VPN Interface Ethernet (Loopback0)		
IPv4 Configuration	lo0_int_ip_addr maskbits	2.2.0.12/32
Switchport: this template has 4 Fast Ethernet ports configured for access and one Gigabit ethernet port configured as trunk.		
Interface 1 (FE0/0/1)	switchport_1_if_shutdown	FALSE
	switchport_1_if_access_vlan	12
Interface 2 (FE0/0/2)	switchport_2_if_shutdown	FALSE
	switchport_2_if_access_vlan	112
Interface 3 (FE0/0/3)	switchport_3_if_shutdown	FALSE
	switchport_3_if_access_vlan	212
Interface 4 (FE0/0/4)	switchport_4_if_shutdown	FALSE
	switchport_4_if_access_vlan	232
Interface 5 (Gi0/0/5)	switchport_5_if_shutdown	FALSE
	switchport_5_if_trunk_allowed_vlans	1,12,112,212,232
SNMP		
Basic Configuration	snmp_shutdown	FALSE
	snmp_device_name	IR1101-Location-4
	snmp_device_location	Olympic

Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK

One Cisco IR1101 on Remote Location 3 uses device template Name: IR1101_CELL_OSPF_with_TRUNK, the other device uses IR1101_INET_OSPF_with_TRUNK. Following table contains a list of variables on the template and some example values used on the implementation.

Table 51 Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK

Section	Variable	IR1101-Location3-1 IR1101_INET_OSPF_with_T RUNK	IR1101-Location3-2 IR1101_CELL_OSPF_ with_TRUNK
System: variables contain device specific settings. From this template, it is possible to configure baud rate for console connection.			
Basic Configuration	system_site_id	10010317	10010318
	system_system_ip	2.2.0.117	2.2.0.118
	system_hostname	IR1101-Location3-1	IR1101-Location3-2
	system_device_groups	RL,IR1101,US,L3	RL,IR1101,US,L3
	system_console_baud_rate	9600	9600
GPS	system_latitude	47.82	47.82
	system_longitude	-123.78	-123.78
Advanced	system_port_hop	FALSE	FALSE
	system_port_offset	0	0
VPN0: one default routes per device for the single transit			
IPv4 Route (1)	vpn0_next_hop_ip_address_1	GigabitEthernet0/0/0	Cellular0/1/0
IPv4 Route (2)	vpn_ipv4_ip_prefix2		
	vpn0_next_hop_ip_address_2		
IPv4 Route (3)	vpn_ipv4_ip_prefix3		
	vpn0_next_hop_ip_address_3		
VPN0 interface Cellular: Only present on second device. Shaping rate set to 10Mbps, this value should be configured according to service provider offered upstream bandwidth. Preference is set to a lower number than WAN interface in the peer router to meet traffic symmetry requirement for DPI.			
Basic Configuration	vpn0_cell1_int_shutdown		FALSE
Tunnel>Advanced Options>Encapsulation	vpn0_cell0_3_0_tunnel_ipsec_pre ference		0
ACL	vpn_cell3_qos_shaping-rate		10000
VPN0 interface INET: Only present on first device. Shaping rate set to 100Mbps, this value should be configured according to service provider offered upstream bandwidth. Preference is set to a higher number than WAN interface in the peer router to meet traffic symmetry requirement for DPI.			
Basic Configuration	vpn0_inet_int_shutdown	FALSE	
Device Specific	vpn0_inet_tunnel_ipsec_preferenc e	100	
ACL/QoS	vpn_inet_qos_shaping-rate	100000	
VPN Interface SVI 1(VPN 1): VRRP values are left blank since there is no VRRP on this location.			
Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan17	vlan18
	vpn_svi_if_description_SVI_1	Shared Services	Shared Services

Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK

IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.17.1/24	10.12.18.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1		
	vpn_if_vrrp_priority_1		
	vpn_if_vrrp_track_prefix_list_1		
	vpn_if_vrrp_vrrp_ipaddress_1		
OSPF (VPN 1): Both routers advertise same networks but OSPF metric will be different depending on the associated local policy. Router with higher preference is assigned localized policy OSPF_EDGE_PREFER for a metric of 10, the other router is assigned localized policy OSPF_EDGE_SEC for a metric of 20. Metrics are assigned for traffic symmetry required for DPI			
Basic Configuration	ospf_router_id	2.2.0.117	2.2.0.118
	ospf_redistribute_route_policy	OSPF_EDGE_PREFER	OSPF_EDGE_SEC
Area	ospf_area_a_num	1	1
	ospf_name_iface	vlan17	vlan18
	ospf_area_range_address_0	10.22.2.0/24	10.22.2.0/24
VPN Interface SVI 1 (VPN 10): VRRP values are left blank since there is no VRRP on this location			
Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan117	vlan118
	vpn_svi_if_description_SVI_1	security	security
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.117.1/24	10.12.118.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1		
	vpn_if_vrrp_priority_1		
	vpn_if_vrrp_track_prefix_list_1		
	vpn_if_vrrp_vrrp_ipaddress_1		
OSPF (VPN 10): Both routers advertise same networks but OSPF metric will be different depending on the associated local policy. Router with higher preference is assigned localized policy OSPF_EDGE_PREFER for a metric of 10, the other router is assigned localized policy OSPF_EDGE_SEC for a metric of 20. Metrics are assigned for traffic symmetry required for DPI			
Basic Configuration	ospf_router_id	10.12.117.2	10.12.118.2
	ospf_redistribute_route_policy	OSPF_EDGE_PREFER	OSPF_EDGE_SEC
Area	ospf_area_a_num	10	10
	ospf_name_iface	vlan116	vlan116
	ospf_area_range_address_0	10.22.10.0/24	10.22.10.0/24
VPN Interface SVI 1 (VPN 11): VRRP values are left blank since there is no VRRP on this location			
Basic Configuration	vpn_service_svi_shutdown	FALSE	FALSE
	vpn_svi_if_name_SVI_1	vlan217	vlan218
	vpn_svi_if_description_SVI_1	employee data	employee data
IPv4 Configuration	vpn_if_svi_if_ipv4_prefix_SVI_1	10.12.217.1/24	10.12.218.1/24
	vpn_svi_dhcp_helper_SVI_1	10.22.2.4	10.22.2.4
VRRP	vpn_if_vrrp_grpid_1		
	vpn_if_vrrp_priority_1		
	vpn_if_vrrp_track_prefix_list_1		

Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK

	vpn_if_vrrp_vrrp_ipaddress_1		
OSPF (VPN 11): Both routers advertise same networks but OSPF metric will be different depending on the associated local policy. Router with higher preference is assigned localized policy OSPF_EDGE_PREFER for a metric of 10, the other router is assigned localized policy OSPF_EDGE_SEC for a metric of 20. Metrics are assigned for traffic symmetry required for DPI			
Basic Configuration	ospf_router_id	10.12.217.2	10.12.218.2
	ospf_redistribute_route_policy	OSPF_EDGE_PREFER	OSPF_EDGE_SEC
Area	ospf_area_a_num	11	11
	ospf_name_iface	vlan216	vlan218
	ospf_area_range_address_0	10.22.11.0/24	10.22.11.0/24
VPN Interface Ethernet (Loopback0)			
IPv4 Configuration	lo0_int_ip_addr maskbits	2.2.0.117/32	2.2.0.118/32
Switchport: Interface Fast Ethernet 0/0/1 is a trunk interface to be connected to Cisco IE switch. Other interfaces are access only to connect end devices.			
Interface 1 (FE0/0/1)	switchport_1_if_shutdown	FALSE	FALSE
	switchport_1_if_trunk_allowed_vlans	1,17,117,217,237	1,18,118,218,238
Interface 2 (FE0/0/2)	switchport_2_if_shutdown	FALSE	
	switchport_2_if_access_vlan	117	118
Interface 3 (FE0/0/3)	switchport_3_if_shutdown	FALSE	
	switchport_3_if_access_vlan	217	218
Interface 4 (FE0/0/4)	switchport_4_if_shutdown	FALSE	
	switchport_4_if_access_vlan	17	18
SNMP			
Basic Configuration	snmp_shutdown	FALSE	FALSE
	snmp_device_name	IR1101-Location3-1	IR1101-Location3-2
	snmp_device_location	Olympic	Olympic

Device Template Values for IR1101_CELL_OSPF_with_TRUNK and IR1101_INET_OSPF_with_TRUNK