IoT Industrial Router Design Guide Extension to SD-WAN Small Branch Design Case Study

First Published: 2023-05-01

Last Modified: 2023-05-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Introduction

The Cisco SD-WAN solution can be extended beyond carpeted, air-conditioned spaces typical of traditional enterprise branches, offices, and datacenters. The Cisco current industrial Internet of Things (IoT) routing portfolio is compatible with Cisco vManage and can be used to extend the enterprise network into remote locations to meet the needs of various industrial use cases. Transportation, energy generation and distribution, remote site monitoring, and many more industries each have their own unique requirements and conditions that must be evaluated carefully when designing a secure, resilient, and manageable network.

Scope of Document

This document builds on the foundational information in the Cisco SD-WAN Small Branch Design Case Study which describes how the Cisco SD-WAN solution including Cisco vManage is designed and built using many of the commonly-supported features. In this document, the Cisco Industrial IoT routing portfolio is introduced and the available supported SD-WAN features on the IoT platforms are described. Test configurations for select features are also provided as examples. Application of specific hardware and features to meet the needs of individual IoT use cases are discussed in other documents.

This document was written based on software versions 17.10.1 for IOS-XE, and 20.10 for vManage.

Intended Audience

This document is intended for IT architects and engineers that already have some familiarity with Cisco SD-WAN including vManage and are interested in understanding how the technology can be extended beyond typical carpeted spaces such as offices and data centers.

Cisco Industrial Routing Portfolio for SD-WAN

The following table outlines the key capabilities of three of the latest entries in the Cisco Industrial IoT routing portfolio, the IR1101, IR1800, and IR8300 series, which are enabled to operate in SD-WAN mode, managed by vManage.

Table 1: Industrial Router Options Specifications

	Catalyst IR1101 Rugged Series Router	Catalyst IR1800 Rugged Series Router	Catalyst IR8300 Rugged Series Router
Available Base Router PIDs	IR1101-K9 IR1101-A-K9	IR1821-K9 IR1831-K9 IR1833-K9 IR1835-K9	IR8340-K9

	Catalyst IR1101 Rugged Series Router	Catalyst IR1800 Rugged Series Router	Catalyst IR8300 Rugged Series Router
Key Features	Highly modular design: • DIN rail mount • Wall mount • Panel mount • Modular LTE and 5G • SCADA integration • SD-WAN ready • Powered by IOS-XE	Modular design with mobile features: • Din rail mounting • Wall mounting • Panel mounting • Ignition power management • Modular LTE and 5G • SCADA integration • Automotive certifications • SD-WAN ready • Powered by Cisco IOS-XE	Industrial-grade fully integrated routing and switching platform: • Rack mount • Precision timing module • Energy industry certifications • Modular LTE and 5G • SD-WAN ready • Powered by Cisco IOS-XE
Ports and Backhaul	• Four FastEthernet switchports • WAN SFP (DSL or GigabitEthernet) • One serial port (RS232 DTE) • Single and Dual Cellular, as well as Dual SIM	• Four GigabitEthernet switchports with PoE+ • WAN SFP (DSL or GigabitEthernet) • 1 or 2 serial ports (RS232 or RS232/RS485) • Single and Dual Cellular, as well as Dual SIM	• 2 combination (RJ45/SFP) GigabitEthernet WAN • 12 GE LAN ports (4 each RJ45, combo, SFP) • 2 NIM slots (2 port T1E1, 8 port RS232) • GNSS/PTP/ IRIG-B/TOD timing

	Catalyst IR1101 Rugged Series Router	Catalyst IR1800 Rugged Series Router	Catalyst IR8300 Rugged Series Router
Expansion Modules	IRM-1100-SP • Second SFP GE WAN • Second PIM slot for cellular modem, etc. IRM-1100-4A2T • 2 x GE LAN • 4 x Async serial (RS232/485/422) IRM-1100-SPMI • GPIO • Second SFP GE WAN • Second PIM slot for cellular modem, etc. • mSATA slot for up to 100GB storage	N/A	N/A
Wi-Fi	N/A	WP-WIFI6 • 802.11ax • 2x2 uplink/downlink MIMO 2 spatial streams • PHY rate up to 1.488 Gbps • WPA3	N/A

	Catalyst IR1101 Rugged Series Router	Catalyst IR1800 Rugged Series Router	Catalyst IR8300 Rugged Series Router
CPU, Memory, Edge Compute	ARM64 4-core 600 MHz 4GB RAM 862MB RAM for IOx	IR1821, IR1831, IR1833: • ARM64 4-core 600 MHz • 4GB RAM • 862MB RAM for IOx IR1835: • ARM64 4-core 1.2GHz • 8GB RAM • 1724MB RAM for IOx	8-core x86 Intel Atom 8GB RAM
Power Consumption	6.6W-12W for base router, +10W for expansion module and extra modem	16W-27W, up to 71W with PoE load	60W-80W for base router, +6W-7W for additional NIM module
OTHER FEATURES			
Dimensions	2.36 in. x 5.22 in. x 4.92 in. (60 x 132.5 x 124.9 mm) for base router	2.20 x 11.04 x 8.06 in. (55.9 x 280.4 x 204.7 mm)	3.5 x 17.25 x 15 in. (88.9 x 438.2 x 381 mm)

Additional details for each of the three routers are available in the product datasheets:

Catalyst IR1101 Series Rugged Datasheet: https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html

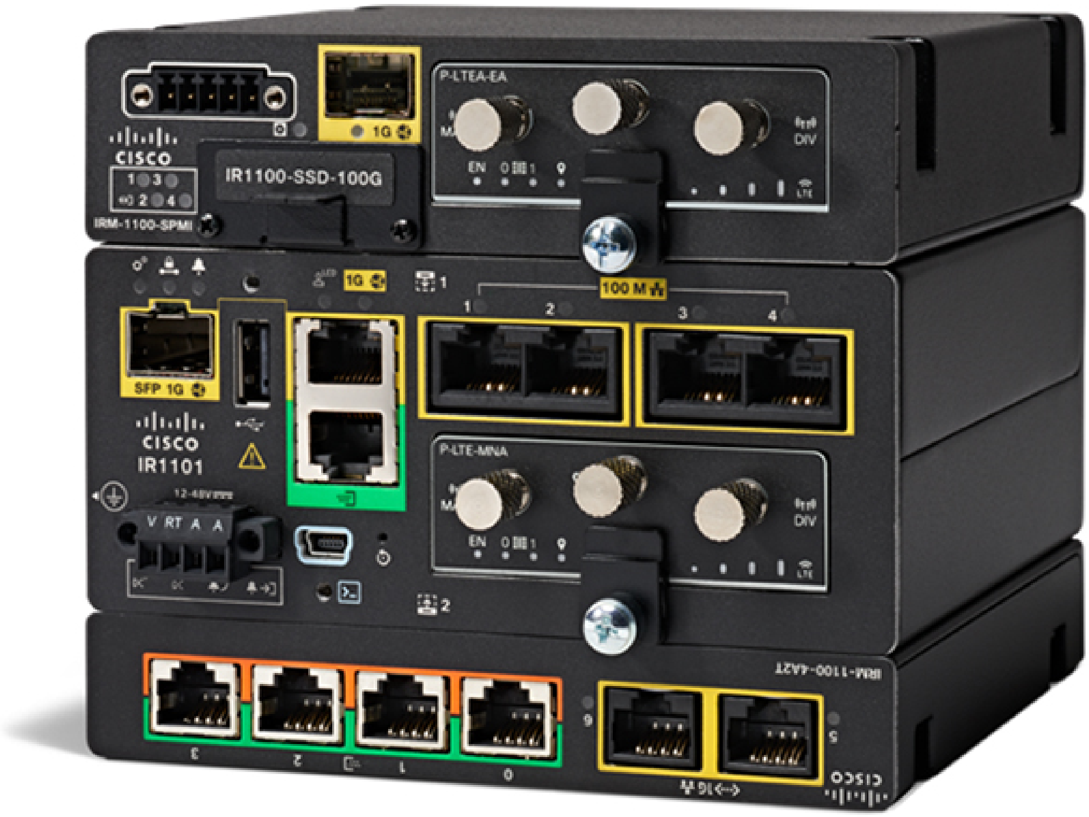
Catalyst IR1800 Series Rugged Datasheet: https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir1800-rugged-series-routers/nb-06-cat-ir1800-rugged-ser-rout-ds-cte-en.html

Catalyst IR8300 Series Rugged Datasheet: https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-ir8300-rugged-series-router/nb-06-cat-ir8340-rugged-ser-rout-ds-cte-en.html

Cisco Catalyst IR1101 Rugged Series Routers

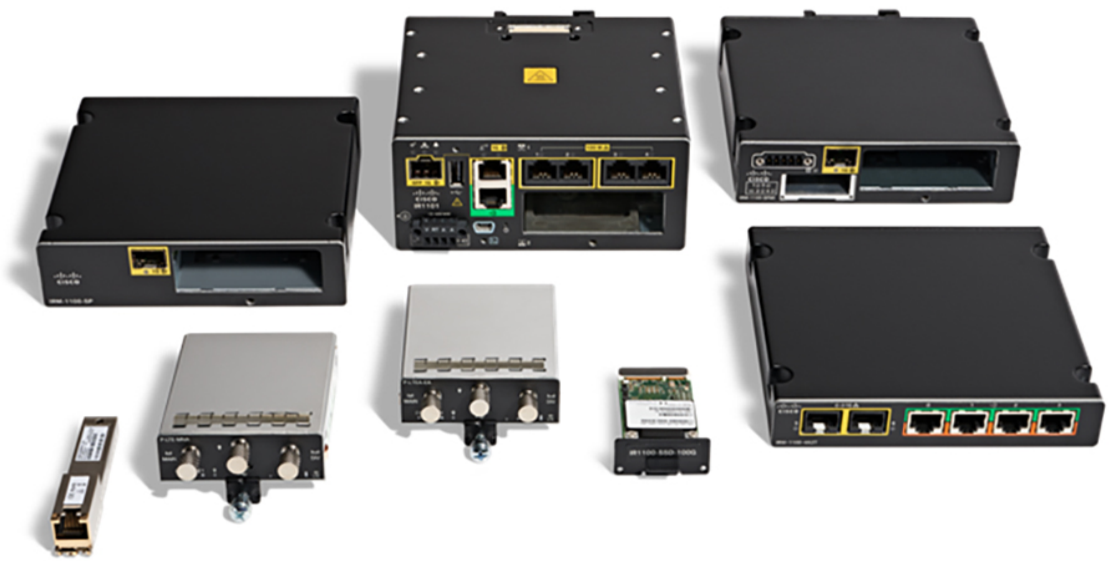
The Cisco Catalyst IR1101 Rugged Series of routers provides a compact, modular platform based on Cisco IOS-XE and 4GB of RAM. Despite its low power utilization, modular interfaces provide a variety of connectivity options for both the WAN and the LAN. The IR1101 is targeted at use cases including connected roadways and intersections, utility grids, public safety, oil and gas pipelines, and kiosks.

Figure 1: Cisco IR1101



Available interfaces and modules expand the core capabilities of the router to add solid state storage, DSL, two cellular interfaces (including 4G LTE and 5G), serial ports, additional ethernet ports, and GPIO.

Figure 2: Cisco IR1101 Available Hardware



Cisco Catalyst IR1800 Rugged Series Routers

The Cisco Catalyst IR1800 Rugged Series provides an ideal platform for in-vehicle deployments in fleets, mass-transit, and similar use cases. Modularity enables up to two simultaneous 5G cellular connections for maximum performance that can be extended to local devices connected via serial, ethernet, or even Wi-Fi6 via a built-in access point. The IR1800 series also runs Cisco IOS-XE and comes in two performance levels. The IR1821, IR1831, and IR1833 feature 4GB of RAM, and the IR1835 features 8GB of RAM and a faster processor. Additional capabilities include an optional dead-reckoning module for location tracking even when GPS satellite signal is lost, and IOx for edge compute.

Figure 3: Cisco IR1835 Rear View of Cellular and Wi-Fi Modules

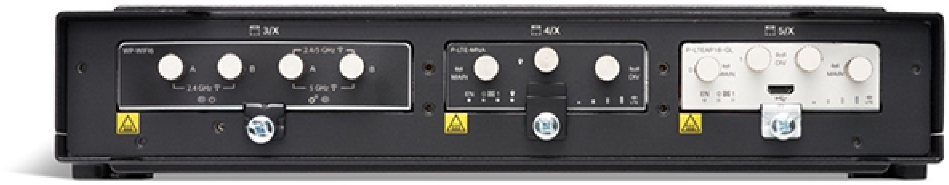
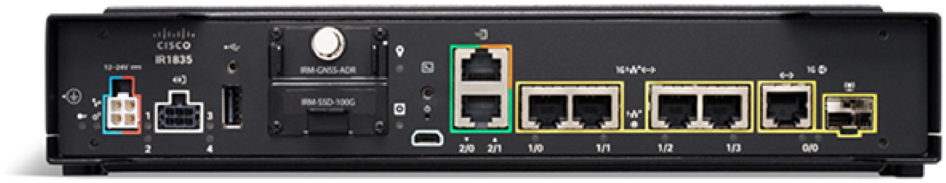


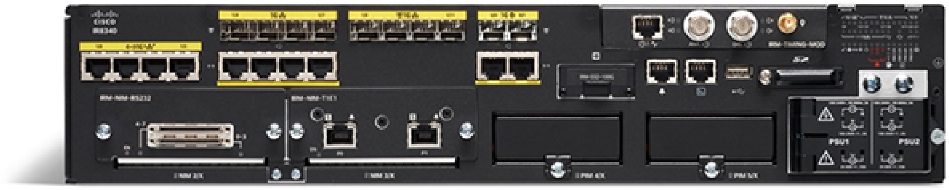
Figure 4: Cisco IR1835 Front View



Cisco Catalyst IR8300 Rugged Series Router

The Catalyst IR8300 Rugged Series router is highest performance router in the IoT portfolio. With expansive connectivity options through its modular architecture, as well as a precision time source, and industry certifications it is the ideal choice for a utilities deployments of distribution automation.

Figure 5: Cisco IR8340 Front View



Cisco IOS-XE and Two Execution Modes

The three routers discussed in this document (IR1101, IR1800, IR8340) all run the Cisco IOS-XE operating system. In these platforms, the operation system can be booted in either Autonomous mode, or Controller mode. To work with the Cisco SD-WAN solution, the router runs in Controller mode. The table below, taken from the Cisco SD-WAN Getting Started Guide, outlines the key differences between the two modes.

Table 2: Autonomous and Controller Mode Comparison

Feature	Autonomous Mode	Controller Mode
Configuration Method	• Command Line Interface (CLI) • NETCONF	
Onboarding Modes	• Plug and Play • Config-Wizard • WebUI • Bootstrap (USB, bootflash, and so on) • Auto-Install (Python Script, TCL Script) • ZTP (Using DHCP Option 150 and Option 67)	• Plug and Play • Bootstrap (USB, bootflash, and so on)
Licensing	Cisco Smart Licensing	Cisco High Performance Security (HSEC) software licensing. No device licensing.
Image Type	Universalk9	Universalk9
Dual-IOSd redundancy model	Supported	Not Supported
High Availability	Supported	Not Supported
Global configuration mode	Configure Terminal	Config-transaction

Overview of applicable and available feature templates

Cisco vManage leverages template-based configuration to ensure consistency across potentially many routers with similar configuration requirements, and aids in the ease of deployment. Feature templates provide the mechanism for configuring most capabilities on SD-WAN routers including the industrial routers for IoT use cases. These feature templates are subsequently grouped together in a Device Template that is specific to a hardware model (such as the IR1835) and then applied to one or more devices of that type that need a common configuration. The single device template (and its constituent feature templates) applied to the router(s) can be created with some degree of flexibility allowing the user to insert unique values, like an IP address or site ID, for each individual device.

The table below lists the available feature templates for the IR1101, IR1800, and IR8340 routers as of the vManage 20.10 release. The subsequent sections of this document describe many of the features in more detail, especially those with greater relevance in IoT use cases.

Table 3: Available Feature Templates for IR1101, IR1800, IR8340

Available Feature Templates (GUI Based)	IR1101	IR1800	IR8340
Cisco AAA	X	X	X
Cisco BFD	X	X	X
Cisco NTP	X	X	X
Cisco OMP	X	X	X
Cisco Security	X	X	X
Cisco System	X	X	X
Global Settings	X	X	X
Security App Hosting			X
Cisco Secure Internet Gateway (SIG)	X	X	X
Cisco VPN	X	X	X
Cisco VPN Interface Ethernet	X	X	X
Cisco VPN Interface GRE	X	X	X
Cisco VPN Interface IPsec	X	X	X
VPN Interface Cellular	X	X	X
VPN Interface Ethernet PPPoE	X	X	
VPN Interface Multilink	X	X	
VPN Interface SVI	X	X	
Cellular Controller	X	X	X
Cellular Profile	X	X	X
Cisco Banner	X	X	X
Cisco BGP	X	X	X
Cisco DHCP Server	X	X	X
Cisco IGMP	X	X	X
Cisco Logging	X	X	X

Available Feature Templates (GUI Based)	IR1101	IR1800	IR8340
Cisco Multicast	X	X	X
Cisco OSPF	X	X	X
Cisco OSPFv3	X	X	X
Cisco PIM	X	X	X
Cisco SNMP	X	X	X
CLI Add-On Template	X	X	X
EIGRP	X	X	X
GPS	X	X	X
Probes	X	X	
Switch Port	X	X	X
TrustSec	X	X	X
ISR1K/IR18 Wireless		X	

Expanding Capability Using CLI Templates

One special type of feature template is the CLI Add-on template. This unique feature template allows a user to enter text configuration commands to enable functionality that is supported on the platform, but no GUI-based feature template has been developed yet.

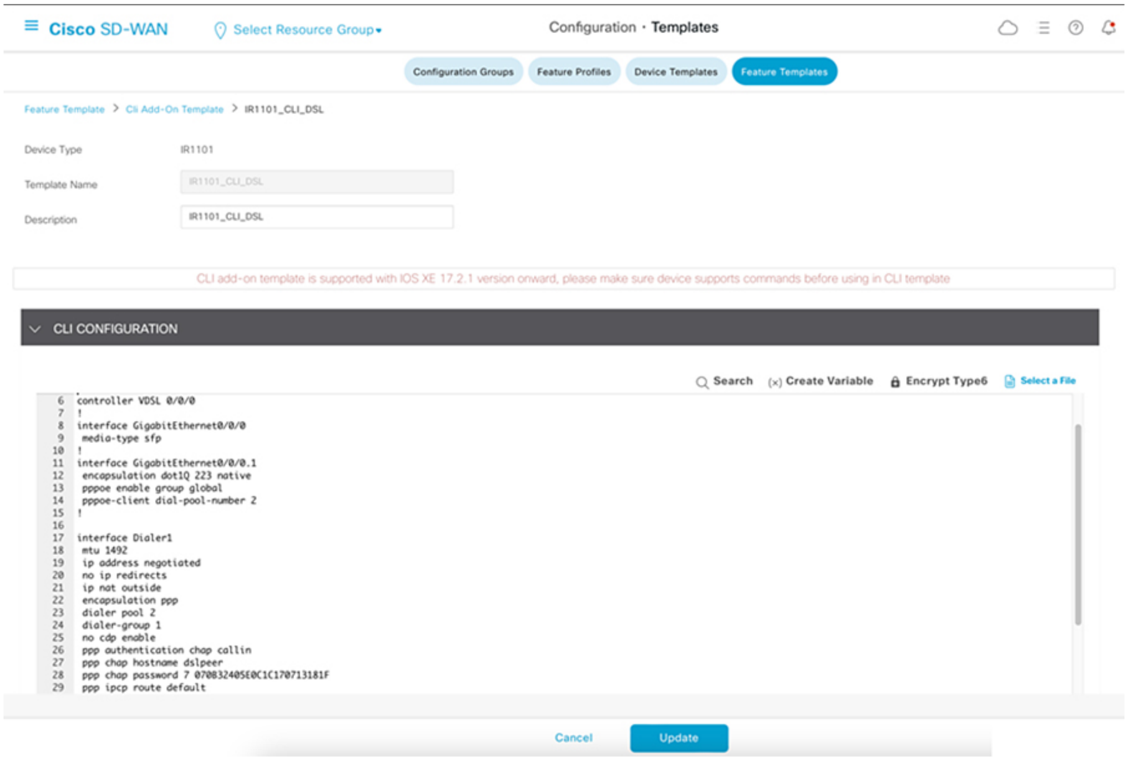
Because only one CLI Add-on template can be selected in the Device Template, if multiple features are required, they will need to be concatenated in a single CLI template. For users with Cisco IOS command line experience, this will be familiar.

Supported IoT related features enabled through CLI Add-on template, as of Cisco vManage version 20.10 include:

- DSL
- Ignition sense and Ignition power management
- 802.1x for LAN clients
- IOx Local Manager
- SCADA Serial Raw Socket Encapsulation
- GPIO

The Configuration section includes example CLI templates for these IoT-centric features.

Figure 6: Example of CLI Add-on Feature Template



Device Type IR1101

Template Name IR1101_CLI_DSL

Description IR1101_CLI_DSL

CLI add-on template is supported with IOS XE 17.2.1 version onward, please make sure device supports commands before using in CLI template

```
controller VDSL 0/0/0
!
interface GigabitEthernet0/0/0
 media-type sfp
!
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 223 native
 pppoe enable group global
 pppoe-client dial-pool-number 2
!

interface Dialer1
 mtu 1492
 ip address negotiated
 no ip redirects
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dslpeer
 ppp chap password 7 070B32405E0C1C170713181F
 ppp ipcp route default
```

Note: In vManage version 20.10 and IOS-XE version 17.10.1, there is an issue that requires a simple CLI Add-on template always be added to the device template for IR1101, IR1800, IR8300 to prevent an error from being generated when attaching the template to a device. The required configuration lines look like the following, but the actual interface numbering may vary based on the specific hardware platform. This will be fixed in a future release.

```
!
line 0/0/0
line 0/2/0
!
```

CHAPTER 2

IoT features for SD-WAN

This section describes some of the key IoT related features available in Cisco SD-WAN based on Cisco vManage. It includes limitations and best practices to be aware of during design and implementation. Specific recommendations of how to piece together different features to achieve individual IoT use cases are beyond the scope of this document.

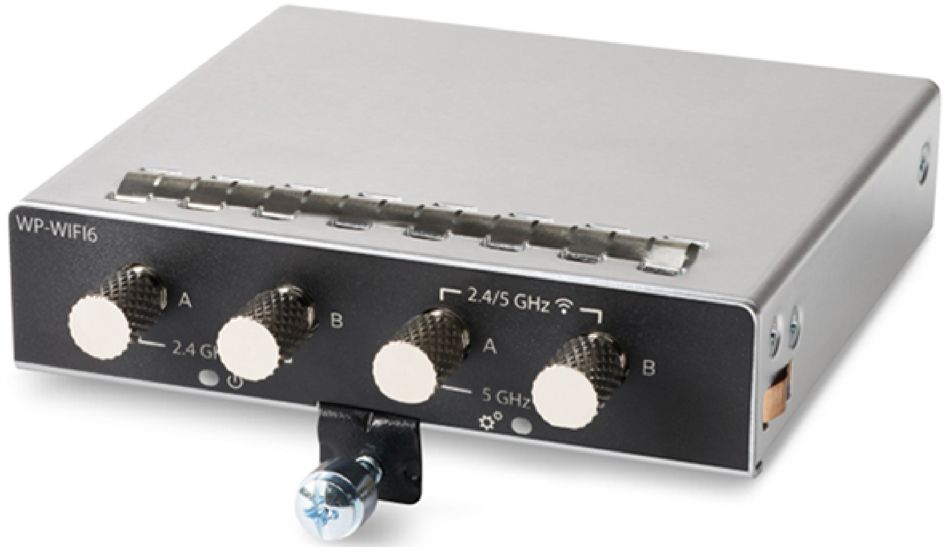
Wi-Fi

Currently in the IoT routing portfolio compatible with Cisco vManage, only the IR1800 series includes Wi-Fi capabilities. The IR1800 series supports a Wi-Fi-6 module with 2x2 MIMO and 2 spatial streams based on the Cisco 9105AXI access point. When the router is running in non-SD-WAN mode, the access point can be configured to be managed by a traditional wireless controller like a Cisco 9800, or it can be configured to act as a standalone Workgroup Bridge (WGB) for an additional WAN interface.

Alternatively, in Embedded Wireless Controller (EWC) mode the access point registers to an integrated controller running locally on the same module that operates as a wireless hotspot. Of these three modes (controller based, WGB, and EWC hotspot), currently only the EWC hotspot mode is supported when the router is managed by the vManage SD-WAN controller. CLI Add-on template configuration is not support for the access point, which has its own CLI separate from the router.

Feature template support for the wireless module in the IR1800 includes the ability to configure multiple SSIDs, each with authentication types including WPA2 Personal, WPA2 Enterprise, or open and traffic can be associated with a VLAN that terminates on the IR1800 – typically within a Service VPN. Captive portal-based authentication is not currently supported. The two radios (2.4 GHz and 5 GHz) can be independently enabled or disabled.

Figure 7: WP-WiFi6 Module for IR1800 Series Routers



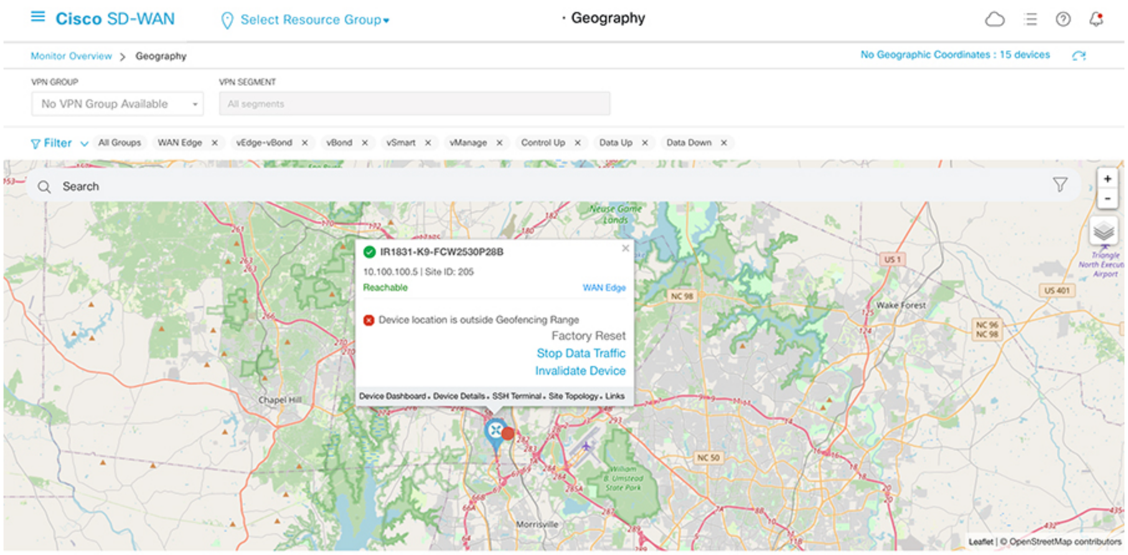
Location Tracking and Geofencing

The IoT routers equipped with supported cellular modems can be configured as GPS receivers. The GPS signal will allow the router to be located geographically based on latitude and longitude coordinates. This location can subsequently be shared with vManage and plotted on a map that is pulled from Google Maps via API. The reported location will be updated every few minutes.

Cisco vManage can also utilize a geofence around a specific location (either manually defined, or automatically detected by the router). If the router detects that it is outside the geofence area (in the shape of a circle, 100m to 10km radius around the router), it can be set to trigger an alert on the dashboard or send an SMS message. From the dashboard, if a router leaves the geofence, the administrator can quickly and easily act by disabling data traffic or even invalidating the device certificate.

At this time, only the cellular modem GPS receiver can be used as the source for mapping and geofencing within the vManage dashboard. Either the cellular modem or the dead reckoning module can be configured with a CLI template to send a NMEA stream to a specified IP address and port number to be processed further, however it is not possible to associate the NMEA stream with a particular Service VPN, therefore the destination needs to be reachable within VPN0.

Figure 8: Cisco IR1831 location detected outside of geofence



IR1831-K9-FCW2530P28B
10.100.100.5 | Site ID: 205
Reachable
WAN Edge

Device location is outside Geofencing Range

Cellular Airtime Optimization Options and Design Guidance

Cellular networks excel in providing WAN connectivity in remote deployments where a wired connection is not feasible and can greatly speed up the roll out of new remote sites or branches. However, these and other advantages do come with a cost. Often cellular connections come with a data cap per month, or expensive overage charges if the cap is exceeded. When paired with potentially hundreds or thousands of cellular connected devices, the costs can add up quickly.

With all default settings, a cellular-connected IR1101 managed by vManage can produce over 15 GB per month of management traffic. This overhead includes things like frequent verbose statistics monitoring, frequent connection monitoring to all spoke routers in the mesh network, and DTLS sessions with the vBond and vSmart controllers. While in a wired environment these settings provide great visibility and performance for the network, they may not be ideal for data-limited cellular deployments. It is possible to reduce this overhead through configuration.

Table 4: SD-WAN Management Data Overhead with Default Settings

TYPE OF DATA	24 HOUR PERIOD	30 DAY PERIOD
VMANAGE STATISTICS MONITORING	244 MB	7.3 GB
BFD SESSIONS	201 MB	6 GB
*** DTLS SESSION WITH VBOND**	40 MB	1.2 GB
DTLS SESSION WITH SINGLE VSMART	35 MB	1 GB
TOTAL	520 MB	15.6 GB

After tweaking some of the parameters as subsequently described, the bandwidth utilization can be **reduced** by over 50%. It is possible to reduce the bandwidth even more, based on the actual requirements and settings.

Table 5: Bandwidth Utilization Affecting Settings – Default and Modified

SETTING	DEFAULT VALUE	MODIFIED VALUE
STATISTICS BEING MONITORED	All	Only “Device Health” and “Device System Status” enabled
STATISTICS MONITORING INTERVAL	30 minutes	60 minutes
BFD INTERVAL	1 second	10 seconds
TUNNEL TOPOLOGY	Full mesh (9 spokes)	Hub and spoke

Table 6: SD-WAN Management Data Overhead with Modified Settings

TYPE OF DATA	24 HOUR PERIOD	30 DAY PERIOD
VMANAGE STATISTICS MONITORING	128 MB	2.8 GB
BFD SESSIONS	6 MB	180 MB
*** DTLS SESSION WITH VBOND**	40MB	1.2 GB
DTLS SESSION WITH VSMART	34 MB	1 GB
TOTAL	208 MB	5.2 GB

***Note:** The testing result for “DTLS session with vBond” is based on a lab setup with a single vSmart controller. When combined with a default setting of 2 for “max-control-connections”, the edge router did not reach steady state with vBond. If the number of vSmarts was increased to 2 (or more), it would be expected that the data utilization from edge to vBond would be negligible.

AVAILABLE OPTIONS FOR REDUCING BANDWIDTH UTILIZATION

Monitoring

By default, all statistics monitoring is enabled in vManage for each edge router. The statistics will be gathered every 30 minutes.

To reduce data usage, the collection interval can be increased from the default of 30 minutes. The specific type of statistics can also be adjusted on a granular basis for individual or all devices.

Bi-directional Forwarding Detection (BFD)

Bi-directional forwarding detection (BFD) by default runs on every tunnel connecting pairs of edge routers, checking the data plane connectivity between devices. In an IoT deployment that does not require spoke-to-spoke connectivity, setting up a hub-and-spoke topology can have several benefits, including greatly reducing the number of BFD sessions from a spoke router, potentially down to a single session (with a single WAN interface and single hub router).

Depending on business and technical requirements, it may make sense to consider changing the BFD hello interval to be less aggressive. For example, the default interval of 1 second could be increased to 10 seconds for cellular interfaces, while remaining default for wired backhaul connections. An increased interval will reduce data utilization but have the adverse effect of increasing time required to detect a soft failure in the WAN.

Low Bandwidth Link Setting

This configuration command is relevant only for a spoke router in a hub-and-spoke deployment scenario, where the spoke has a low-bandwidth link, such as an LTE link. This is enabled by default on cellular connections. You include this configuration command only on the spoke router, to minimize traffic sent between the hub and the spoke.

The low bandwidth synchronizes all the BFD sessions and control session hello-interval on LTE WAN circuits to timeout at the same time. The periodic heartbeat messages are sent out at the same time to make optimal usage of LTE circuits radio waves or radio frequency energy to transmit and receive packets. The low bandwidth feature cannot reduce the number of hello packets to be transmitted (Tx) or received (Rx) for the sessions but synchronizes the hello interval timeout for the sessions.

For example, if the BFD session and control connection hello-interval is 1 sec, and there is no user data traffic active on LTE circuits, then the sessions hello packets transmitted is spread across 1 sec window interval. Each session will timeout anywhere within that 1 sec interval and transmits the hello packet. This makes the LTE radio to be active almost all the time. With low bandwidth feature, all the session hello packets transmit at the same time and leave the rest of the 1 sec interval idle, making optimal use of LTE modem radio energy.

Track Transport Disable

The Track Transport setting is used to regularly check whether the DTLS connection between the device and a Cisco vBond Orchestrator is up. By default, transport checking is enabled. Disabling this check can reduce some bandwidth utilization.

vSmart OMP Sessions

In a deployment with multiple redundant vSmart controllers, the “max-control-connections” parameter controls, on a per-interface level, is the number of DTLS/TLS control sessions from each edge router to vSmart. By default, this value is two, and it is recommended to not change this value.

Another step taken to minimize the amount of control plane traffic is to not send or receive OMP control traffic over a cellular interface when other interfaces are available. This behavior is inherent in the software and is not configurable.

Cellular as Backup WAN

If cellular is a backup connection, enable **last-resort-circuit** to make the modem dormant (thus use no data) until it is required due to a primary WAN failure. This will introduce an additional ~7 second delay in failing over WAN interfaces to reduce bouncing between interfaces.

vManage Connection Preference

Set vmanage-connection-preference to **prefer primary interface** for connecting to vManage for control plane traffic over cellular.

Managing Multiple WAN Interfaces

The industrial routers offer a variety of WAN interfaces to enable maximum flexibility in deployment scenarios that often have limited WAN options available. The WAN interface options include the following:

WAN INTERFACE	IR1101	IR1800	IR8300
ETHERNET	X	X	X

WAN INTERFACE	IR1101	IR1800	IR8300
DSL	X	X	
CELLULAR (SINGLE OR DUAL)	X (dual with expansion module)	X (dual on 1831,1833,1835)	X
CURWB (EXTERNAL RADIO VIA ETHERNET)	X	X	X
T1/E1			X

When multiple WAN connections are available to a SD-WAN router it is important to carefully gather requirements about the types of applications and traffic that are expected at the site, characteristics of the WAN providers, and business objectives, such as:

- Transmit and receive bandwidth required (megabits per second)
- Latency, loss, jitter tolerance
- SLA provided by the service provider
- Bandwidth allowance per month
- Cost
- Resiliency requirements
- Public versus private addressing

Ethernet

The routed ethernet port on the IR series is fully supported as a WAN interface, as configured using a **Cisco VPN Interface Ethernet** feature template. This interface could be connected to a variety of wired (copper or fiber) networks, either directly or through an external modem, such as satellite.

Using dynamic addressing via DHCP is common in this case and provides the ability to do Plug-n-Play provisioning in the field. Static addressing is also supported and can be enabled at day 0 deployment using a bootstrap configuration file on a USB flash drive.

In some circumstances, it can be useful to use a physical Ethernet interface configured as a switchport (access or trunk) and associate it with one or more VLANs. The VLAN(s) can then be tied to a layer three SVI interface which can act as a WAN transport. This can be helpful when connected to an upstream switch or a modem (like the Cisco IW9167 CURWB radio) that supports 802.1q trunking.

xDSL

The IR1101 and IR1800 series routers support a VDSL2 / ADSL2(+) WAN interface provided by inserting an **SFP-VADSL2+-I** module in the GigabitEthernet 0/0/0 SFP port. Currently, as of version 20.10, vManage does have a DSL feature template for some device models, but this will not work with the IoT specific SFP module. Instead, a **CLI Add-on** template is required and an example configuration is provided in the Configuration section. Bootstrapping with a USB flash drive also works for provisioning the router over DSL.

When using broadband interfaces like DSL it is recommended to use **Adaptive QOS** as documented here: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/ios-xe-17/qos-book-xe/m-adaptive-qos.html

Cellular

Cellular connectivity on the IR1101, IR1800, and IR8300 is provided through PIM modules. The base IR1101 supports a single PIM module, and a second one can be added through an expansion module (IRM-1100-SP or IRM-1100-SPMI). The IR1821 supports a single PIM, while the IR1831, IR1833, and IR1835, IR8340 each support two PIM modules.

Modularity provides these platforms great flexibility in terms of speeds, bands, geographic and carrier compatibility, and future proofing. The table below lists the currently available PIM modules:

CELLULAR PIM MODEL	DESCRIPTION
P-LTE-MNA	CAT4, Band14 FirstNet Ready
P-LTE-VZ	CAT4, Verizon
P-LTE-US	CAT4, AT&T
P-LTE-GB	CAT4, Europe
P-LTE-IN	CAT4, India
P-LTE-IN	CAT4, Japan
P-LTEA-EA	CAT6, USA / Canada / UAE / Europe
P-LTEA-EA	CAT6, Australia / NZ / Japan / India / Singapore / Malaysia / Thailand
P-LTEAP18-GL	CAT18, Global, FirstNet Ready, CBRS
P-5GS6-GL	5G Sub 6GHz, Global, CBRS

Most of the cellular modules include two SIM card slots. This offers an extra layer of redundancy, so that if a signal is lost on the primary/active SIM in the modem, and another SIM card is present, the modem will reload itself using the secondary SIM card, which may require loading a different version of the carrier-specific firmware. Because the modem must reload for this process to work, it can take around 3 minutes before a connection can be established with the second SIM. The router and modem will not automatically reload again to the primary SIM card when the signal is available again.

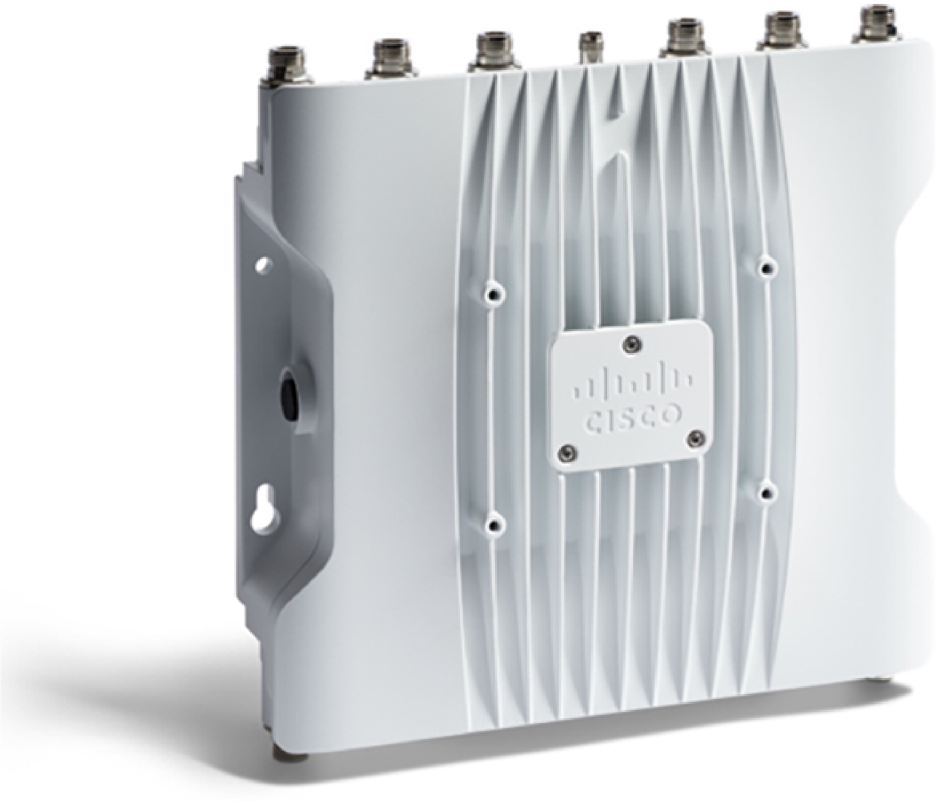
Cisco Ultra Reliable Wireless Backhaul (CURWB)

Cisco Ultra Reliable Wireless Backhaul (CURWB) provides a high bandwidth, resilient, low latency wireless WAN uplink that can be leveraged by SD-WAN enabled industrial routers using an external radio – namely the Cisco IW9167. To the Cisco industrial router, the CURWB uplink appears as just a layer two connection via one of the switchports. The CURWB radios can be deployed in several ways including Point-to-Point and Point-to-Multipoint.

It is recommended to pre-provision the CURWB radio that is wired to the router, as vManage cannot manage the radio itself. Cisco vManage configuration of the SD-WAN router involves using a combination of **VPN Interface SVI** feature template, and a **CLI Add-on** template to configure the SVI as a tunnel interface. The router switchport is configured as an 802.1Q trunk towards the external CURWB radio.

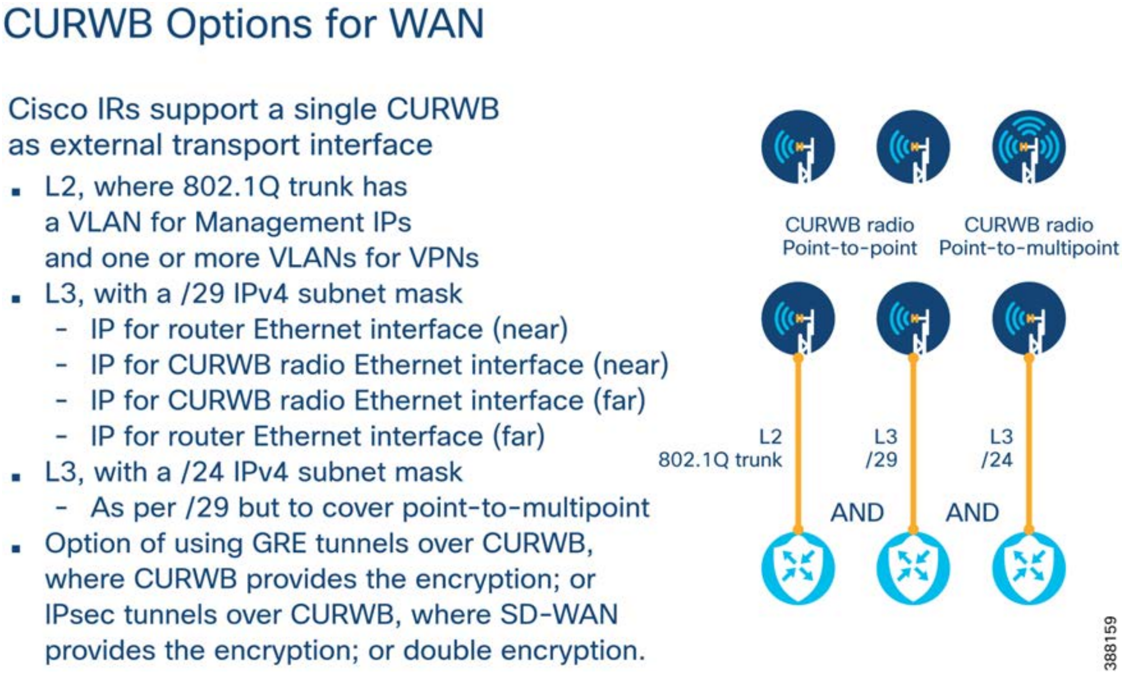
Because the CURWB radio link provides a layer of encryption, the use of IPsec for the SD-WAN underlay network on this uplink may not be required if the network beyond the remote CURWB radio is trusted. In this case, the VPN0 transport can be set to use GRE instead of IPsec.

Figure 9: Cisco Ultra Reliable Wireless Backhaul IW9167E Access Point



The diagram below shows three options for how the CURWB network could be setup for layer 2 versus layer 3, addressing schema, and point-to-point versus point-to-multipoint.

Figure 10: CURWB Options for WAN



CURWB Options for WAN

Cisco IRs support a single CURWB as external transport interface

- L2, where 802.1Q trunk has a VLAN for Management IPs and one or more VLANs for VPNs
- L3, with a /29 IPv4 subnet mask
  - IP for router Ethernet interface (near)
  - IP for CURWB radio Ethernet interface (near)
  - IP for CURWB radio Ethernet interface (far)
  - IP for router Ethernet interface (far)
- L3, with a /24 IPv4 subnet mask
  - As per /29 but to cover point-to-multipoint
- Option of using GRE tunnels over CURWB, where CURWB provides the encryption; or IPsec tunnels over CURWB, where SD-WAN provides the encryption; or double encryption.

Resilience Between Multiple WAN Interfaces

The SD-WAN solution excel s at managing multiple WAN links, and providing intelligent routing, failure detection, and resiliency. Decoupling the underlay network from the overlay service VPNs creates a more cohesive experience for users and applications regardless of the transport.

Bidirectional Forwarding Detection (BFD) is a monitoring protocol that runs in the data plane and constantly monitors the availability of an overlay tunnel. The BFD timers are configurable, but by default will detect a failure within about seven seconds, reporting the change to the routing table so that traffic can take an alternate path.

IPsec preference is a user-defined value that can be configured on each VPN0 Tunnel interface. If multiple WAN links are up and working, the link with the higher preference will be used for data transport. By default, the preference will be the same across WAN links, thus facilitating ECMP load balancing.

Administrative distances can also be set on each underlay route to assign a preference to one type of interface over another based on cost, reliability, latency, etc. This administrative distance is applied to the default route egress for each WAN interface.

For best results it is recommended to set the administrative distance to be the same on each WAN interface (a value of 254 for example) and allow the IPsec preference and BFD monitoring functions to make the routing decision for service VPN traffic. If the WAN interface default routes have different administrative distances, an IPsec tunnel will only be built over the interface with the lowest distance.

When using cellular interfaces with a limited data plan, and an additional WAN link as a primary uplink, it may be helpful to enable the **last resort** option on the cellular interface. This will cause the cellular interface to go dormant and not use any data until the primary uplink loses connectivity. There will be a delay of around one minute while the failure is detected, and the cellular connection is brought up.

Load Balancing Techniques

IoT users often rely on disparate WAN interfaces for connectivity. It can be desirable to use these interfaces in an active-standby manner as discussed previously, or to fully utilize the bandwidth of all (or some) links simultaneously using load balancing. The Cisco IOS-XE router running in SD-WAN mode will try to use equal cost multi-path load balancing based on a per-flow basis. A flow is an IP conversation between two IP addresses (source and destination) but could also be configured (with the **Enhance ECMP keying** setting) to factor in the layer four (for example, TCP or UDP) port number for greater potential in having more flows to load balance.

In the case where a site has two or more WAN interfaces with considerably different bandwidth available to each (Gigabit fiber, and LTE cellular for example) it may be desirable to set each VPN tunnel interface to have a specific **Weight** value that will be used to perform unequal cost load balancing. For example, an ethernet interface could be assigned a weight of 5, and LTE interface a weight of 1. The Ethernet link would be given 5 times as many flows as the LTE interface.

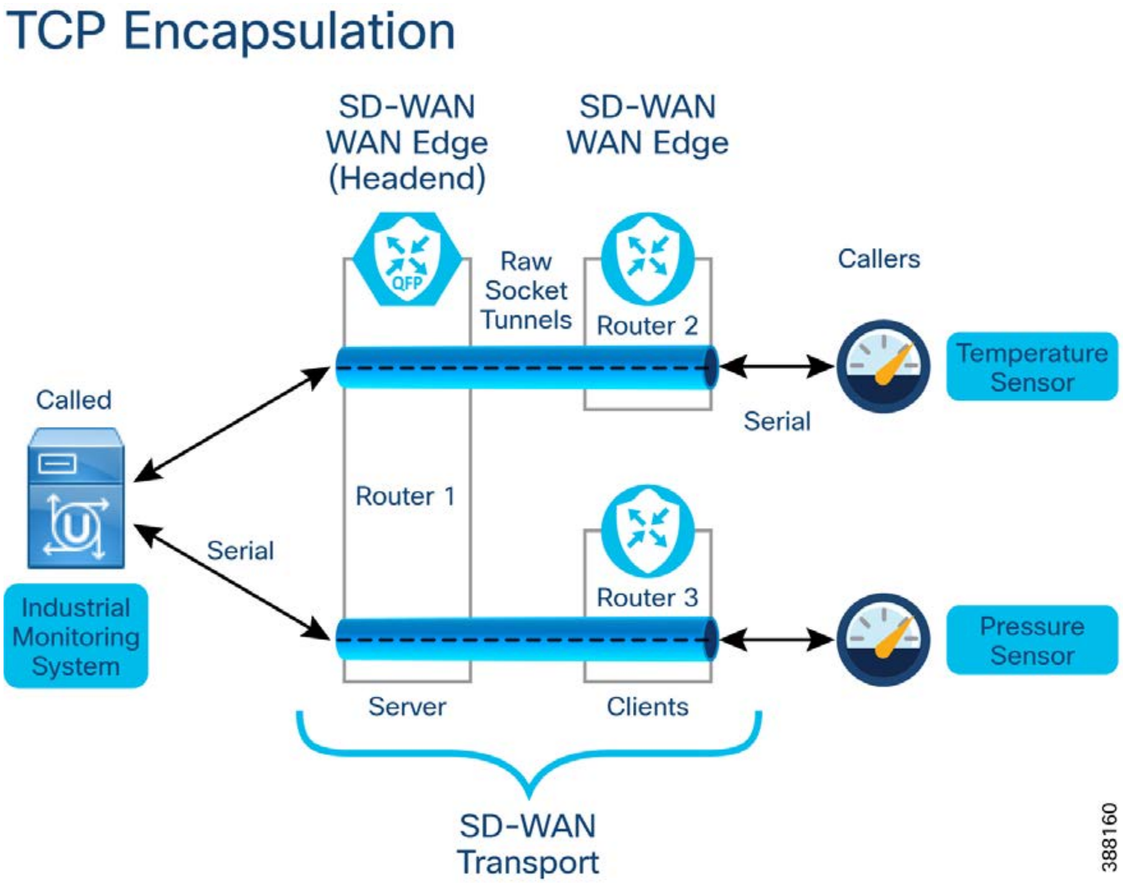
Serial I/O

Industrial IoT devices still commonly use serial interfaces that are considered “legacy” technologies in the IT world. Machine to machine communication often relies on these low bandwidth links to connect equipment at remote locations back to centralized controllers or similar devices. Cisco SD-WAN solution can be used to enable serial connected devices at disparate geographical locations to talk by encapsulating serial data in either TCP or UDP packets that can traverse the secure IPsec overlay network.

Details of CLI required for configuring raw socket TCP and UDP can be found in The IR1101 Software Configuration Guide and pertains in this regard to all industrial router models.

Raw Socket TCP Encapsulation

The illustration below shows how a remote temperature or pressure sensor (or any other serial connected sensor or piece of equipment) is connected using a **Raw Socket TCP** client/server model. Here the serial device/sensor is connected to the SD-WAN edge router (IR1101, IR1800, IR8340) serial port which encapsulates the serial data over a segmented service VPN across the SD-WAN overlay network to a far-end raw socket server on an SD-WAN edge router in the monitoring center. The TCP connection is initiated by the SD-WAN Edge router and to the SD-WAN edge monitoring sensor router which acts as a listener.

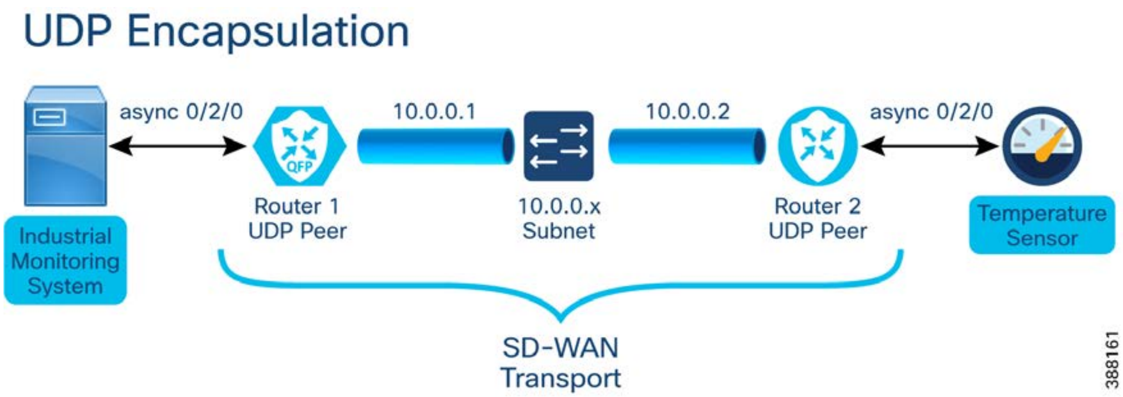


Raw Socket UDP Encapsulation

The illustration below shows how a remote temperature sensor (or any other serial connected sensor or piece of equipment) is connected using a **Raw Socket UDP** model. Here, the serial data is transferred between the sensor and monitoring system across the SD-WAN transport network using SD-WAN edge routers (Router 2 and Router 1) as UDP peers.

In this example, the Raw Socket UDP peer (SD-WAN Edge Router 2) receives streams of serial data from the sensor and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. Router 2 then sends the packetized data across the SD-WAN network to the Raw Socket peer (Router 1) at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the monitoring system.

Figure 11:



Note As of the time of publication, on IOS-XE 17.10.1 and vManage 20.10, an issue (defect ID: CSCwe26344) exists whereby serial communication can be configured successfully through the CLI add-on template capability of vManage but special handling must be done to modify/change/replace the configuration.

The following lines need to be added to the CLI template for any async port that is in the current CLI template or previously used CLI template. Failure to do so will fail on any further attempts to apply the device template.

For instance, if line 0/3/0 was used in a previously downloaded CLI template but is not used anymore, line 0/3/0 must be part of the current template, even in if not actually used. The same logic applies to all serial ports on either the router base model (IR1101, IR1800, IR8340) or expansion modules (IR1101).

Line to be added:

```
!
line 0/3/0  (repeat for all previously or currently used lines)
!
```

Static 1:1 NAT, Static N:1 Port Forwarding, and Hybrid NAT/PAT

Cisco SD-WAN edge routers enable last mile connectivity to customer owned devices like controller devices, IP Cameras, sensors, SCADA end devices and other IP aware devices. These last-mile customer-owned devices would be referred to as **end devices** or **devices** in this section.

For deployments involving thousands of last-mile end devices, having the field technician configure every end device with a unique IP address is error prone. The use of Network Address Translation (NAT) and Port Address Translation (PAT) are supported by vManage to provide a common set of local IP addresses and/or ports at multiple remote locations with the global IP address being captured and operated on only within the SD-WAN.

There are three approaches to represent the end devices to the hub edge router and operations center:

- **Static NAT (1:1)**
  - For example, a Cisco SD-WAN edge router serving 4 end devices would need 4 NAT global IP addresses.
  - Then, one unique NAT global IP is applied to represent each end device. For example,
    - NAT global ip1 to represent end device 1.
    - NAT global ip2 to represent end device 2, and so on.

- **Port Forwarding (N:1)**
  - In this case, a Cisco SD-WAN edge router serving, for example, 4 end devices would need only 1 NAT global IP.
  - Then, a combination of one common NAT global IP + unique UDP or TCP ports can be provided to represent unique resource on each end device. For example,
    - NAT global ip3 + port X1 to represent a resource (for example, camera 1) on end device 3.
    - NAT global ip3 + port X2 can be used to represent another resource (for example, SSH/FTP) on end device 3.
    - NAT global ip3 + port Y1 to represent resource on end device 4, and so on.

- **Hybrid Approach**
  - Using a combination of both the approaches mentioned above a greater amount of flexibility can achieved.
  - Both the approaches can co-exist, but for different end devices.
  - For example:
    - End device1 can be represented with NAT global IP 1 (1:1 Static NAT)
    - End device2 can be represented with NAT global IP 2 (1:1 Static NAT)
    - End devices 3 & 4 are represented with NAT global IP 3 + port combinations (Port Forwarding)

Guideline for Private/Local IP Configuration on Customer End Devices

This section gives guidelines for the field technicians to configure the local IP address on the end devices connected behind the Cisco SD-WAN Edge router.

The table below lists a sample distribution of IP address range for different types of end devices.

Table 7: NAT Local IP range for various types of end devices – A sample table

Type of End device	NAT Local IP range	First IP	Second IP	Successive IPs
IP Cameras	192.168.0.121- 192.168.0.150	192.168.0.121	192.168.0.122	Etc.
MODBUS end device	192.168.0.151- 192.168.0.200	192.168.0.151	192.168.0.152	Etc.
Variable Signage	192.168.0.201- 192.168.0.250	192.168.0.201	192.168.0.202	Etc.
T104 end device	192.168.0.41- 192.168.0.80	192.168.0.41	192.168.0.42	Etc.

The job of the technician is to configure the IP devices connected behind the Cisco SD-WAN routers with the respective IP address from a previously established NAT pool.

Keeping it simple is very important. Adapting this approach would mean the field technician would just require the table in his hand and should do the same configuration at all locations.

Mapping Between Private IP Subnet and NAT Global IP Address

The mapping between private IP subnet to NAT global IP address is done with the help of **mandatory Centralized Control policy**.

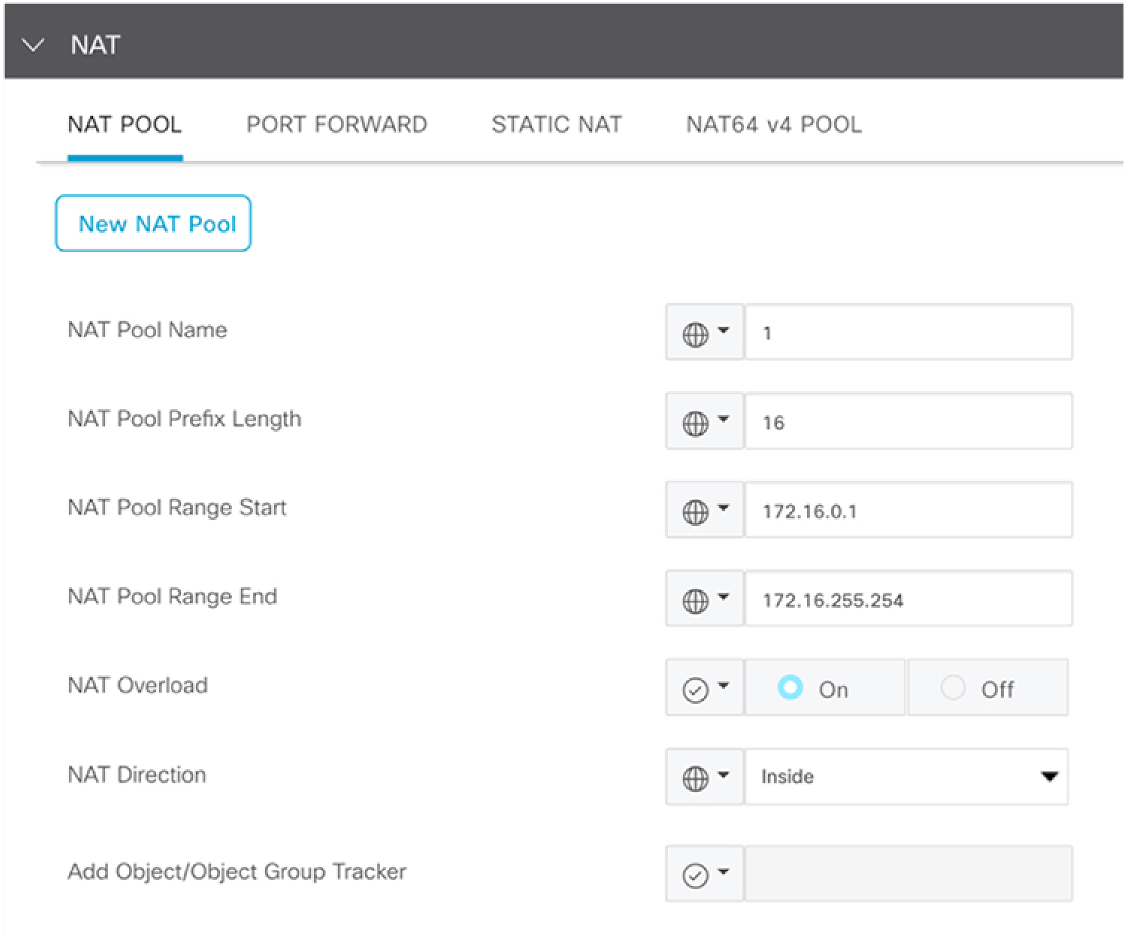
Private IP is what the Field Technician configures on the end device. NAT global IP address is what the vManage user configures to represent that end device, using either a static 1:1 NAT or a Port Forwarding approach. Note that it is likely that the IP addresses of both the private IP and NAT global IP are derived from RFC1918 IP space.

Below is the definition of the centralized control policy using local 192.168.0.0/24 subnet.

- Data prefix is configured to match on “192.168.0.0/24” subnet – say “private_end_device_subnet”
- NAT pool 1 can be defined to serve NAT global IP addresses.
    - For example, 172.16.0.0/16 can serve 64k unique IP addresses.
- From this NAT pool1, the address as configured by the vManage user - would be used for NAT global IP address.
- Whenever there is a match for source data prefix “private_end_device_subnet,”
    - Action Accept
    - With NAT pool 1

Whenever the source IP address matches the data prefix “private_end_device_subnet”, the packet would be accepted and subjected to NAT pool 1.

Figure 12: Example of NAT pool1 definition



NAT Pool Name: 1

NAT Pool Prefix Length: 16

NAT Pool Range Start: 172.16.0.1

NAT Pool Range End: 172.16.255.254

NAT Overload: ● On ○ Off

NAT Direction: Inside

Add Object/Object Group Tracker:

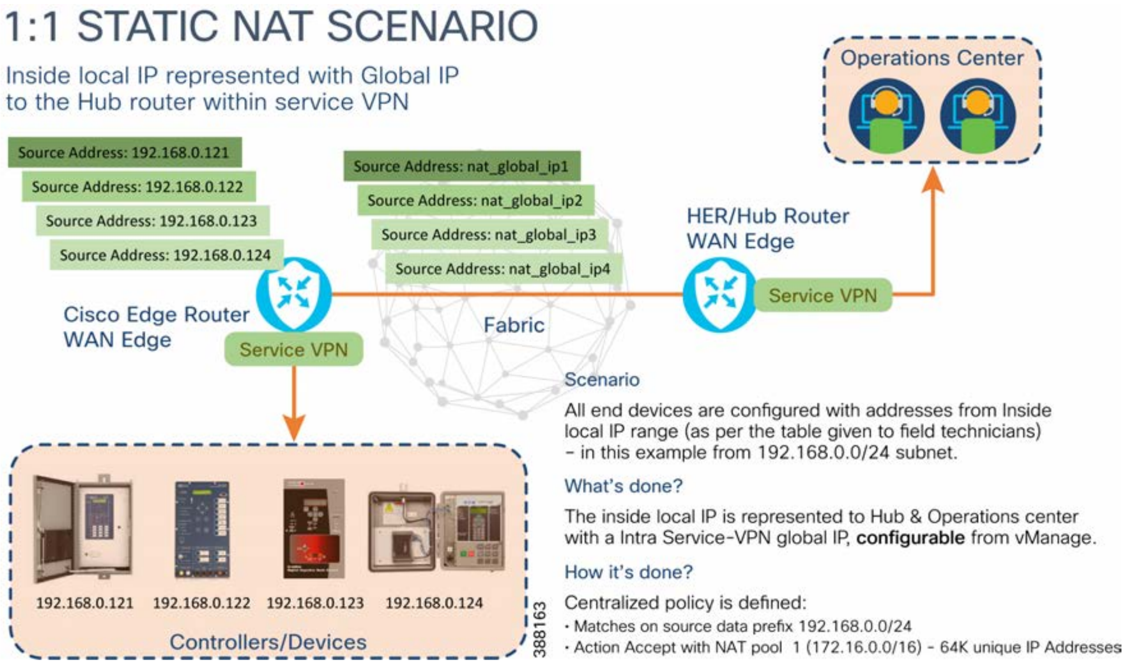
Static 1:1 NAT

This section covers the scenario where every end device (behind the Cisco Router WAN Edge device) is represented to the Operations/Control Center with a unique NAT Global IP address.

The NAT Global IP address is assigned as device value to the variable (also referred as device specific key) defined under **vManage Feature Template** > **Cisco VPN** > **NAT** > **Static NAT** section. This IP needs to be selected out of the NAT Pool range (referred to in the centralized control policy). The NAT pool must be defined under **Feature Template** > **Cisco VPN** > **NAT** > **NAT Pool** section.

Values to such variables can be populated under the device values of the router by vManage user. Device values are accessible under **Configuration** > **Templates** > **Device** templates page.

Figure 13: 1:1 STATIC NAT Scenario – Configurable Under Service VPN Template



1:1 STATIC NAT SCENARIO

Inside local IP represented with Global IP
to the Hub router within service VPN

Scenario

All end devices are configured with addresses from Inside local IP range (as per the table given to field technicians) – in this example from 192.168.0.0/24 subnet.

What's done?

The inside local IP is represented to Hub & Operations center with a Intra Service-VPN global IP, **configurable** from vManage.

How it's done?

Centralized policy is defined:

- Matches on source data prefix 192.168.0.0/24
- Action Accept with NAT pool 1 (172.16.0.0/16) - 64K unique IP Addresses

Operations Center
Source Address: 192.168.0.121
Source Address: 192.168.0.122
Source Address: 192.168.0.123
Source Address: 192.168.0.124
Source Address: nat_global_ip1
Source Address: nat_global_ip2
Source Address: nat_global_ip3
Source Address: nat_global_ip4
HER/Hub Router
WAN Edge
Service VPN
Cisco Edge Router
WAN Edge
Service VPN
Fabric
192.168.0.121
192.168.0.122
192.168.0.123
192.168.0.124
Controllers/Devices
388163

In the figure above, the field technician configures end devices with fixed IP addresses across many different locations.

In the above example, four OMP host routes would be visible on the Hub Router – one for nat_global_ip1, second for nat_global_ip2, third for nat_global_ip3 and fourth for nat_global_ip4 for each edge router.

Therefore, as your deployment scales consideration is needed around the route scaling of the Hub Routers.

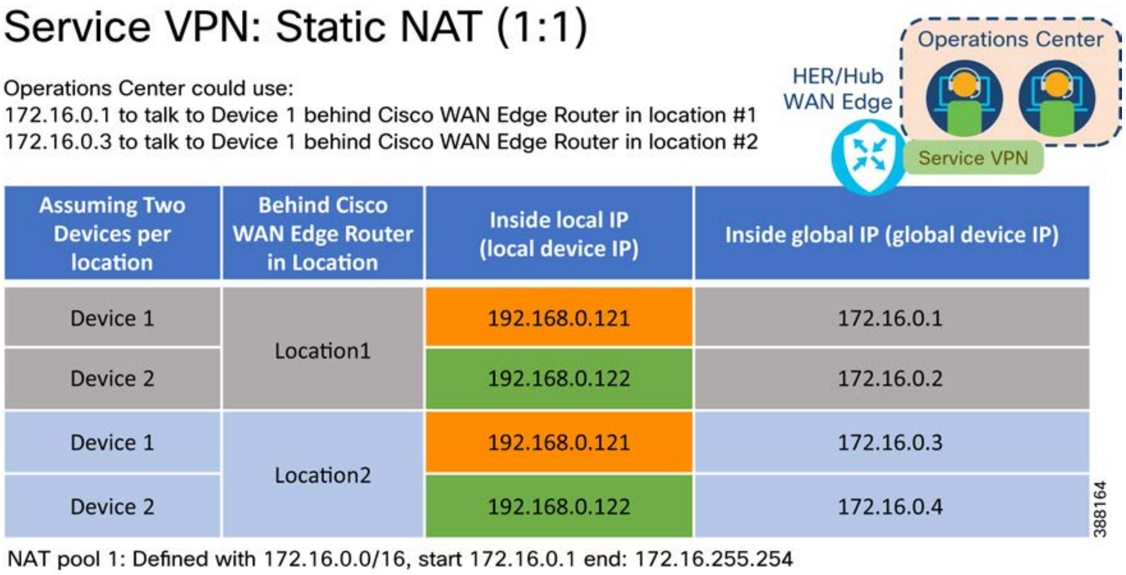
Across many locations, the end devices would all have the IP address from the private subnet (192.168.0.0/24), but it would be represented to the operations center with unique NAT global IP address, configurable from vManage. This allows tremendous flexibility in remotely mapping the NAT global IP address to the customer-owned end devices, while at the same time, the field technician job is kept simple (to configure the IP address from the 192.168.0.0/24 subnet).

If the topology used is Hub and Spoke, then this NAT global IP address is reachable within the service VPN, only from the Hub router and the network behind it.

Static NAT Mapping

The table below shows an example of how 1:1 NAT can be applied to a remote location.

Figure 14: STATIC NAT Scenario – Accessing End Device Across Locations With NAT Global IP Address



Service VPN: Static NAT (1:1)

Operations Center could use:
172.16.0.1 to talk to Device 1 behind Cisco WAN Edge Router in location #1
172.16.0.3 to talk to Device 1 behind Cisco WAN Edge Router in location #2

Operations Center
HER/Hub
WAN Edge
Service VPN
388164

Assuming Two Devices per location	Behind Cisco WAN Edge Router in Location	Inside local IP (local device IP)	Inside global IP (global device IP)
Device 1	Location1	192.168.0.121	172.16.0.1
Device 2		192.168.0.122	172.16.0.2
Device 1	Location2	192.168.0.121	172.16.0.3
Device 2		192.168.0.122	172.16.0.4

NAT pool 1: Defined with 172.16.0.0/16, start 172.16.0.1 end: 172.16.255.254

Explanation:

- In the figure above, the operations center is located behind the Hub edge router and is part of service VPN.
- In this example, the two end devices are located behind each Cisco SD-WAN edge router.

  End device1 in location1 and location2 (and across all the locations) are configured with same local end device IP of 192.168.0.121.
- End device2 in location1 and location2 (and across all the locations) are configured with same local end device IP of 192.168.0.122.
- To access End device 1 in location1, Operations center needs to talk to 172.16.0.1
- To access End device 2 in location1, Operations center needs to talk to 172.16.0.2
- To access End device 1 in location2, Operations center needs to talk to 172.16.0.3
- To access End device 2 in location2, Operations center needs to talk to 172.16.0.4

Static N:1 Port Forwarding

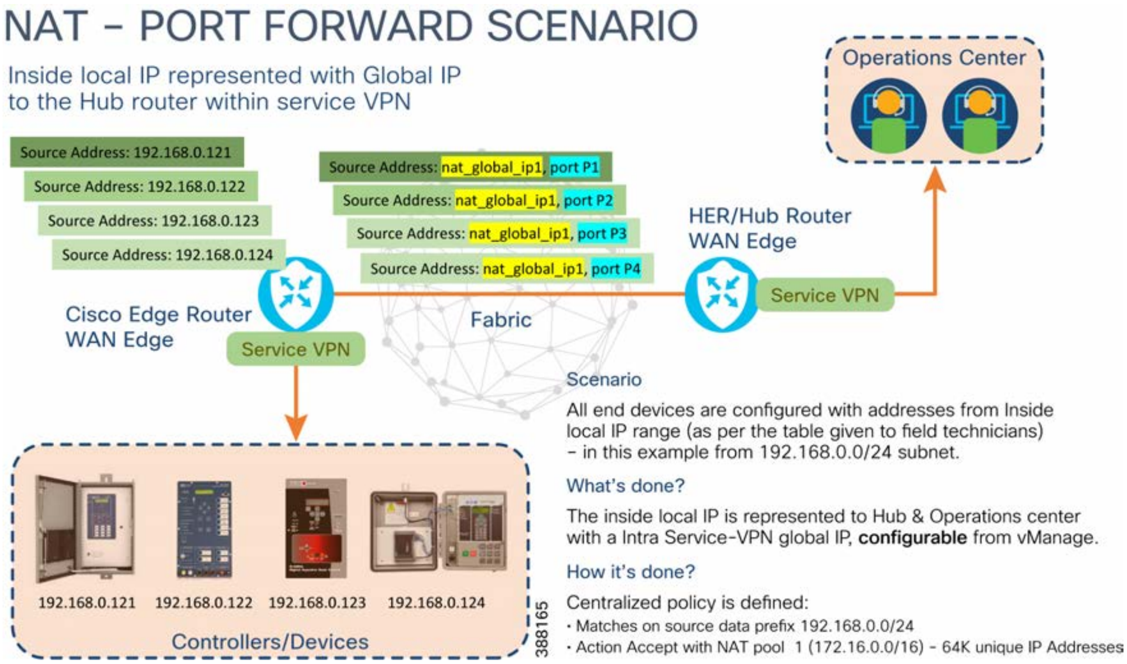
Port forwarding offers an alternative to static NAT, where system scaling also brings a large load on the Head-end edge router due to each router advertising each status NAT entry.

With a **Port Address Translation (PAT)** approach, all the end devices (behind the Cisco WAN edge router) can be represented to the Operations/Control Center with one NAT Global IP address accompanied by a port identifier that is unique to each device behind the edge router.

The NAT Global IP address is assigned as device value to the variable (also referred as device specific key) defined under **vManage Feature Template** > **Cisco VPN** > **NAT** > **Port Forward** section. Like “Static NAT”, this IP needs to be selected out of the NAT Pool range (referred in the centralized control policy). The NAT pool must be defined under the **Feature Template** > **Cisco VPN** > **NAT** > **NAT Pool** section.

The table below shows an example of how Port Forwarding can be applied to a remote location.

Figure 15: N:1 NAT - Port Forwarding Scenario – Configurable Under Service VPN Template



NAT – PORT FORWARD SCENARIO

Inside local IP represented with Global IP
to the Hub router within service VPN

Source Address: 192.168.0.121
Source Address: 192.168.0.122
Source Address: 192.168.0.123
Source Address: 192.168.0.124
Source Address: nat_global_ip1, port P1
Source Address: nat_global_ip1, port P2
Source Address: nat_global_ip1, port P3
Source Address: nat_global_ip1, port P4
Operations Center
HER/Hub Router
WAN Edge
Service VPN
Fabric
Cisco Edge Router
WAN Edge
Service VPN
192.168.0.121
192.168.0.122
192.168.0.123
192.168.0.124
Controllers/Devices
388165

Scenario

All end devices are configured with addresses from Inside local IP range (as per the table given to field technicians) – in this example from 192.168.0.0/24 subnet.

What's done?

The inside local IP is represented to Hub & Operations center with a Intra Service-VPN global IP, **configurable** from vManage.

How it's done?

Centralized policy is defined:

- Matches on source data prefix 192.168.0.0/24
- Action Accept with NAT pool 1 (172.16.0.0/16) - 64K unique IP Addresses

In the above figure, the field technician configures end devices with fixed IP addresses for end devices, across all locations. Here, Global IP1, port P1 represents service/port A on End device 192.168.0.121. Global IP1, port P4 represents service/port B on End device 192.168.0.121.

Across all locations, the end devices would all have the IP address from the private subnet (192.168.0.0/24), but it would be represented to the operations center with one NAT global IP address per Cisco SD-WAN Edge router, configurable from vManage. This allows tremendous flexibility in remotely mapping the NAT global IP address + port combinations to represent the service/ports on the customer owned End devices. Example of service/ports could be HTTP, SSH, FTP, DNP3, MODBUS, and so on.

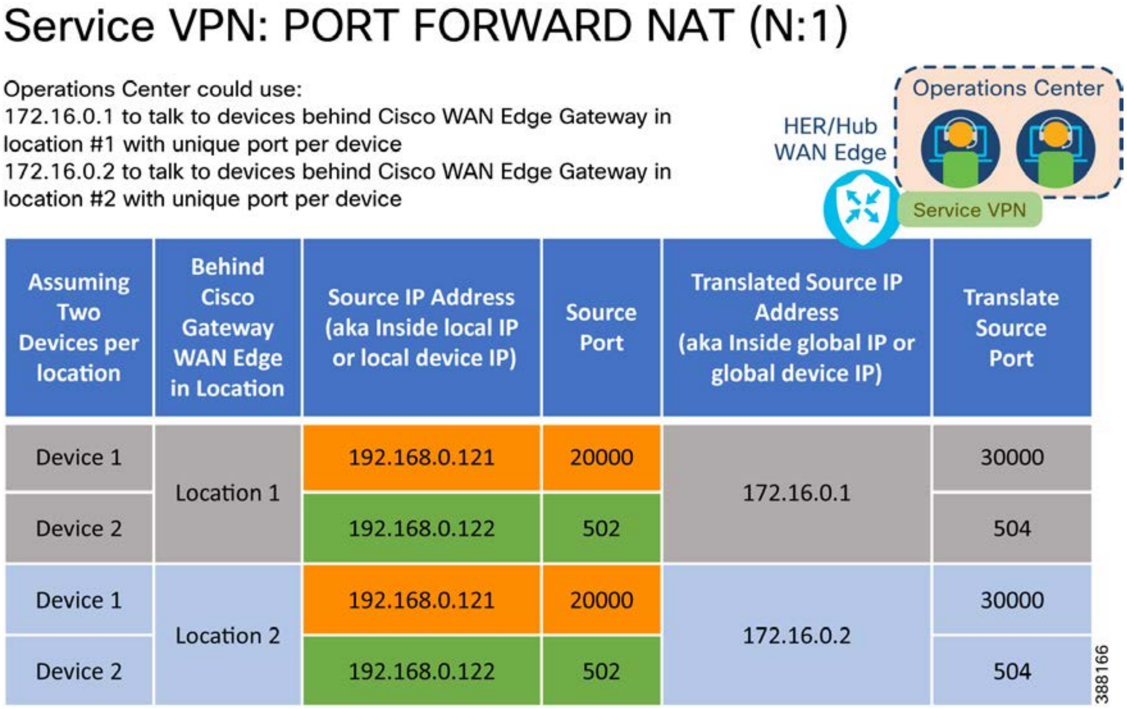
The port number of the end device must be noted down. It could be either the default port number or a custom port number as configured by the field technician.

In the above example, only one NAT Global IP is used, which is ***nat_global_ip1****. Hence, only one OMP route would be visible on the Hub Router. If the topology used is Hub and Spoke, then this NAT global IP address is reachable within service VPN, only from the Hub router and the network behind it.*

N:1 NAT -Port Forwarding Mapping

The table below shows an example of how 1:1 NAT with Port Forwarding can be applied to remote locations.

Figure 16: N:1 NAT – PORT FORWARD Scenario – Accessing End Device Across Locations With NAT Global IP Address.



Service VPN: PORT FORWARD NAT (N:1)

Operations Center could use:
172.16.0.1 to talk to devices behind Cisco WAN Edge Gateway in location #1 with unique port per device
172.16.0.2 to talk to devices behind Cisco WAN Edge Gateway in location #2 with unique port per device

Operations Center
HER/Hub
WAN Edge
Service VPN
388166

Assuming Two Devices per location	Behind Cisco Gateway WAN Edge in Location	Source IP Address (aka Inside local IP or local device IP)	Source Port	Translated Source IP Address (aka Inside global IP or global device IP)	Translate Source Port
Device 1	Location 1	192.168.0.121	20000	172.16.0.1	30000
Device 2		192.168.0.122	502		504
Device 1	Location 2	192.168.0.121	20000	172.16.0.2	30000
Device 2		192.168.0.122	502		504

- In the figure above, the operations center is located behind the Hub router and is part of service VPN.
- In this example, two end devices are located behind each Cisco SD-WAN Edge Router.
- End device1 in all locations are configured with same local end device IP of 192.168.0.121
- End device2 in all locations are configured with same local end device IP of 192.168.0.122
- To access End device 1 in location1, Operations center needs to talk to 172.16.0.1 on port 30000
- To access End device 2 in location1, Operations center needs to talk to 172.16.0.1 on port 504
- To access End device 1 in location2, Operations center needs to talk to 172.16.0.2 on port 30000
- To access End device 2 in location2, Operations center needs to talk to 172.16.0.2 on port 504

Points to Note

- As noted in the table above, the source port and Translate source port do not have to match but must be carefully tracked.
- All End devices are configured with the same private IP 192.168.0.X across all locations.
- 172.16.0.0/16 NAT pool 1 is defined to represent the end devices (global IP) to Operation/Control Center.
- Each Cisco SD-WAN Edge router is identified with unique global IP (out of defined Nat pool 1). IP entered as a variable in vManage device values. Global IP is nothing but the “Translated Source IP Address”.
- At the Operation/Control Center, this “global IP + Translated source Port” combination is used to communicate with the corresponding end device.

Impact of Routes on Head-End Router

Irrespective of the number of end devices connected behind the Cisco SD-WAN router, every spoke router would advertise only one host route (single NAT Global IP known as Translated Source Address) to the Hub edge router. This would mean 10k OMP routes on the hub router for 10k Cisco SD-WAN Edge router deployments.

Limitations of port forwarding

Port forwarding offers a simple alternative to mapping the device address space in a manner simple to the technician and with lower impact on the Head-end edge router than a pure NAT approach.

However, port forwarding does have a few limitations:

- If the application in the control center is inflexible on the port to be used, it could inhibit proper port selection.
- If the application does not use TCP/IP protocol but, instead, a proprietary protocol.
- If there is more than one connected device behind the Cisco SD-WAN edge router speaking the same protocol. The applications in the control/operations center should be capable of talking to the single NAT global IP address on a different port number for each connected device, say 20000, 20001, and 20002 using one port for each end device belonging to same family.
    - This can be mitigated with a hybrid NAT/PAT approach.

NAT Hybrid Approach (Using Static NAT + Port Forward)

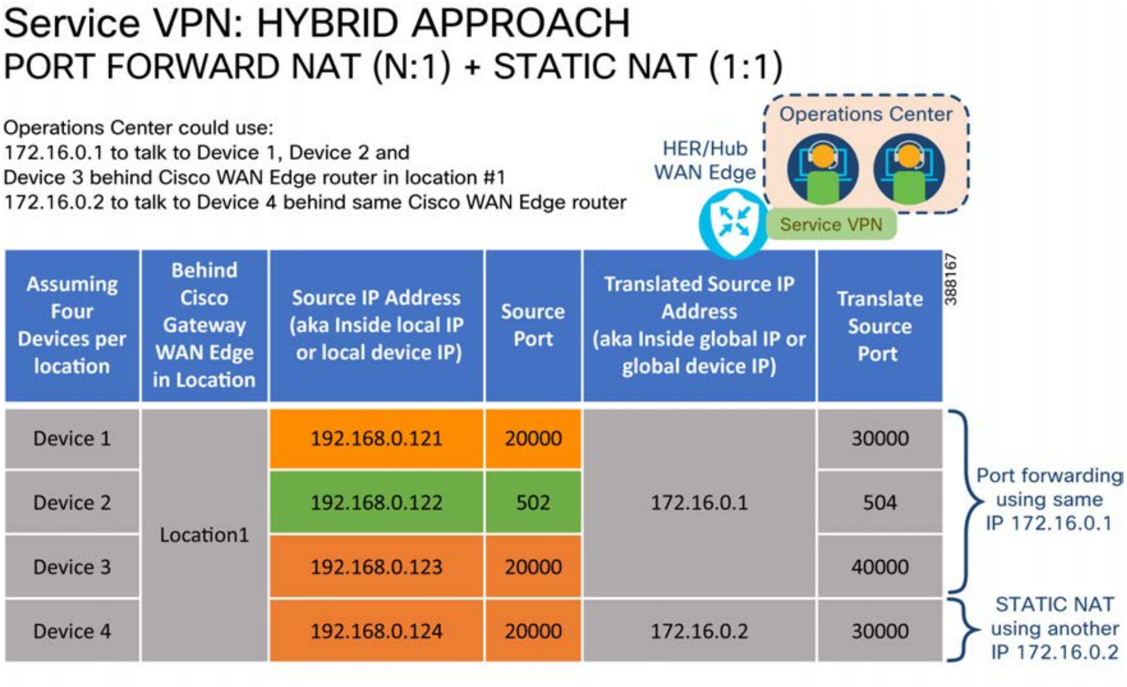
Consider a scenario where there are 4 end devices connected behind a Cisco WAN Edge Router.

The options available are:

- Use static NAT and represent each end device with unique NAT global IP (Translated source IP address). This uses **4 translated source IP address** from NAT pool.
- Use Port forward and represent all the end devices with one common NAT global IP while using port numbers to differentiate between. This uses **1 translated source IP address** from NAT pool.
- Hybrid Approach, which combines the best of the two worlds, where we represent most of the end devices with one common NAT global IP and use static NAT where exclusive access to an end device is needed on multiple port numbers.

The table below shows an example of a hybrid approach with a mix of 1:1 NAT with 1:1 NAT with Port Forwarding applied to remote locations.

Figure 17: Service VPN: NAT – Hybrid Approach



Service VPN: HYBRID APPROACH
PORT FORWARD NAT (N:1) + STATIC NAT (1:1)

Operations Center could use:
172.16.0.1 to talk to Device 1, Device 2 and
Device 3 behind Cisco WAN Edge router in location #1
172.16.0.2 to talk to Device 4 behind same Cisco WAN Edge router

Assuming Four Devices per location	Behind Cisco Gateway WAN Edge in Location	Source IP Address (aka Inside local IP or local device IP)	Source Port	Translated Source IP Address (aka Inside global IP or global device IP)	Translate Source Port
Device 1	Location1	192.168.0.121	20000	172.16.0.1	30000
Device 2		192.168.0.122	502		504
Device 3		192.168.0.123	20000		40000
Device 4		192.168.0.124	20000	172.16.0.2	30000

Port forwarding using same IP 172.16.0.1

STATIC NAT using another IP 172.16.0.2

In the figure above, 4 end devices are enabled for connectivity with the help of Cisco SD-WAN Edge router. The first 3 end devices are enabled for connectivity with the help of Port Forwarding. The last end Device 4 is enabled for connectivity with the help of Static NAT using another NAT global IP (172.16.0.2)

The Operations center can communicate with:

- End Device 1 using “Translated source IP Address” of 172.16.0.1 and destination port 30000.
- End Device 2 using “Translated source IP Address” of 172.16.0.1 and destination port 504.
- End Device 3 using “Translated source IP Address” of 172.16.0.1 and destination port 40000.
- End Device 4 using “Translated source IP Address of 172.16.0.2

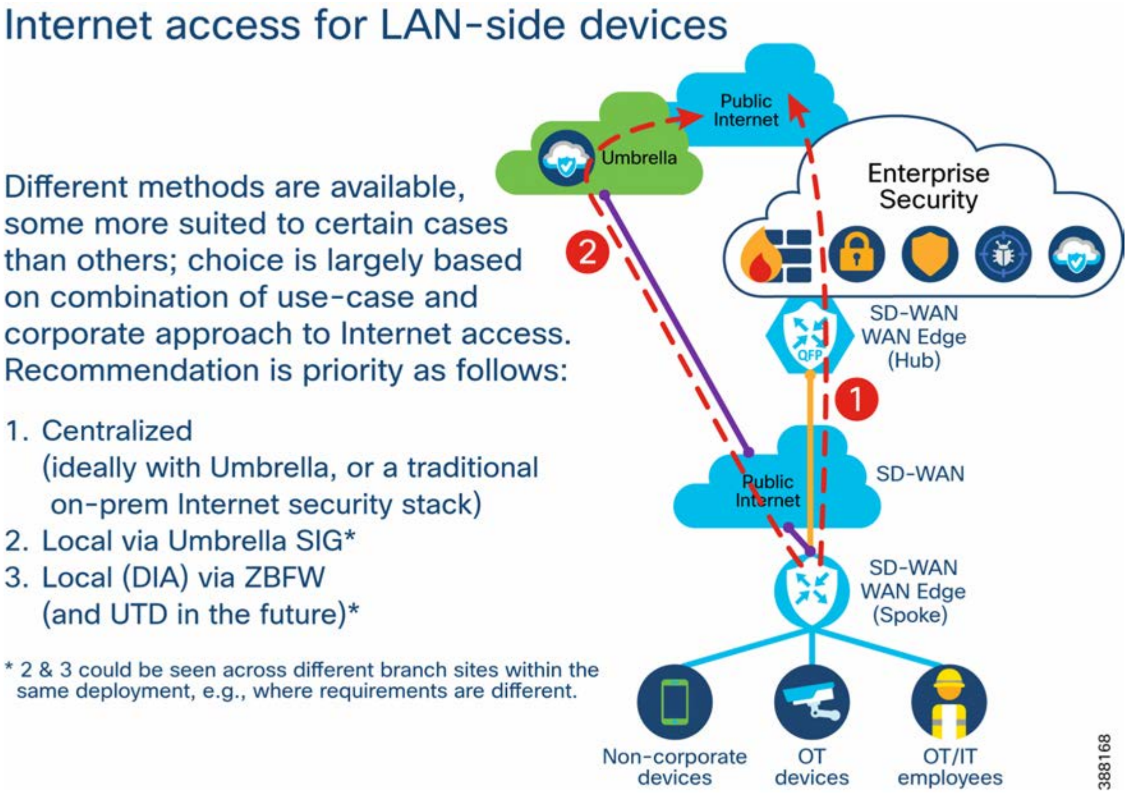
This way, the Router advertises only two routes (172.16.0.1/32 and 172.16.0.2/32) to the Hub router.

For Head-end applications that can communicate only on fixed port, this hybrid approach can be used as mitigation step.

Security and Internet Access

Depending on the requirements of the use case, there are several options available for providing internet connectivity for the LAN devices behind the industrial router. This section outlines three of the options: centralized, direct internet access with local security, and access via Umbrella SIG.

Figure 18: Internet access for LAN-side devices



Internet access for LAN-side devices

Different methods are available, some more suited to certain cases than others; choice is largely based on combination of use-case and corporate approach to Internet access. Recommendation is priority as follows:

1. Centralized (ideally with Umbrella, or a traditional on-prem Internet security stack)
2. Local via Umbrella SIG*
3. Local (DIA) via ZBFW (and UTD in the future)*

* 2 & 3 could be seen across different branch sites within the same deployment, e.g., where requirements are different.

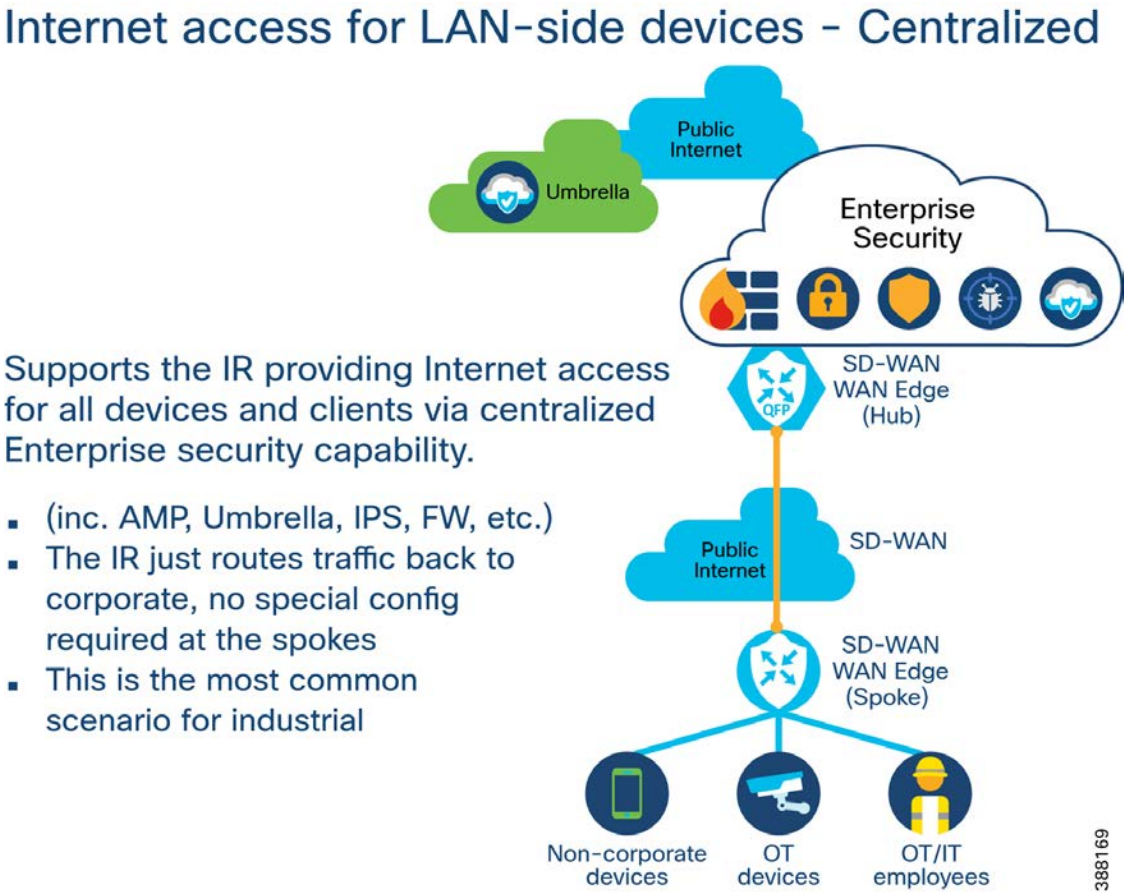
Route via Hub

IoT use cases for SD-WAN can present some unique design considerations. These use cases can include deployments of potentially thousands of edge routers, each connecting similar equipment like machinery or sensors back to a central application server. Often the individual remote sites do not need to talk to each other, only the datacenter or headquarters.

In this type of scenario where the edge routers only need connectivity back to a single (or small number of) headend devices, a hub and spoke topology is recommended. This design provides several benefits, including:

- Greatly reduced number of BFD sessions required, compared to a full mesh, leading to reduced overhead bandwidth utilization.
- Reduces tunnel requirements -- allows you to run lower-end cEdges at the spokes for a potential cost savings.
- Secures branch traffic from other branch traffic by either not permitting traffic between sites or by forcing traffic through centralized security at the hub site.

Figure 19: Internet access for LAN-side devices - Centralized



Internet access for LAN-side devices - Centralized

Supports the IR providing Internet access for all devices and clients via centralized Enterprise security capability.

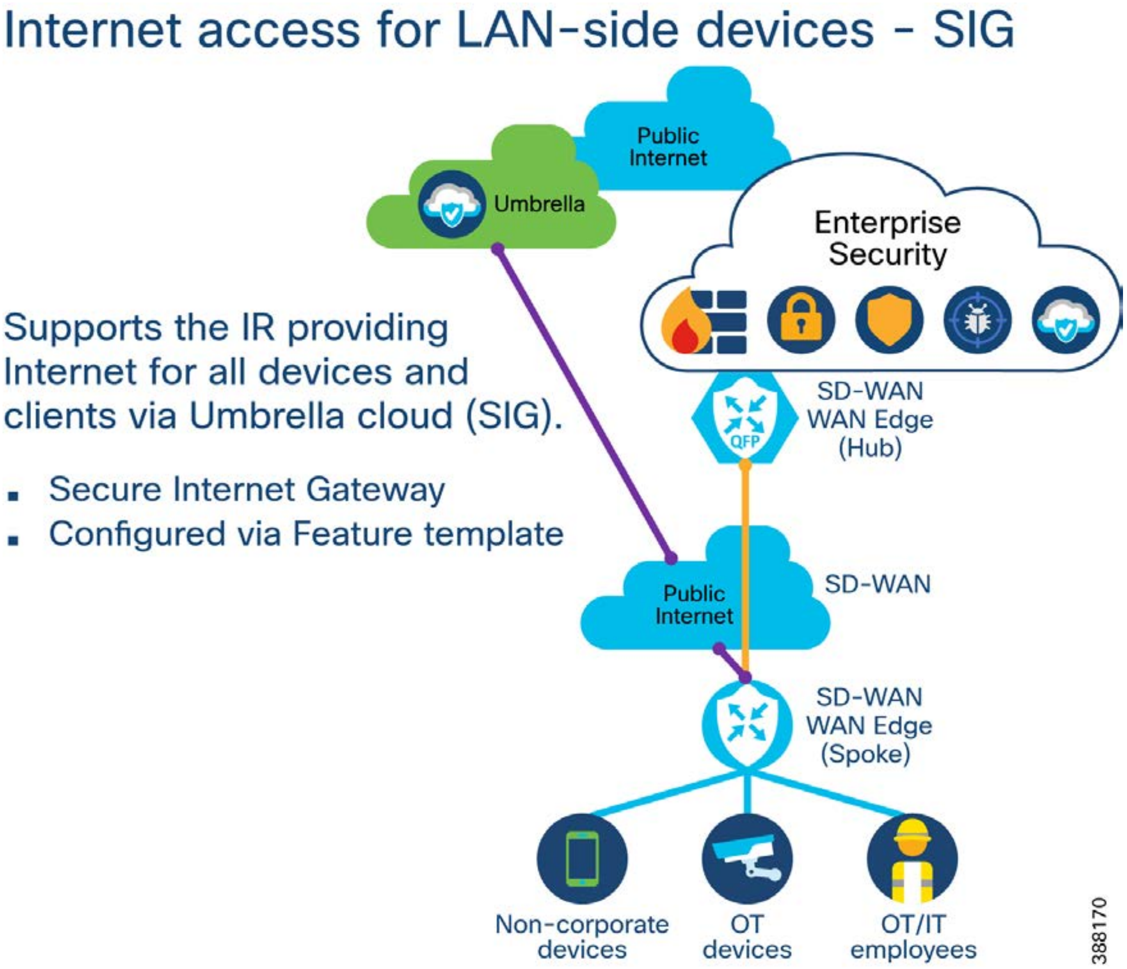
- (inc. AMP, Umbrella, IPS, FW, etc.)
- The IR just routes traffic back to corporate, no special config required at the spokes
- This is the most common scenario for industrial

Umbrella SIG

Cisco Umbrella security solution integrates with vManage SD-WAN to provide cloud-delivered firewall, DNS security, web gateway, threat intelligence, and cloud security broker functionality. This works by creating redundant tunnels on the edge router to the Cisco Umbrella cloud, and then using routing or policies to send the desired traffic to the cloud thereby offloading processing from the edge and ensuring a consistent (or granular) experience across sites with centralized security policies.

As of vManage version 20.10, the Cellular interface cannot be selected from the drop down within the feature template as a source interface. As a workaround you can use a Loopback interface or make the source interface value into a variable that is specified for each cEdge router -- for example fill in a value of “Cellular 0/1/0” for an IR1101.

Figure 20: Internet Access for LAN-side Devices - SIG



Internet access for LAN-side devices - SIG

Supports the IR providing Internet for all devices and clients via Umbrella cloud (SIG).

- Secure Internet Gateway
- Configured via Feature template

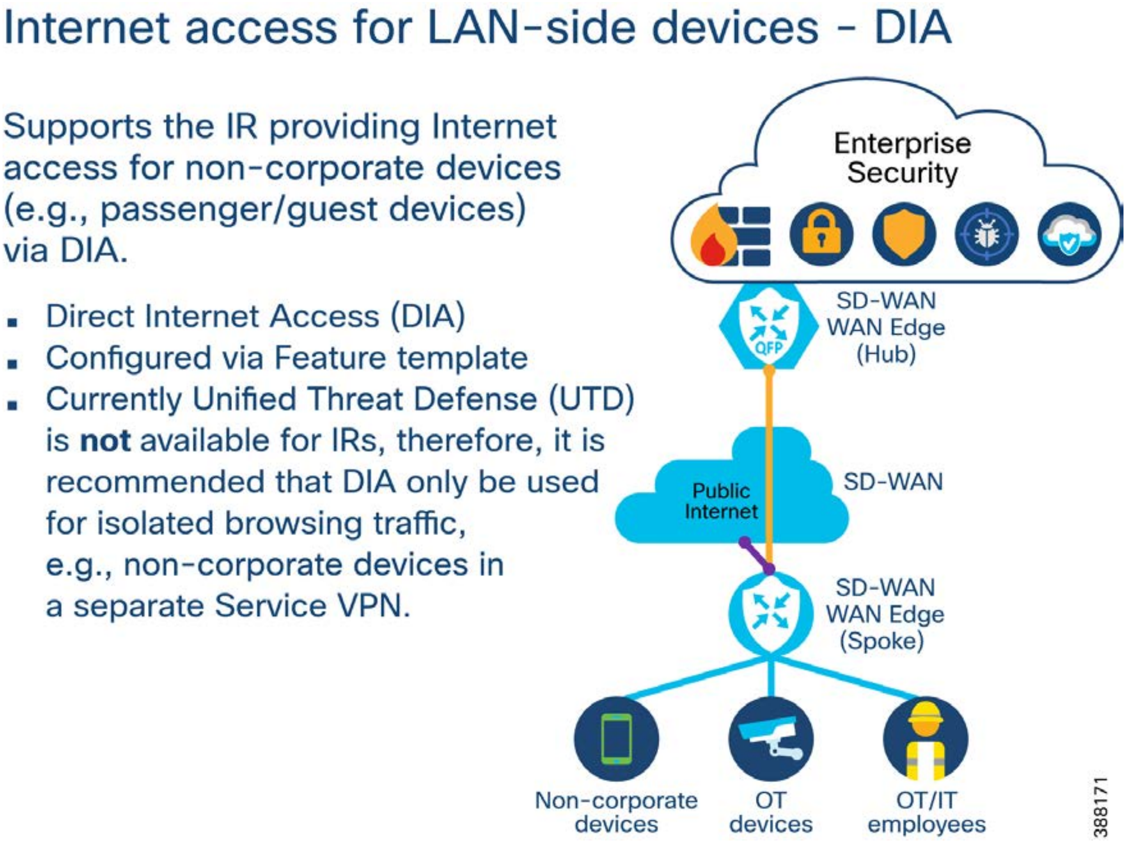
For additional configuration details, refer to the “Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios” Technote:

https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/217562-configure-umbrella-sig-tunneles-on-activ.html#

Direct Internet Access

In a general SD-WAN use case, all traffic leaving an edge router from LAN devices inside a service VPN will be carried in the overlay network tunnel to another edge router, and then onto its destination. For traffic within the enterprise this provides an ideal, secure path for the dataflow, but for internet traffic a different approach often makes better sense. Direct Interface Access (DIA) from an edge router will allow devices and applications within a Service VPN to immediately egress the VPN and go to the internet instead of routing through the overlay network (see “Route via Hub” section). Causing internet-bound traffic to go directly to the internet, instead of passing through other intermediate SD-WAN edge routers can decrease bandwidth utilization and offload processing from central site routers. When subtended devices or clients are given direct internet access, it is required that NAT/PAT be configured because the clients will be leveraging a private address, not routable from the internet.

Figure 21: Internet Access for LAN-side Devices - DIA



Internet access for LAN-side devices - DIA

Supports the IR providing Internet access for non-corporate devices (e.g., passenger/guest devices) via DIA.

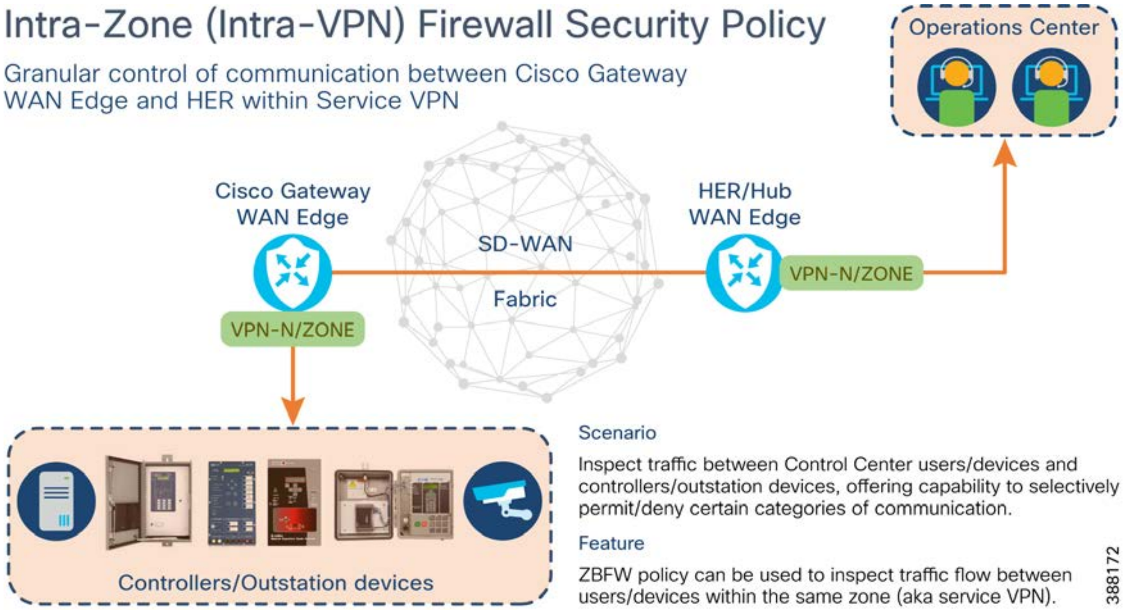
- Direct Internet Access (DIA)
- Configured via Feature template
- Currently Unified Threat Defense (UTD) is **not** available for IRs, therefore, it is recommended that DIA only be used for isolated browsing traffic, e.g., non-corporate devices in a separate Service VPN.

For a more detailed look at the design and configuration of Direct Internet Access in Cisco SD-WAN networks, refer to the Cisco SD-WAN: Enabling Direct Internet Access guide:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf

Zone Based Firewall

Figure 22: Intra-VPN: Firewall Security Policy



Intra-Zone (Intra-VPN) Firewall Security Policy

Granular control of communication between Cisco Gateway WAN Edge and HER within Service VPN

Scenario

Inspect traffic between Control Center users/devices and controllers/outstation devices, offering capability to selectively permit/deny certain categories of communication.

Feature

ZBFW policy can be used to inspect traffic flow between users/devices within the same zone (aka service VPN).

The communication between Operations Center and End devices is isolated inside service VPN/Zone. In the above figure, VPN-N is used to contain the application traffic communication between Operations Center & end devices.

Within the same VPN, communication between Control Center and End devices can be selectively permitted or denied, with the help of Firewall security configuration options.

Zone Based Firewall (aka Security Policy) could be used to selectively permit/deny flows between Control Center and IP-aware end devices.

Available granular controls are:

- Source IP/List, Source Port(s)
- Destination IP/List, Destination Port(s)
- Protocols
- Application list

The **Inspect** option should be chosen to allow return communication for permitted traffic.

Listed below are just a few examples, but not limited to it are:

- Permitting access for end devices to reach selective IPs in operations center.
- Denying the end devices from accessing SSH or HTTP in operations center.
- Permitting Operations center to access the End devices via SSH, monitor/control via HTTP(S).
- Selectively permitting the above operations from specific hosts of Operations center, and so on.

Note *Traffic within the LAN segment of a particular service VPN is not inspected.*

LAN IP Addressing

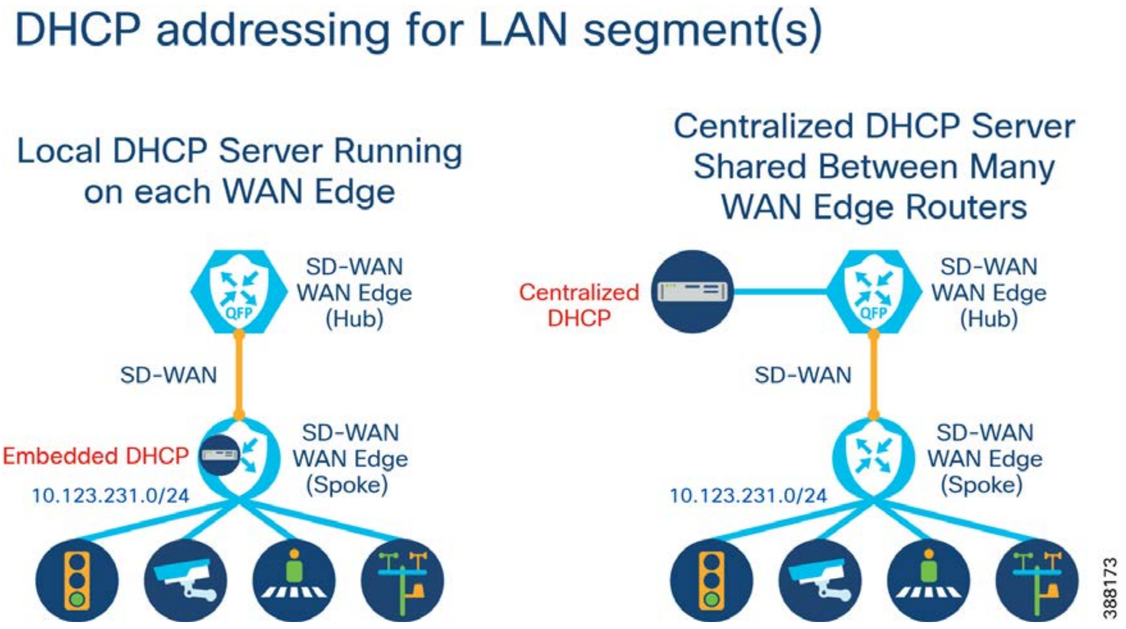
IP addressing for devices behind the industrial WAN Edge router can use one of three general methods: static, DHCP from a local server, or DHCP from a central server. Which option to choose depends on the use case, type of equipment, and any other requirements specific to the deployment.

Static IP address is commonly used in conjunction with a static NAT or port forwarding configuration, especially in scenarios where there are many sites with the same equipment at each. Often these types of equipment are preprovisioned by OT staff that relies on a well-known address to reach each type of equipment (for example, the traffic signal controller at an intersection could always be 192.168.0.23). If static addressing is used, there is no additional configuration required in the vManage feature templates.

DHCP provides a convenient way to address devices when it does not matter what IP address is assigned, or if device connectivity is generally initiated by the device itself, versus some remote client. It is also possible to have DHCP reservations for individual hosts. Each cEdge industrial router can act as the DHCP server for its local LAN networks. This simple approach is ideal in cases where the sites have overlapping (or identical) subnets and will be able to hand out client addresses even if the WAN connection is down for some reason.

In situations where the spoke sites have unique subnets and routing is taking place between them, it can be helpful to utilize a centralized DHCP server located in a datacenter or central site. This centralized method can provide a single place to manage addressing for the entire network, visibility into what addresses are used versus available, and can offload the DHCP function from the spoke routers.

Figure 23: DHCP Addressing Options: Local or Centralized Server

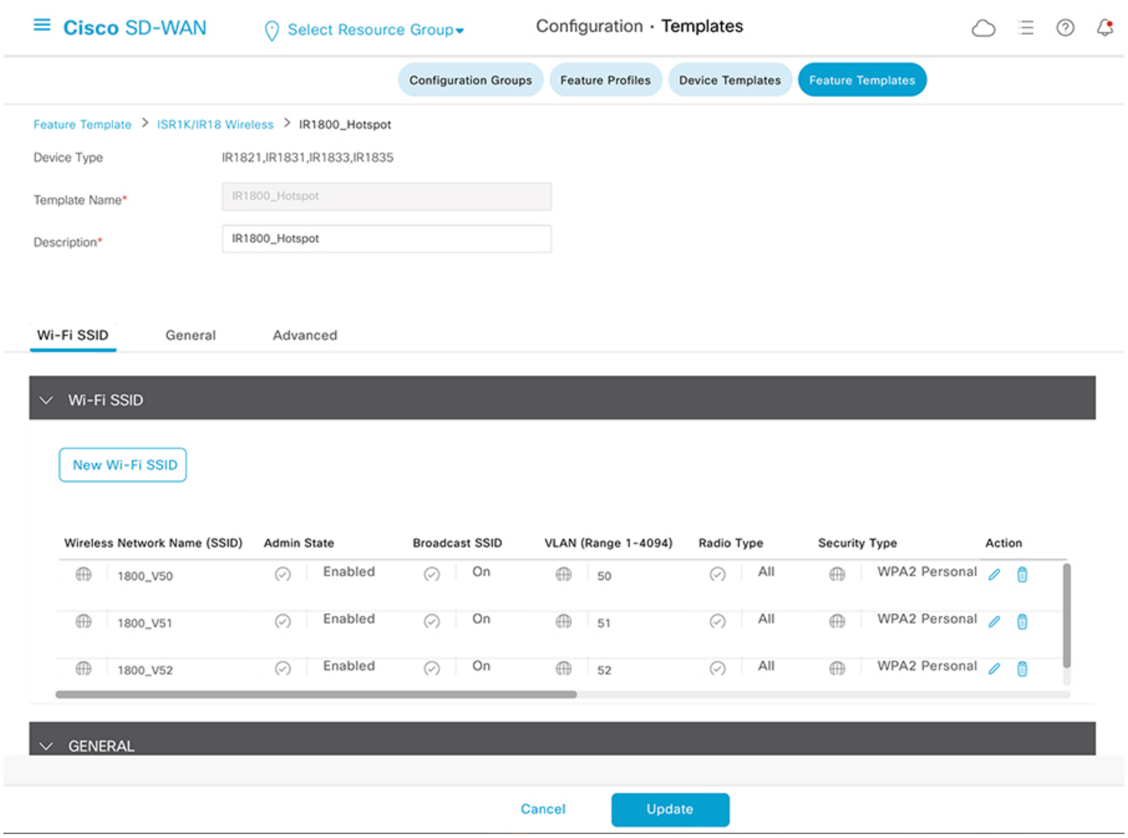


CHAPTER 3

Configurations

Wi-Fi Hotspot

1. Create an “ISR1K/IR18 Wireless” feature template.



Feature Template > ISR1K/IR18 Wireless > IR1800_Hotspot

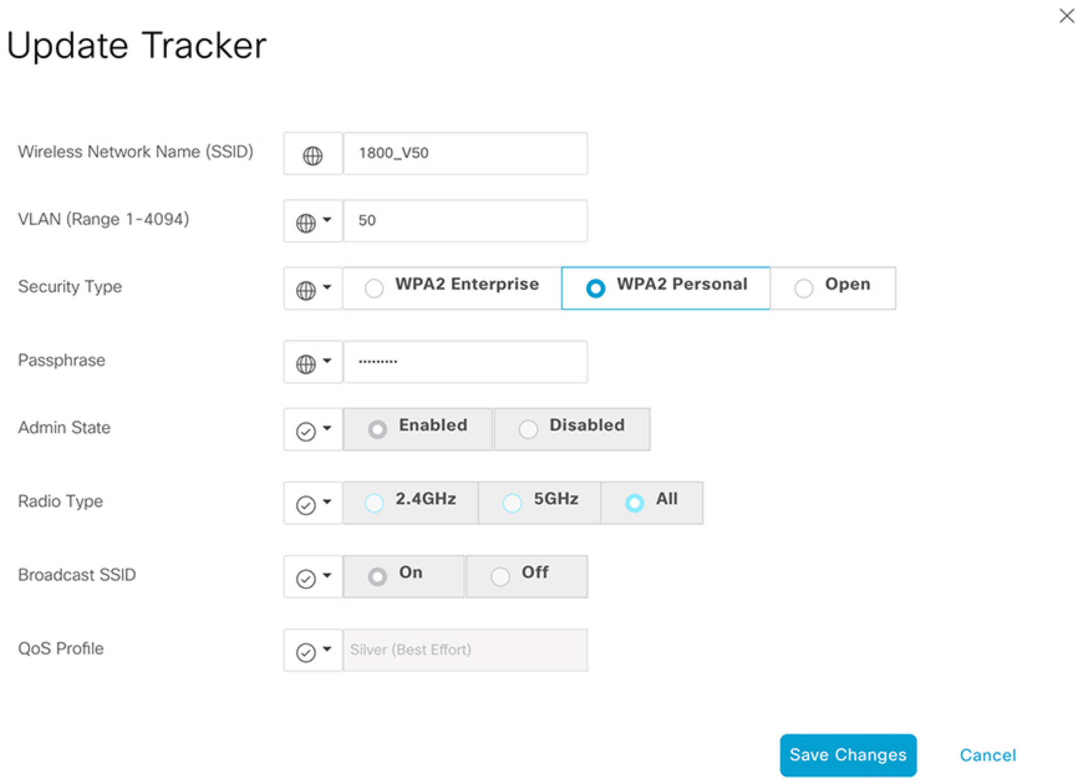
Device Type: IR1821,IR1831,IR1833,IR1835

Template Name*: IR1800_Hotspot

Description*: IR1800_Hotspot

Wireless Network Name (SSID)	Admin State	Broadcast SSID	VLAN (Range 1-4094)	Radio Type	Security Type	Action
1800_V50	Enabled	On	50	All	WPA2 Personal	
1800_V51	Enabled	On	51	All	WPA2 Personal	
1800_V52	Enabled	On	52	All	WPA2 Personal	

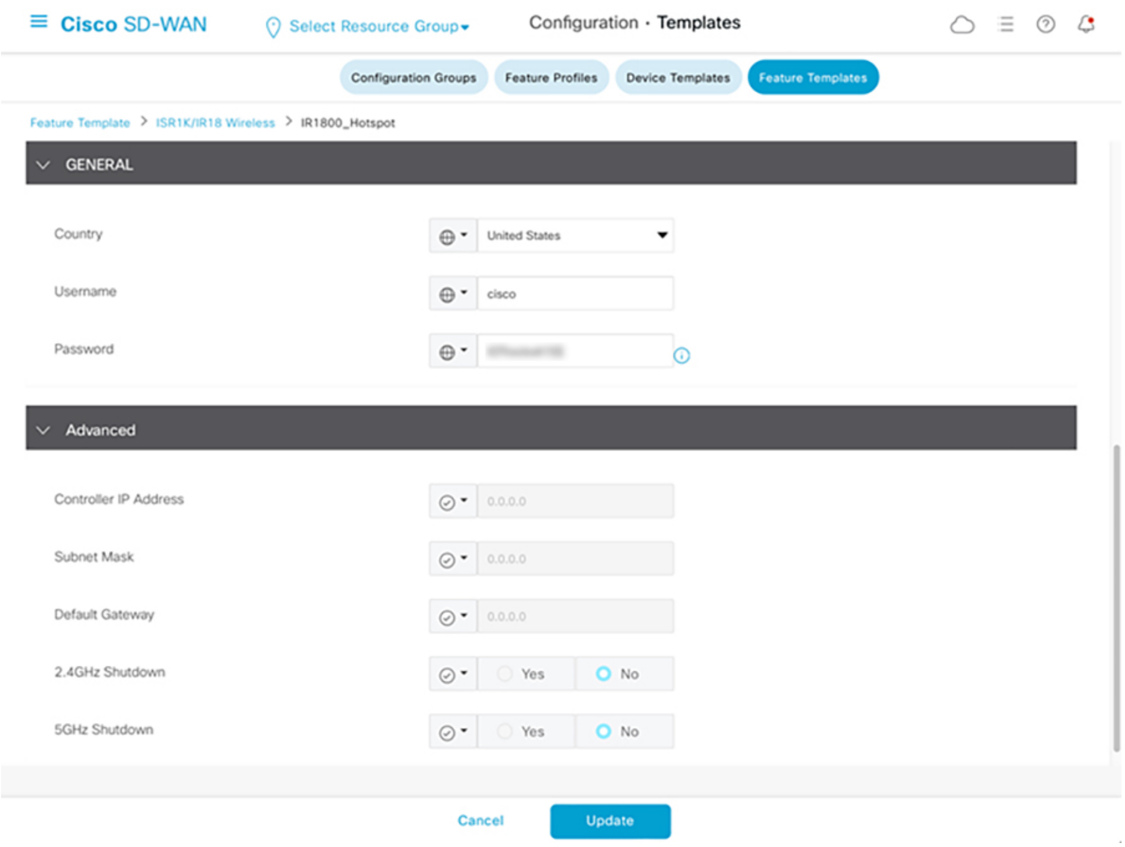
2. Click **New Wi-Fi SSID** and then enter details. Associate it with a specific VLAN. Repeat as needed for multiple VLANs.



Update Tracker

Wireless Network Name (SSID)	1800_V50
VLAN (Range 1-4094)	50
Security Type	○ WPA2 Enterprise ● WPA2 Personal ○ Open
Passphrase	·········
Admin State	● Enabled ○ Disabled
Radio Type	○ 2.4GHz ○ 5GHz ● All
Broadcast SSID	● On ○ Off
QoS Profile	Silver (Best Effort)

3. Enter details for **General** and **Advanced**. The username and password are for the access-point module itself.



Feature Template > ISR1K/IR18 Wireless > IR1800_Hotspot

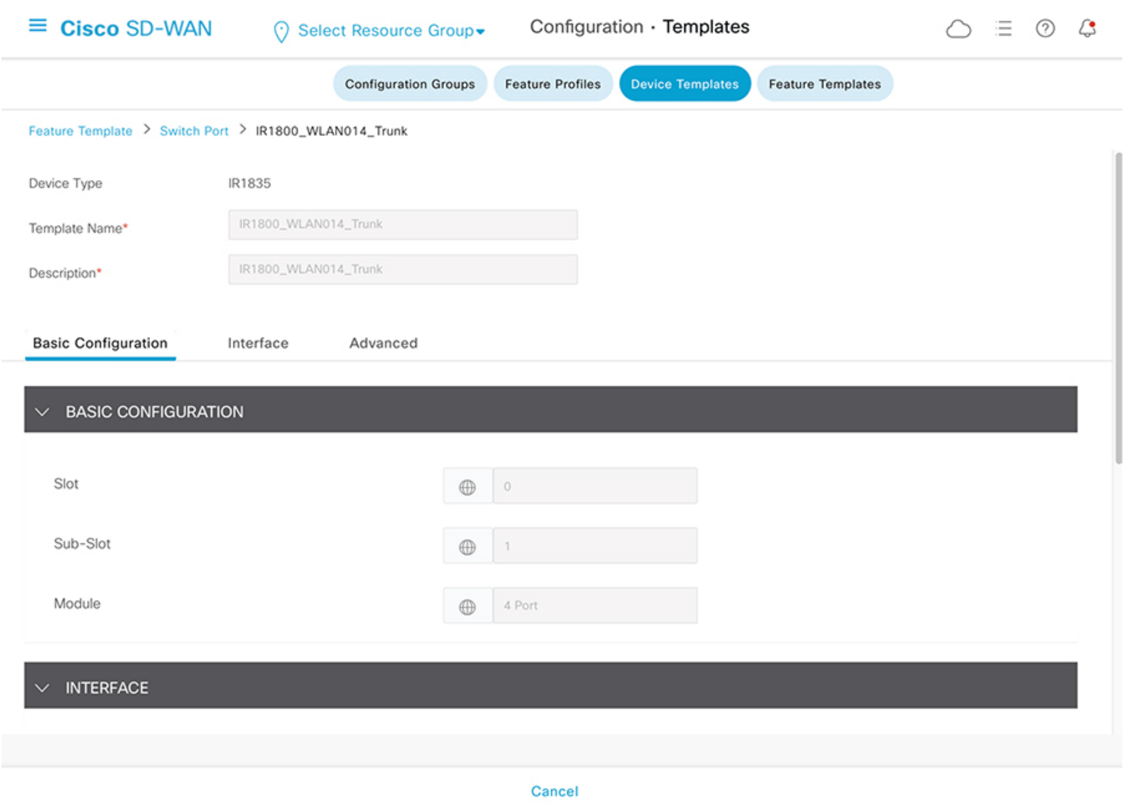
GENERAL

Country	United States
Username	cisco
Password	[redacted]

Advanced

Controller IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
2.4GHz Shutdown	○ Yes ● No
5GHz Shutdown	○ Yes ● No

4. Create a Switch Port feature template to make the Wlan-GigabitEthernet0/1/4 interface into a trunk for the relevant VLANs



Device Type IR1835

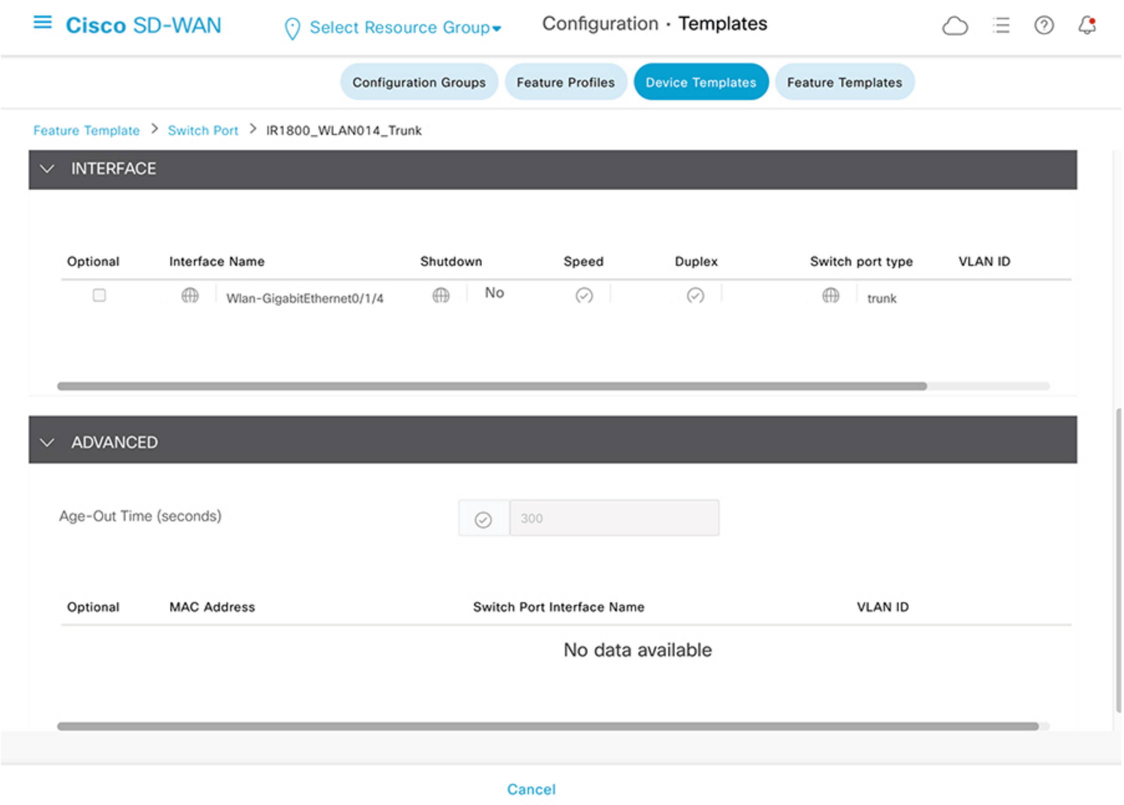
Template Name* IR1800_WLAN014_Trunk

Description* IR1800_WLAN014_Trunk

Slot 0

Sub-Slot 1

Module 4 Port



Feature Template > Switch Port > IR1800_WLAN014_Trunk

INTERFACE

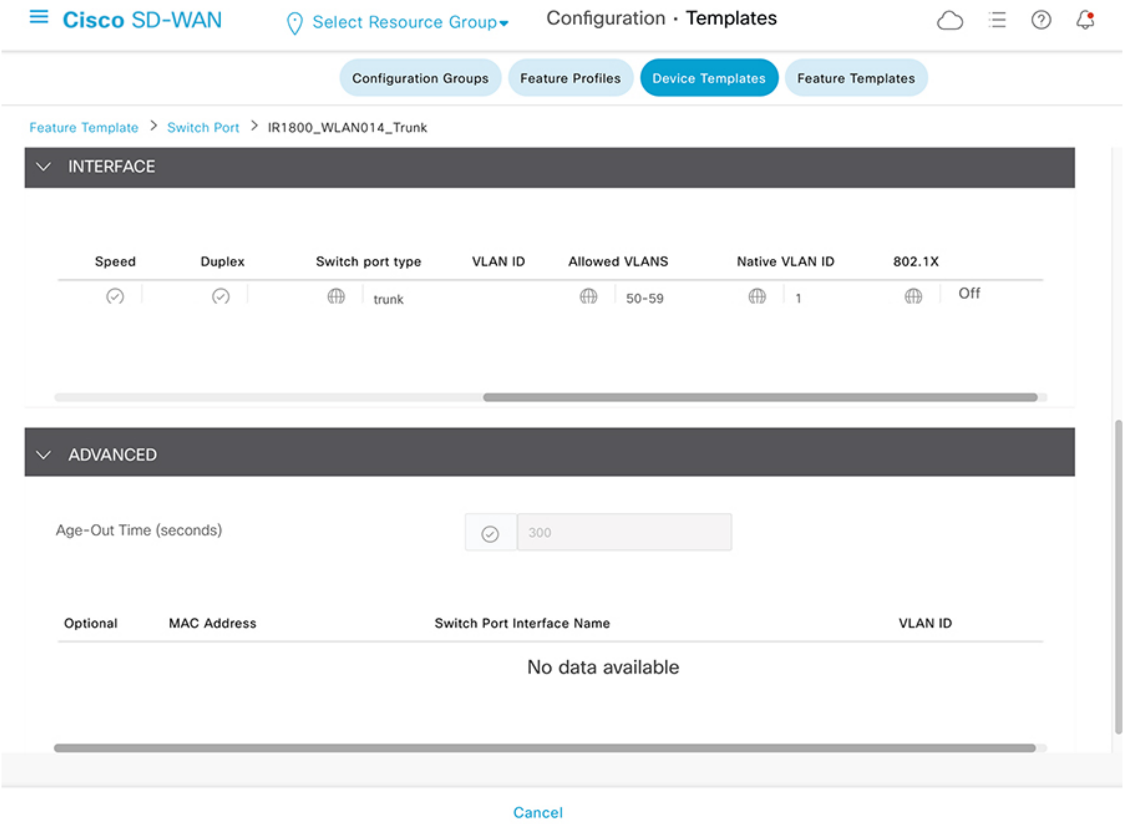
Optional	Interface Name	Shutdown	Speed	Duplex	Switch port type	VLAN ID
□	Wlan-GigabitEthernet0/1/4	No	✓	✓	trunk	

ADVANCED

Age-Out Time (seconds) ✓ 300

Optional	MAC Address	Switch Port Interface Name	VLAN ID

No data available



Feature Template > Switch Port > IR1800_WLAN014_Trunk

INTERFACE

Speed	Duplex	Switch port type	VLAN ID	Allowed VLANS	Native VLAN ID	802.1X
✓	✓	trunk		50-59	1	Off

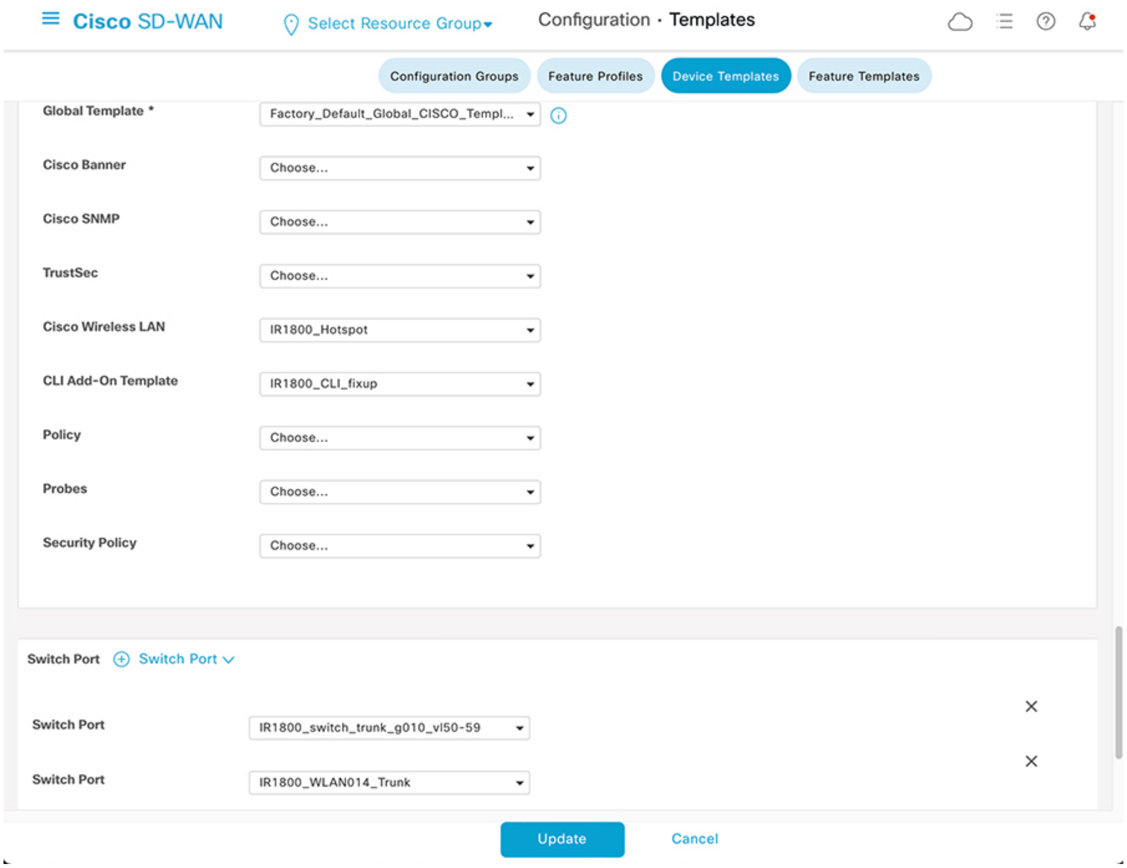
ADVANCED

Age-Out Time (seconds): 300

Optional	MAC Address	Switch Port Interface Name	VLAN ID

No data available

5. Associate the **Cisco Wireless LAN** and **Switch Port** feature templates with the **Device Template**.

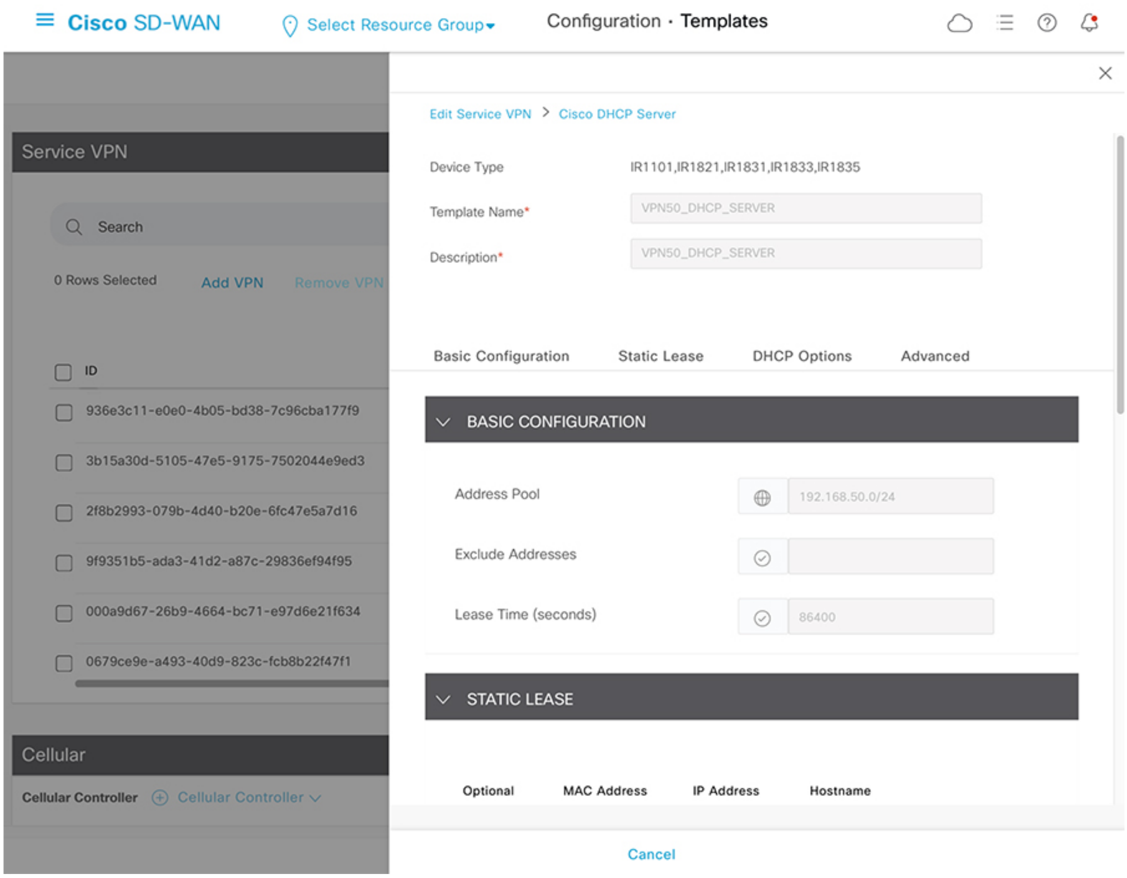


Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
TrustSec	Choose...
Cisco Wireless LAN	IR1800_Hotspot
CLI Add-On Template	IR1800_CLI_fixup
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

Switch Port ⊕ Switch Port

Switch Port	IR1800_switch_trunk_g010_vl50-59
Switch Port	IR1800_WLAN014_Trunk

6. In the **Service VPN** section of the **Device Template**, select the relevant Service VPN and add a new **Cisco DHCP Template**.



Service VPN

Search

0 Rows Selected Add VPN Remove VPN

□ ID

□ 936e3c11-e0e0-4b05-bd38-7c96cba177f9

□ 3b15a30d-5105-47e5-9175-7502044e9ed3

□ 2f8b2993-079b-4d40-b20e-6fc47e5a7d16

□ 9f9351b5-ada3-41d2-a87c-29836ef94f95

□ 000a9d67-26b9-4664-bc71-e97d6e21f634

□ 0679ce9e-a493-40d9-823c-fcb8b22f47f1

Cellular

Cellular Controller: Cellular Controller

Edit Service VPN > Cisco DHCP Server

Device Type: IR1101,IR1821,IR1831,IR1833,IR1835

Template Name*: VPN50_DHCP_SERVER

Description*: VPN50_DHCP_SERVER

Basic Configuration | Static Lease | DHCP Options | Advanced

BASIC CONFIGURATION

Address Pool: 192.168.50.0/24

Exclude Addresses:

Lease Time (seconds): 86400

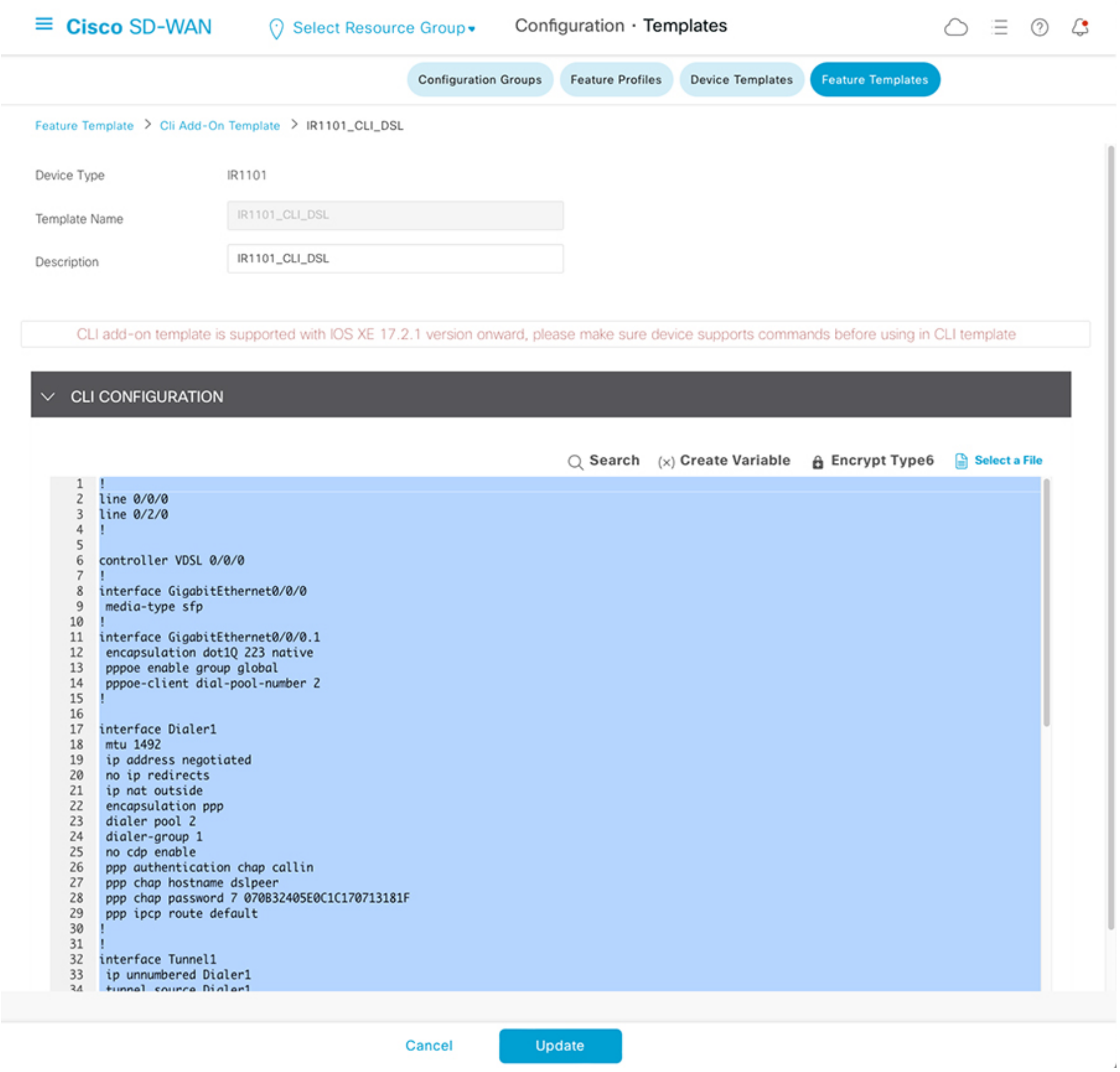
STATIC LEASE

Optional	MAC Address	IP Address	Hostname

Cancel

DSL

1. Create a new CLI Add-on template (or append configuration onto existing one). Using a “VDSL PPPoE VPN Interface” on VPN0 will not work on IR1101 or IR1800.



Device Type IR1101

Template Name IR1101_CLI_DSL

Description IR1101_CLI_DSL

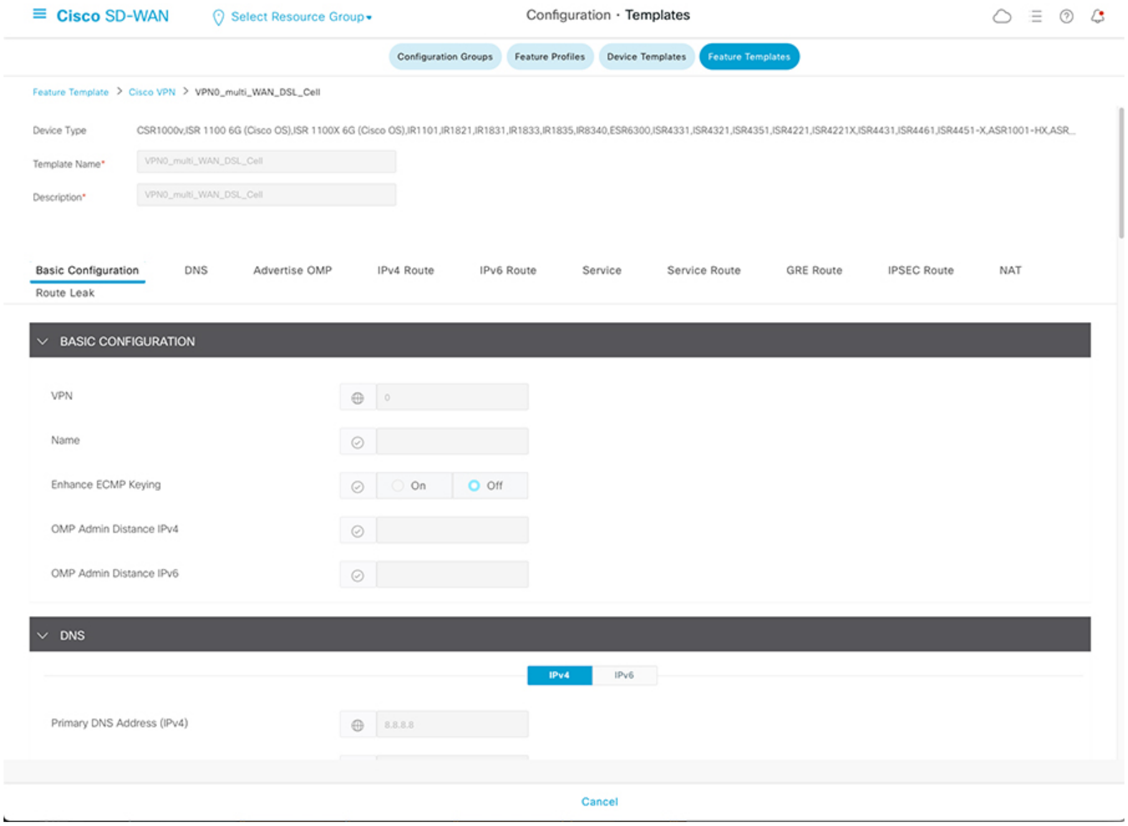
CLI add-on template is supported with IOS XE 17.2.1 version onward, please make sure device supports commands before using in CLI template

```
!
line 0/0/0
line 0/2/0
!

controller VDSL 0/0/0
!
interface GigabitEthernet0/0/0
 media-type sfp
!
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 223 native
 pppoe enable group global
 pppoe-client dial-pool-number 2
!

interface Dialer1
 mtu 1492
 ip address negotiated
 no ip redirects
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dslpeer
 ppp chap password 7 070B32405E0C1C170713181F
 ppp ipcp route default
!
!
interface Tunnel1
 ip unnumbered Dialer1
 tunnel source Dialer1
```

```
!
line 0/0/0
line 0/2/0
!

controller VDSL 0/0/0
!
interface GigabitEthernet0/0/0
 media-type sfp
!
interface GigabitEthernet0/0/0.1
```

```
 encapsulation dot1Q 223 native
 pppoe enable group global
 pppoe-client dial-pool-number 2
!

interface Dialer1
 mtu 1492
 ip address negotiated
 no ip redirects
 ip nat outside
 encapsulation ppp
 dialer pool 2
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dslpeer
 ppp chap password 7 070B32405E0C1C170713181F
 ppp ipcp route default
!
!
interface Tunnel1
 ip unnumbered Dialer1
 tunnel source Dialer1
 tunnel mode sdwan
!

sdwan
 interface Dialer1
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color default
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
exit
ip route 0.0.0.0 0.0.0.0 Dialer1 5
exit
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 1
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
!
```

2. Create or modify a Cisco VPN feature template for **VPN 0** to point to a new Next Hop with a destination of **Dialer1**.



Device Type CSR1000v,ISR 1100 6G (Cisco OS),ISR 1100X 6G (Cisco OS),IR1101,IR1821,IR1831,IR1833,IR1835,IR8340,ESR6300,ISR4331,ISR4321,ISR4351,ISR4221,ISR4221X,ISR4431,ISR4461,ISR4451-X,ASR1001-HX,ASR...

Template Name* VPN0_multi_WAN_DSL_Cell

Description* VPN0_multi_WAN_DSL_Cell

VPN 0

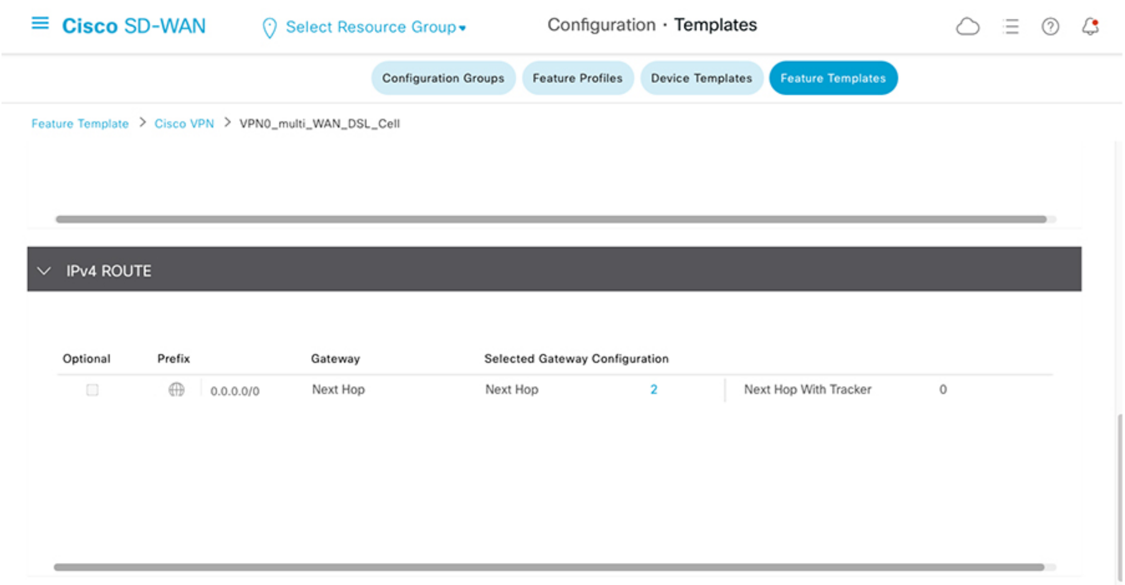
Name

Enhance ECMP Keying ○ On ● Off

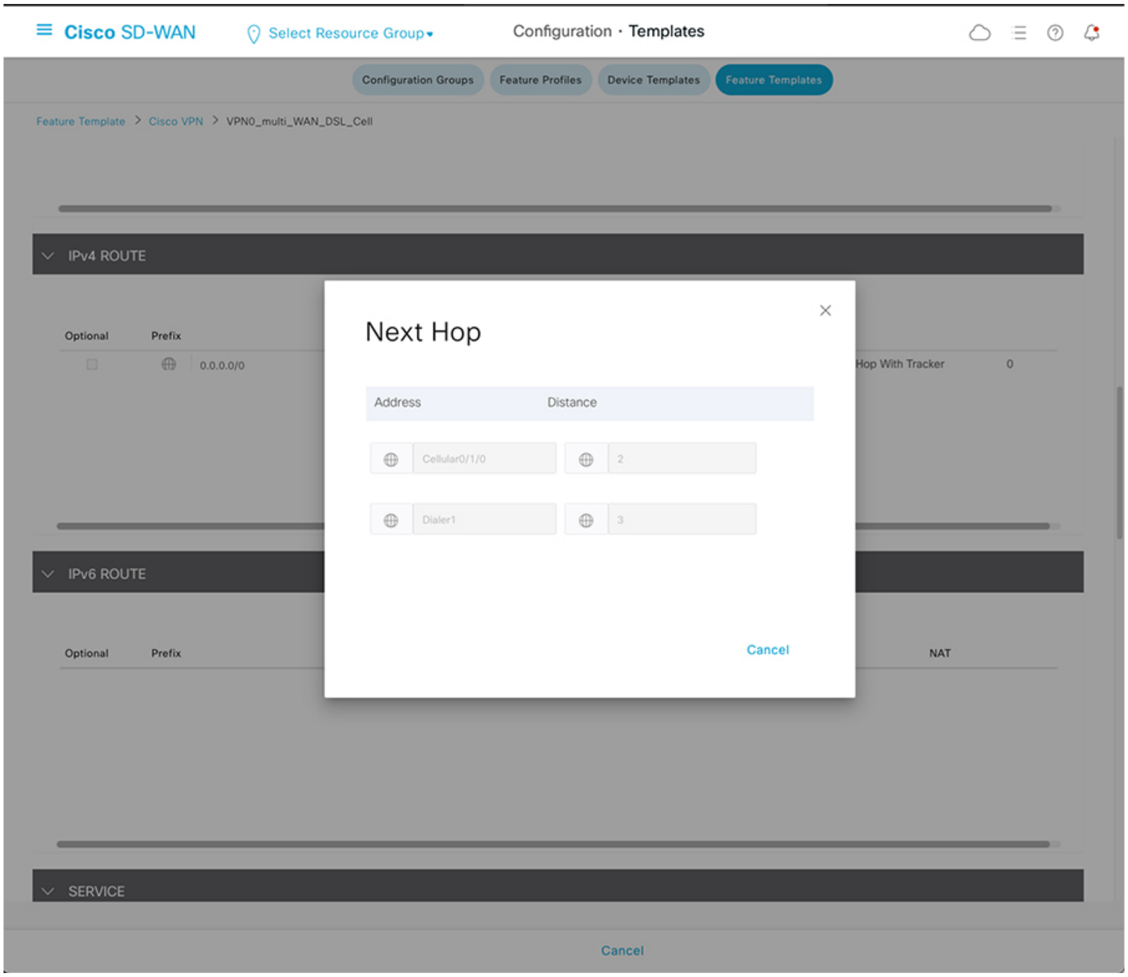
OMP Admin Distance IPv4

OMP Admin Distance IPv6

Primary DNS Address (IPv4) 8.8.8.8



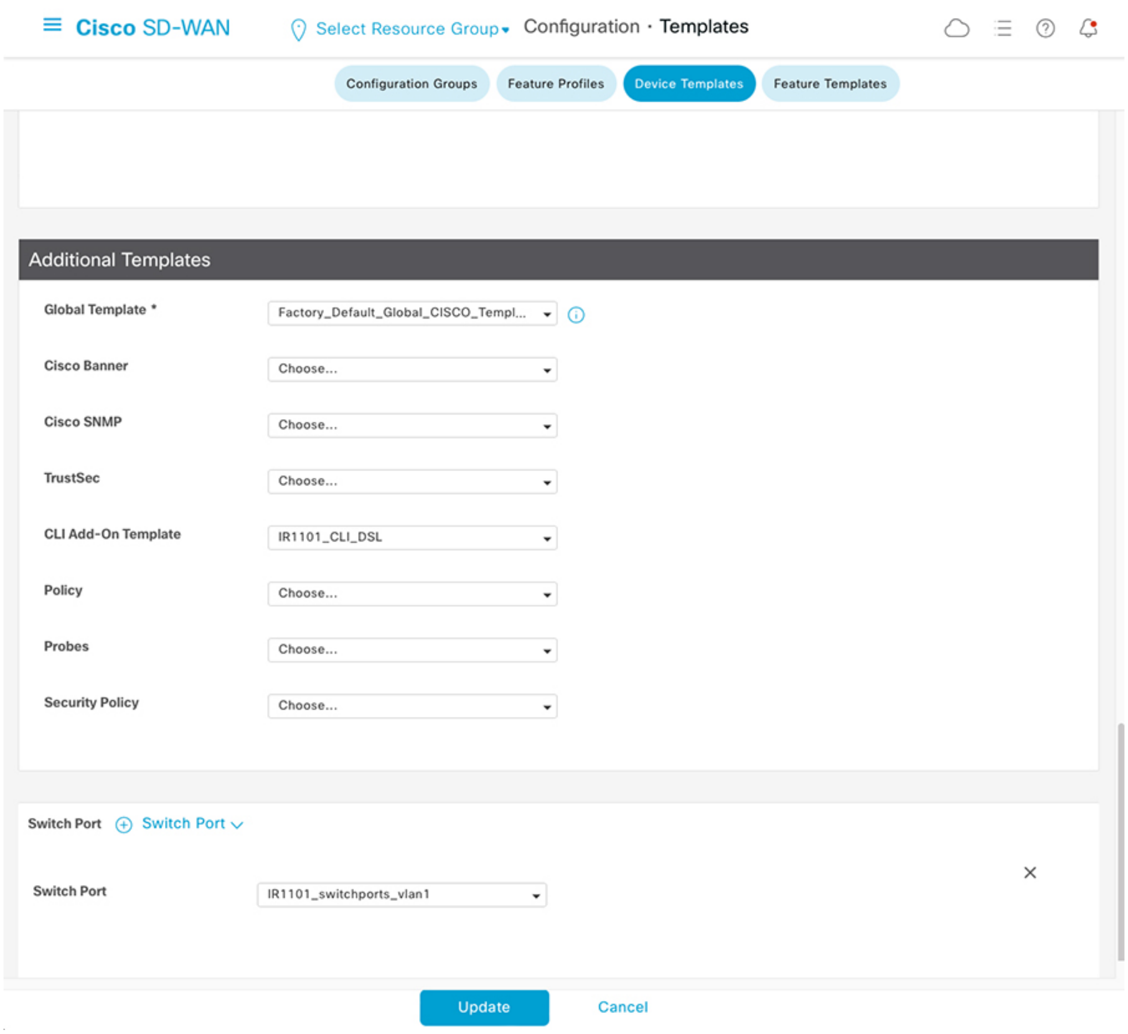
Optional	Prefix	Gateway	Selected Gateway Configuration			
□	0.0.0.0/0	Next Hop	Next Hop	2	Next Hop With Tracker	0



Next Hop

Address	Distance
Cellular0/1/0	2
Dialer1	3

3. Associate the CLI Add-on template to the Device template.



Additional Templates

Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
TrustSec	Choose...
CLI Add-On Template	IR1101_CLI_DSL
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

Switch Port ⊕ Switch Port

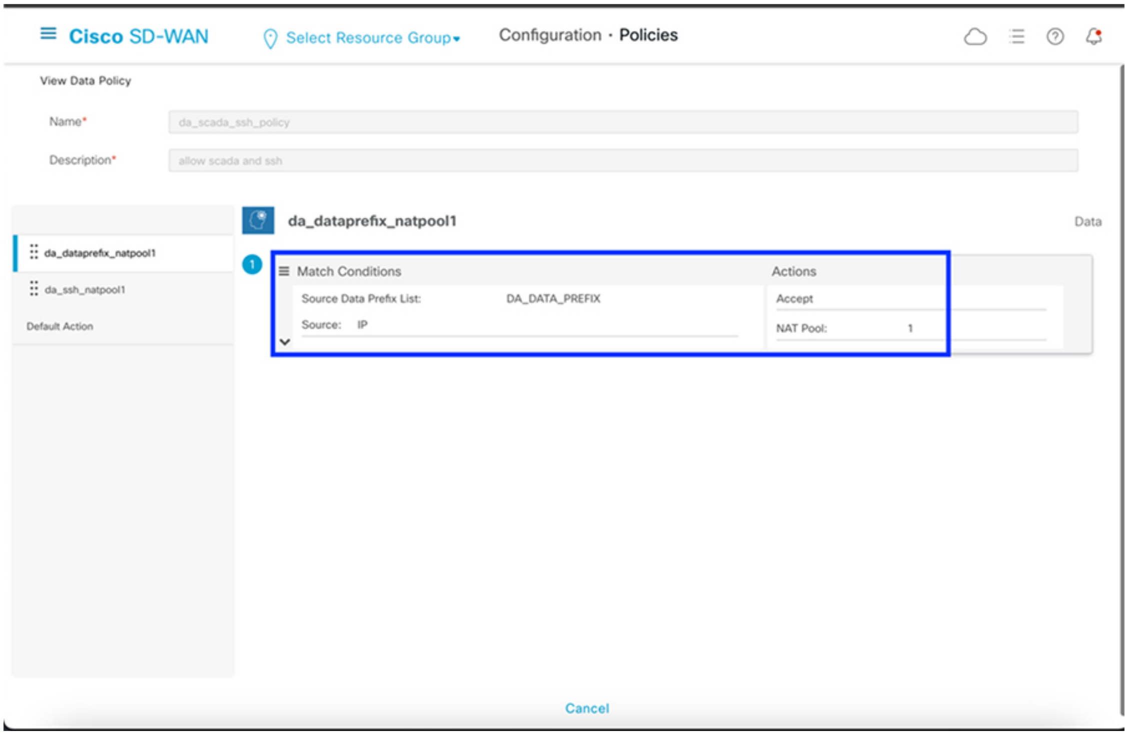
Switch Port	IR1101_switchports_vlan1

NAT Configurations

Configuration for the following section corresponds to the "Static 1:1 NAT, Static N:1 Port Forwarding" section.

Centralized control policy definition

The following definition of Centralized policy configuration can be configured as under the "Traffic Data" definition of "Traffic Rules" section.



View Data Policy

Name* da_scada_ssh_policy

Description* allow scada and ssh

da_dataprefix_natpool1

da_ssh_natpool1

Default Action

da_dataprefix_natpool1

1 Match Conditions

Source Data Prefix List: DA_DATA_PREFIX

Source: IP

Actions

Accept

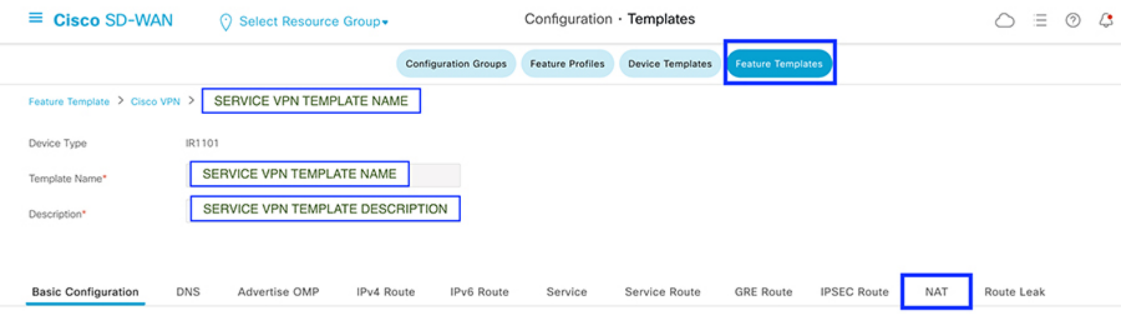
NAT Pool: 1

Match criteria:

- DATA_PREFIX matches on “192.168.0.0/24” subnet.
- Match condition:
  - Match on Source IP
  - Match on Source Data prefix list: DATA_PREFIX
- Action: Accept
  - With NAT pool: 1

NAT pool definition:

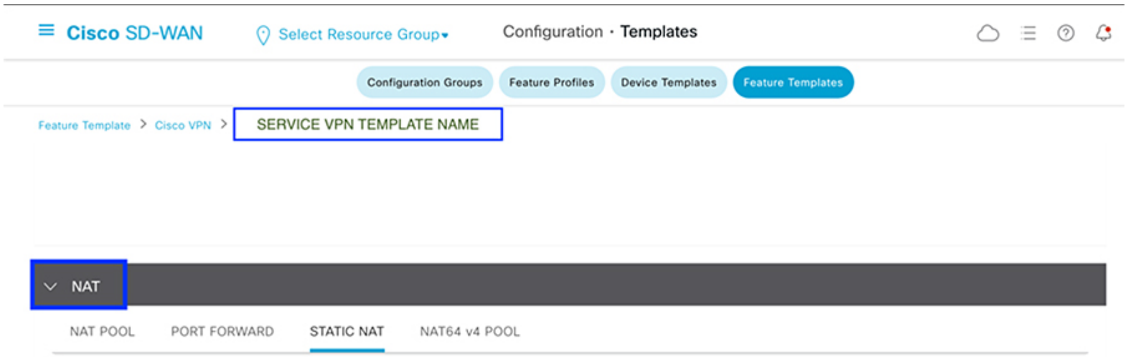
“NAT subsection” configuration is available under **Feature Template** of service VPN configuration.



Device Type IR1101

Template Name* SERVICE VPN TEMPLATE NAME

Description* SERVICE VPN TEMPLATE DESCRIPTION



For the NAT pool definition, refer to the figure **Example of NAT pool1** definition.

Static 1:1 NAT

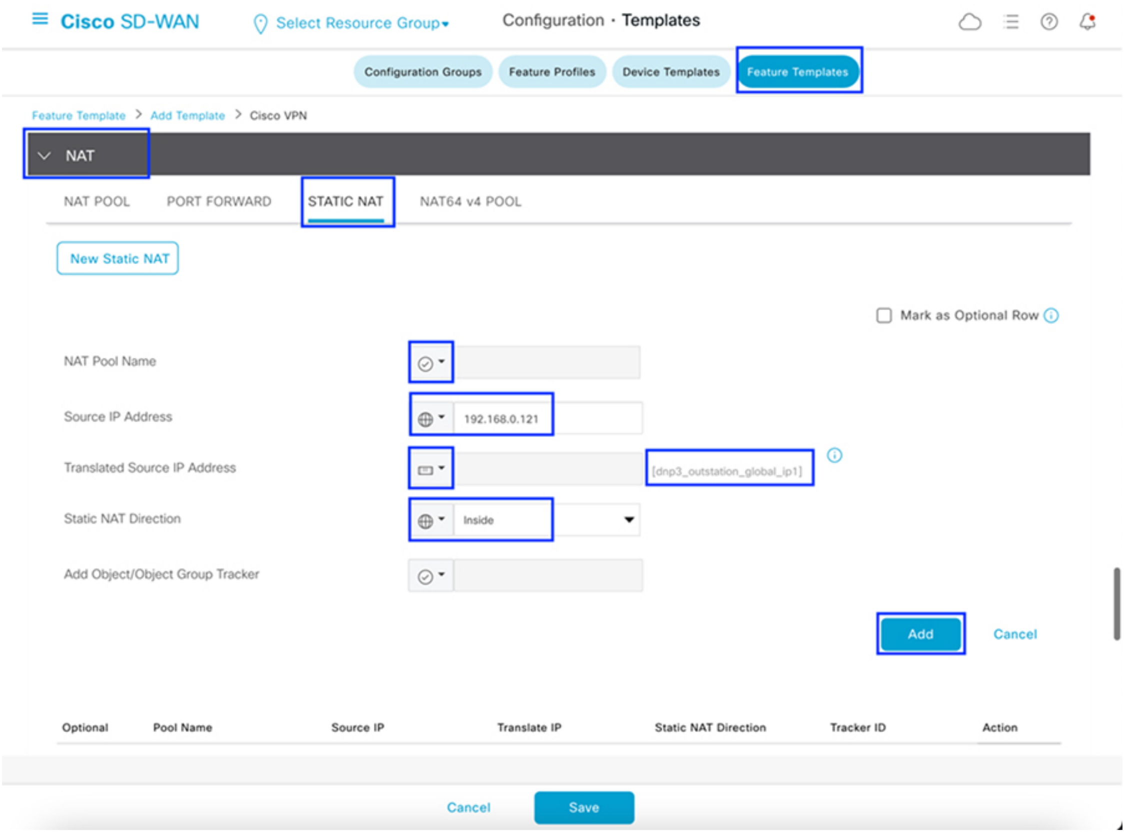
This configuration corresponds to "STATIC NAT" section under **NAT**.

This example assumes a scenario, where two DNP3 outstations and one camera were enabled for connectivity with a Cisco SD-WAN Edge Router.

Source IP Address	Translated Source IP Address
192.168.0.121	dnp3_end_device_global_ip1
192.168.0.122	dnp3_end_device_global_ip2
192.168.0.201	camera_global_ip1

1. Click **New Static NAT** to create a new entry.

Here is an example definition for representing "192.168.0.121" end device with "Translated Source IP Address" represented by "dnp3_end_device_global_ip1" variable.



Feature Template > Add Template > Cisco VPN

NAT

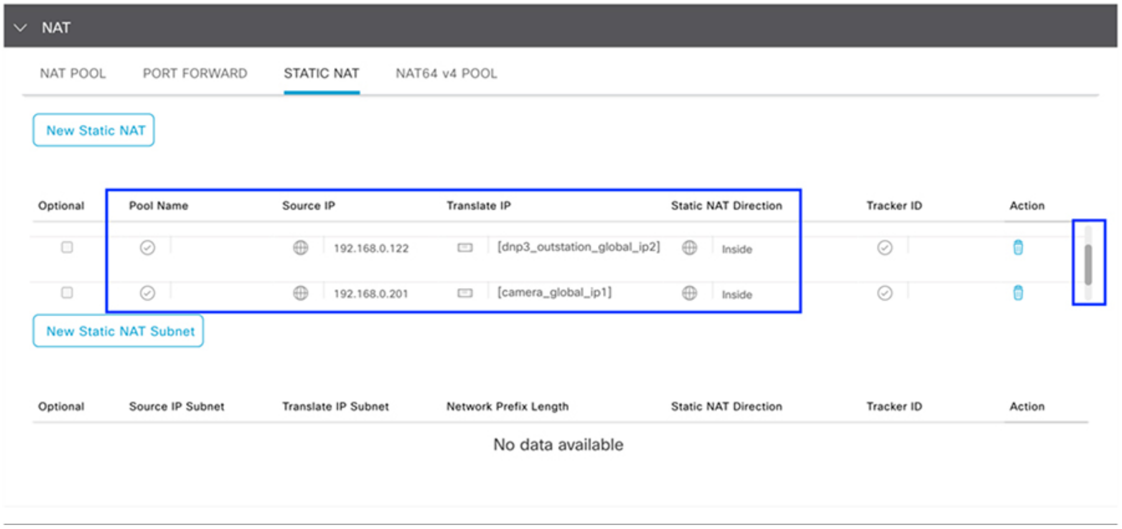
□ Mark as Optional Row

NAT Pool Name	
Source IP Address	192.168.0.121
Translated Source IP Address	[dnp3_outstation_global_ip1]
Static NAT Direction	Inside
Add Object/Object Group Tracker	

Optional	Pool Name	Source IP	Translate IP	Static NAT Direction	Tracker ID	Action

2. Similarly, entries can be created for two end devices shown below. When you finish the configuration, click **Save** to save it.

- 192.168.0.122 - dnp3_end_device_global_ip2
- 192.168.0.201 - camera_global_ip1



Optional	Pool Name	Source IP	Translate IP	Static NAT Direction	Tracker ID	Action
□		192.168.0.122	[dnp3_outstation_global_ip2]	Inside		
□		192.168.0.201	[camera_global_ip1]	Inside		

Optional	Source IP Subnet	Translate IP Subnet	Network Prefix Length	Static NAT Direction	Tracker ID	Action

No data available

NAT Port Forwarding

This configuration corresponds to the “PORT FORWARD” section under **NAT**.

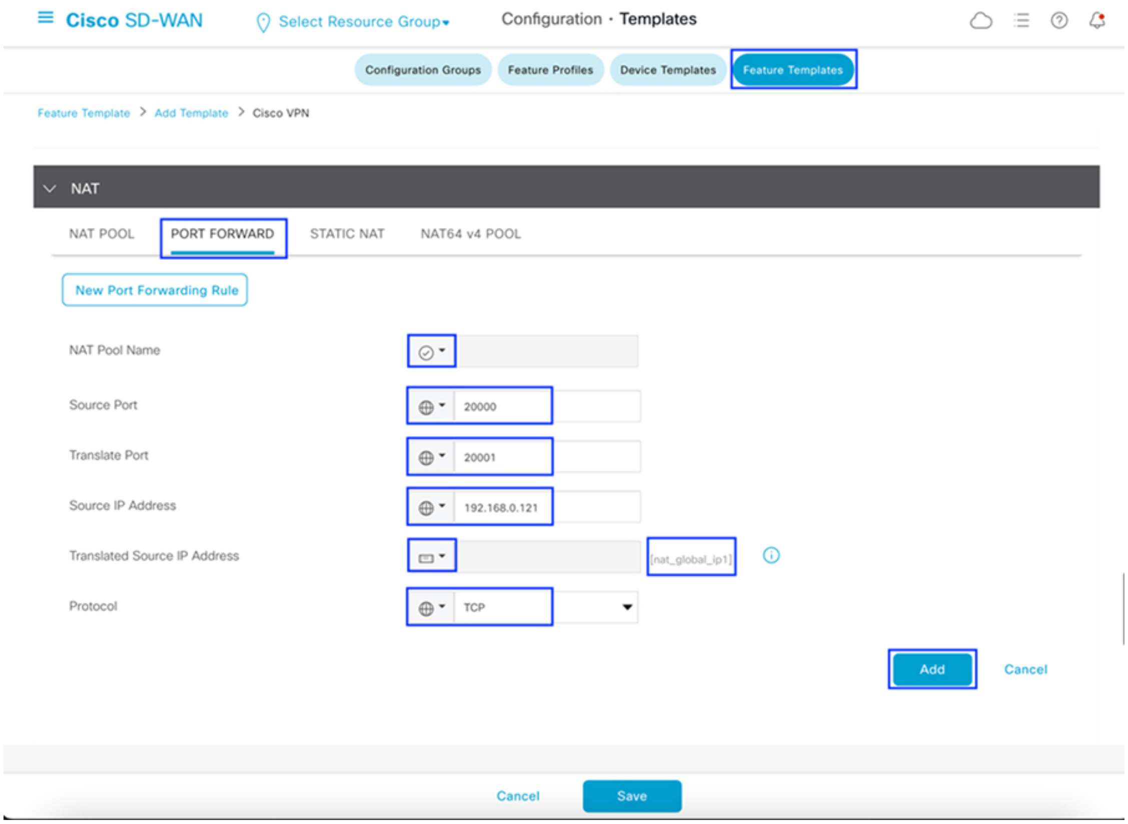
To facilitate a one-to-one comparison in config between “STATIC NAT” and “PORT FORWARD”, the same example scenario is chosen, where two DNP3 outstations and one camera were enabled for connectivity with the Cisco SD-WAN Edge Router. This time, it is with the port forward example.

Description of the End device	Source IP Address	Source Port	Translated Source IP Address	Translate Port (Must be Unique)
DNP3 device 1	192.168.0.121	20000	nat_global_ip1	20001
DNP3 device 2	192.168.0.122	20000		20002
Camera 1	192.168.0.201	80		40001

1. Under **PORT FORWARD**, click **New Port Forwarding Rule** to create a new entry.

This is an example definition for representing “192.168.0.121” end device listening on port 20000 with “Translated Source IP Address” represented by “nat_global_ip1” variable on port 20001.

For the Operations center to communicate with DNP3 device 1 on port 20000, it talks to IP “nat_global_ip1” and port 20001, which in turn is translated and forwarded to the 192.168.0.121 end device on port 20000.



NAT Pool Name

Source Port 20000

Translate Port 20001

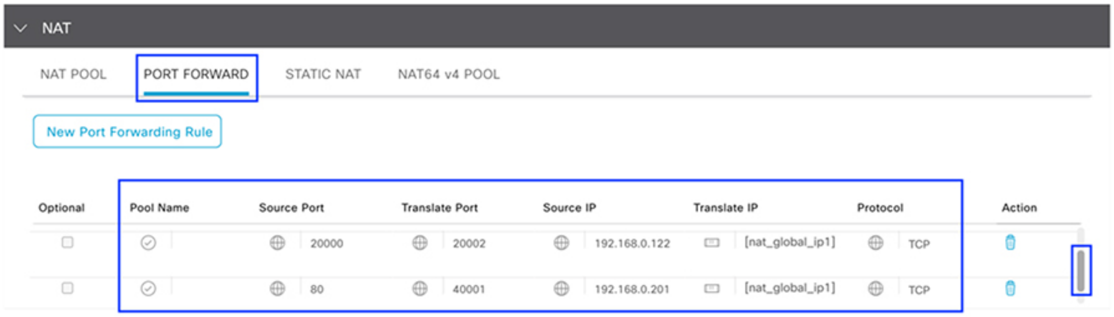
Source IP Address 192.168.0.121

Translated Source IP Address [nat_global_ip1]

Protocol TCP

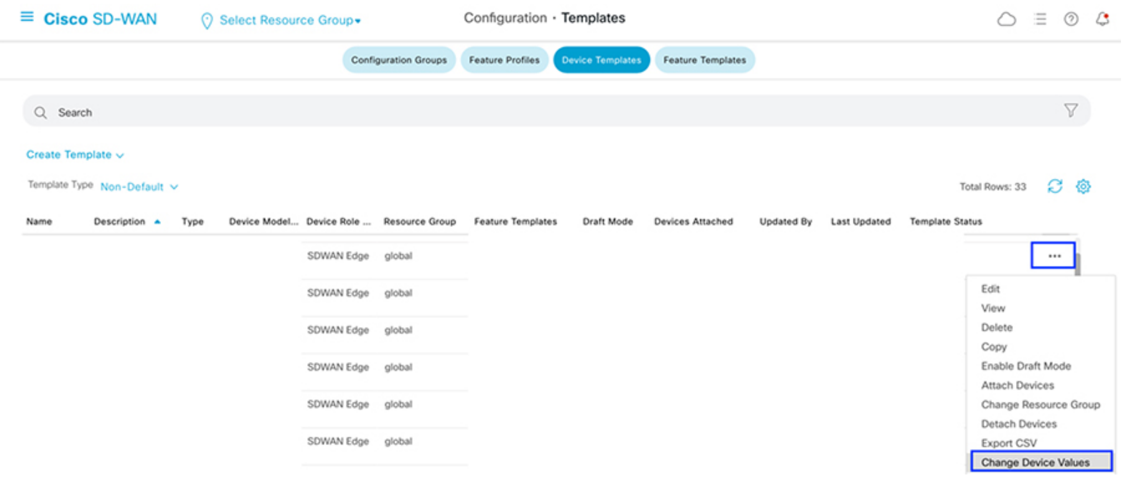
2. In a similar way, entries can be created below for two end devices. When you are finished with the configuration, click **Save** to save it.

Description of the End device	Source IP Address	Source Port	Translated Source IP Address	Translate Port (Must be Unique)
DNP3 device 2	192.168.0.122	20000	nat_global_ip1	20002
Camera 1	192.168.0.201	80		40001



Optional	Pool Name	Source Port	Translate Port	Source IP	Translate IP	Protocol	Action
□		20000	20002	192.168.0.122	[nat_global_ip1]	TCP	
□		80	40001	192.168.0.201	[nat_global_ip1]	TCP	

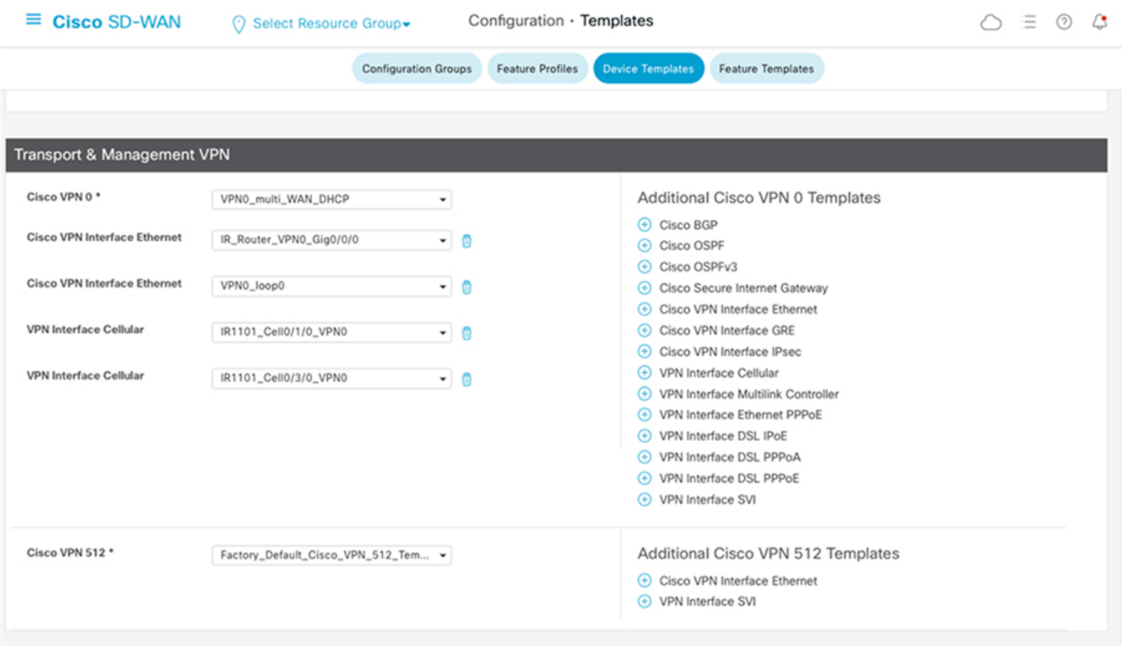
3. When the configuration is pushed to the device or when the template is attached to a device, key variables like “nat_global_ip1”, “dnp3_end_device_global_ip1”, “dnp3_end_device_global_ip2” and “camera_global_ip1” can be populated by the vManage user. The figure that follows shows one way of setting these values using **Change Device Values**.



Name	Description	Type	Device Model...	Device Role ...	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
				SDWAN Edge	global						
				SDWAN Edge	global						
				SDWAN Edge	global						
				SDWAN Edge	global						
				SDWAN Edge	global						
				SDWAN Edge	global						

WAN Dual Active Cellular with Load Balancing

1. From the device template, or main feature template page, create a new Cisco VPN 0 template.



Transport & Management VPN

Cisco VPN 0 * VPN0_multi_WAN_DHCP

Cisco VPN Interface Ethernet IR_Router_VPN0_Gig0/0/0

Cisco VPN Interface Ethernet VPN0_loop0

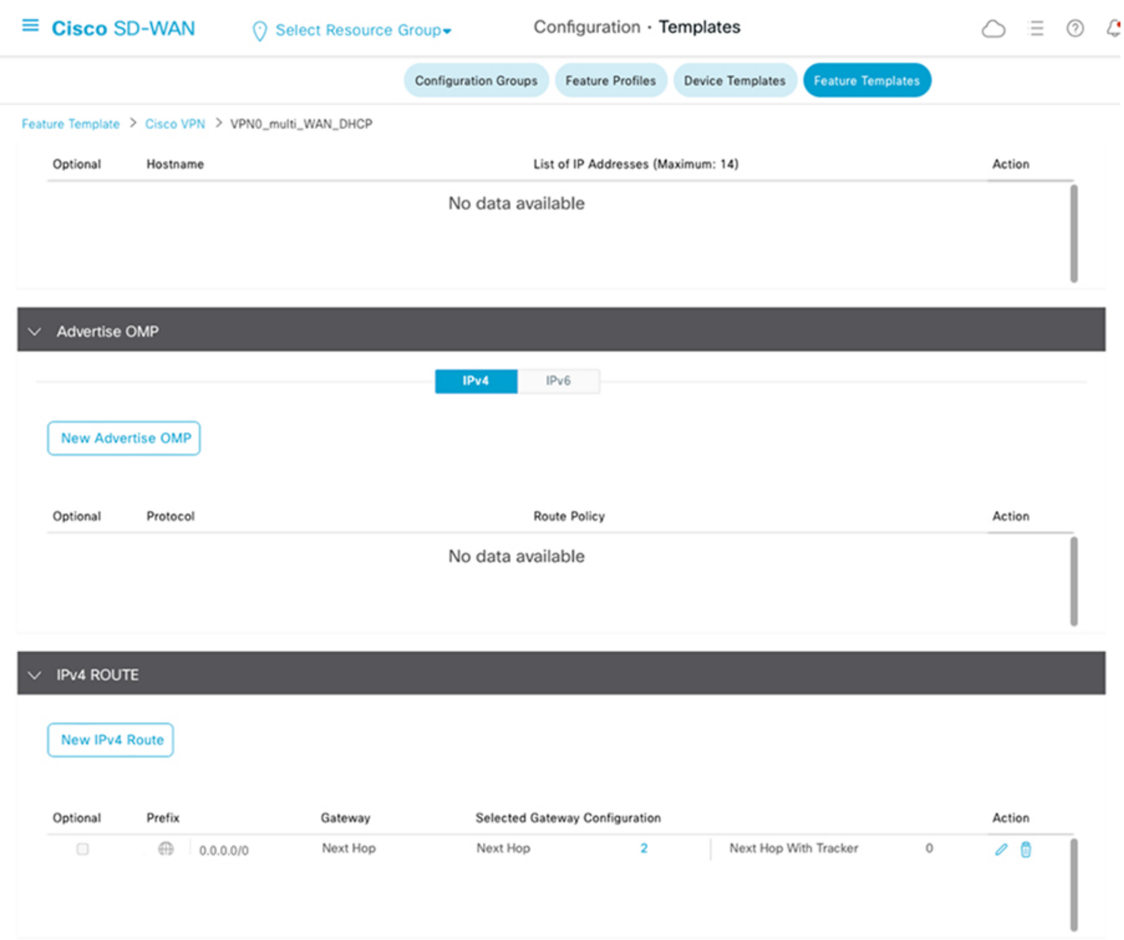
VPN Interface Cellular IR1101_Cell0/1/0_VPN0

VPN Interface Cellular IR1101_Cell0/3/0_VPN0

Cisco VPN 512 * Factory_Default_Cisco_VPN_512_Tem...

Additional Cisco VPN 0 Templates
Cisco BGP
Cisco OSPF
Cisco OSPFv3
Cisco Secure Internet Gateway
Cisco VPN Interface Ethernet
Cisco VPN Interface GRE
Cisco VPN Interface IPsec
VPN Interface Cellular
VPN Interface Multilink Controller
VPN Interface Ethernet PPPoE
VPN Interface DSL IPoE
VPN Interface DSL PPPoA
VPN Interface DSL PPPoE
VPN Interface SVI
Additional Cisco VPN 512 Templates
Cisco VPN Interface Ethernet
VPN Interface SVI

2. Within the Cisco VPN 0 feature template, add a **New IPv4 Route**.



Cisco SD-WAN　Select Resource Group　Configuration · Templates

Configuration Groups　Feature Profiles　Device Templates　Feature Templates

Feature Template > Cisco VPN > VPN0_multi_WAN_DHCP

Optional	Hostname	List of IP Addresses (Maximum: 14)	Action
		No data available	

Advertise OMP

IPv4　IPv6

New Advertise OMP

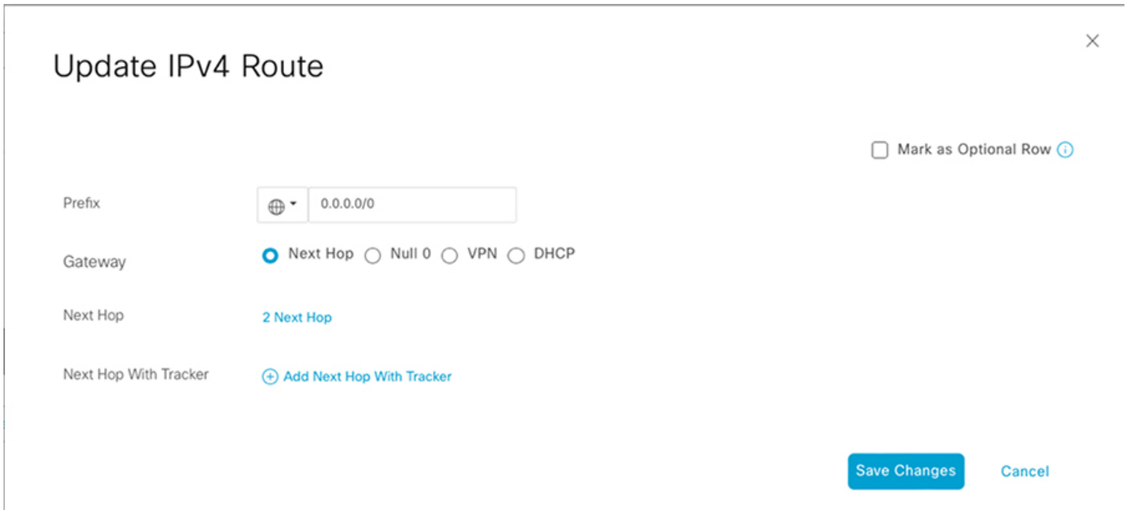
Optional	Protocol	Route Policy	Action
		No data available	

IPv4 ROUTE

New IPv4 Route

Optional	Prefix	Gateway	Selected Gateway Configuration				Action
□	0.0.0.0/0	Next Hop	Next Hop	2	Next Hop With Tracker	0	

3. Add a default route, prefix 0.0.0.0/0, with the Router set to **Next Hop**.



Update IPv4 Route

□ Mark as Optional Row

Prefix: 0.0.0.0/0

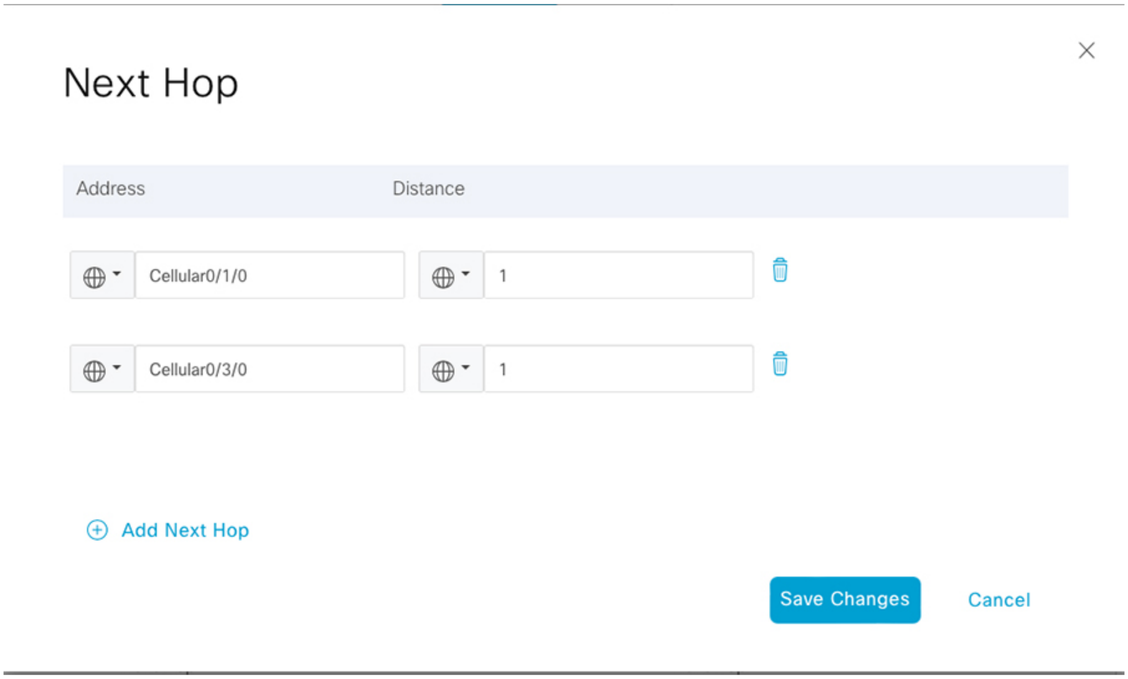
Gateway: ● Next Hop ○ Null 0 ○ VPN ○ DHCP

Next Hop: 2 Next Hop

Next Hop With Tracker: ⊕ Add Next Hop With Tracker

Save Changes　Cancel

4. Add in two next hop addresses, set to the Cellular interface names, each with the same distance metric. Having two equal cost paths active will trigger the ECMP load balancing.



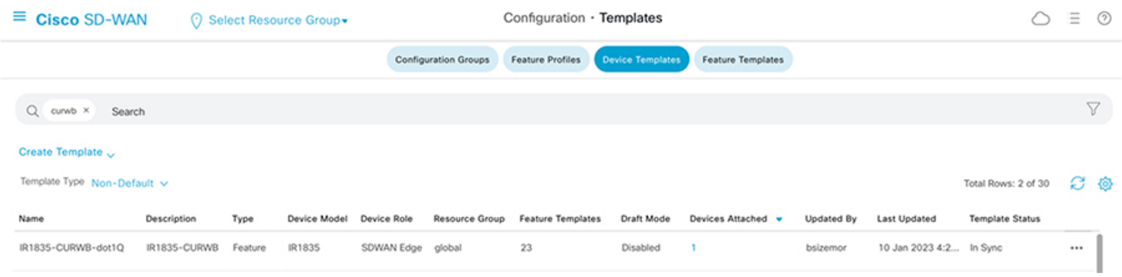
Next Hop

Address	Distance
Cellular0/1/0	1
Cellular0/3/0	1

WAN Failover – CURWB (primary) and Cellular (backup)

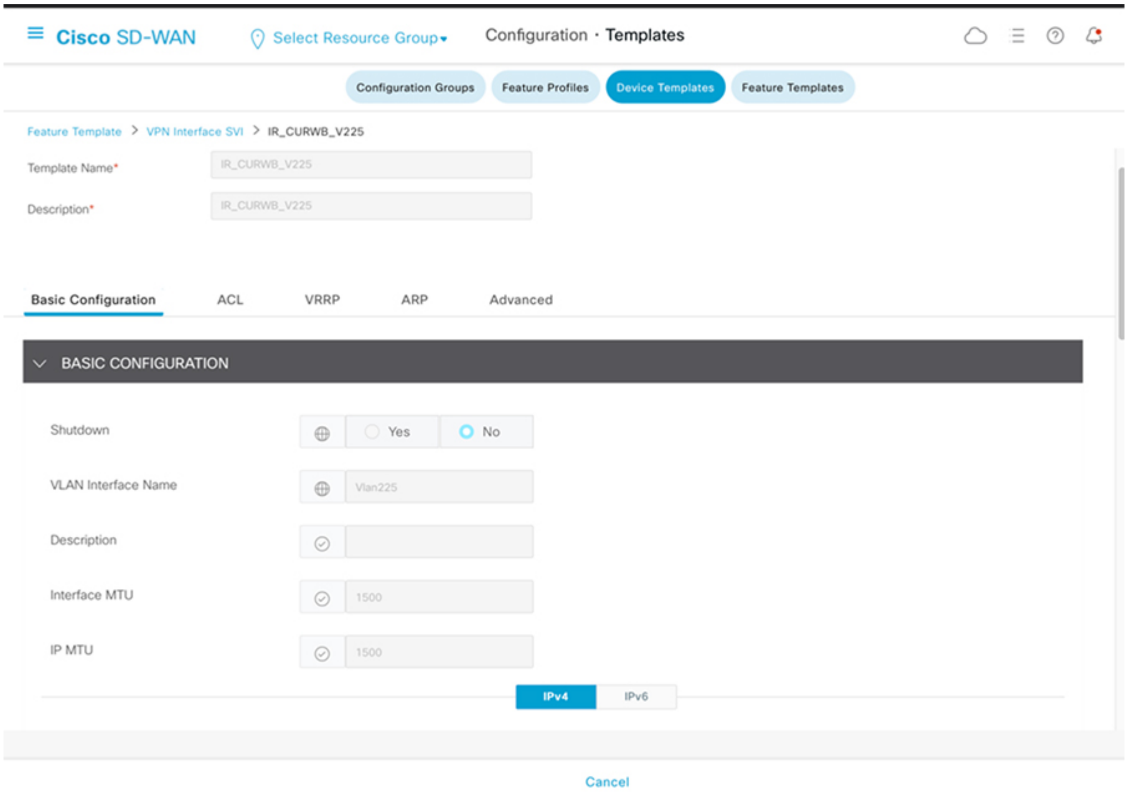
This configuration allows the router to utilize an external IW9167 CURWB radio for a WAN link. The IW9167 is connected to the router (IR1835 in this example) via the switchport interface Gig0/1/0 which is configured as a trunk, and an SVI interface is configured as the layer 3 VPN interface. IPsec preference is used to make the CURWB interface the preferred VPN interface.

1. Create or modify a device template for the router that will be used to pull together all of the relevant feature templates.



Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
IR1835-CURWB-dot1Q	IR1835-CURWB	Feature	IR1835	SDWAN Edge	global	23	Disabled	1	bsizemor	10 Jan 2023 4:2...	In Sync

2. Create a VPN Interface SVI feature template. This creates the SVI interface for VLAN 225 in this example, that will act as a WAN interface. VLAN 225 will be trunked over the switchport and through the CURWB wireless link to the far side network.



Template Name* IR_CURWB_V225

Description* IR_CURWB_V225

Shutdown ○ Yes ● No

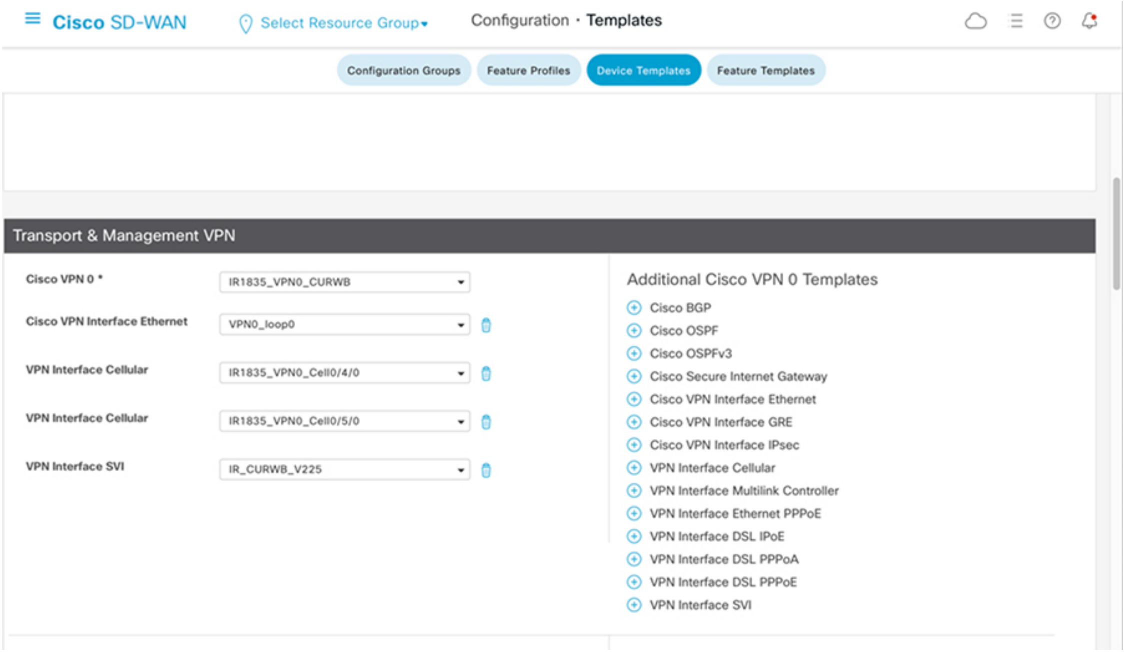
VLAN Interface Name Vlan225

Description

Interface MTU 1500

IP MTU 1500

3. The VPN Interface SVI feature template is referenced in the device template **Transport & Management VPN** section.



Cisco VPN 0 * IR1835_VPN0_CURWB

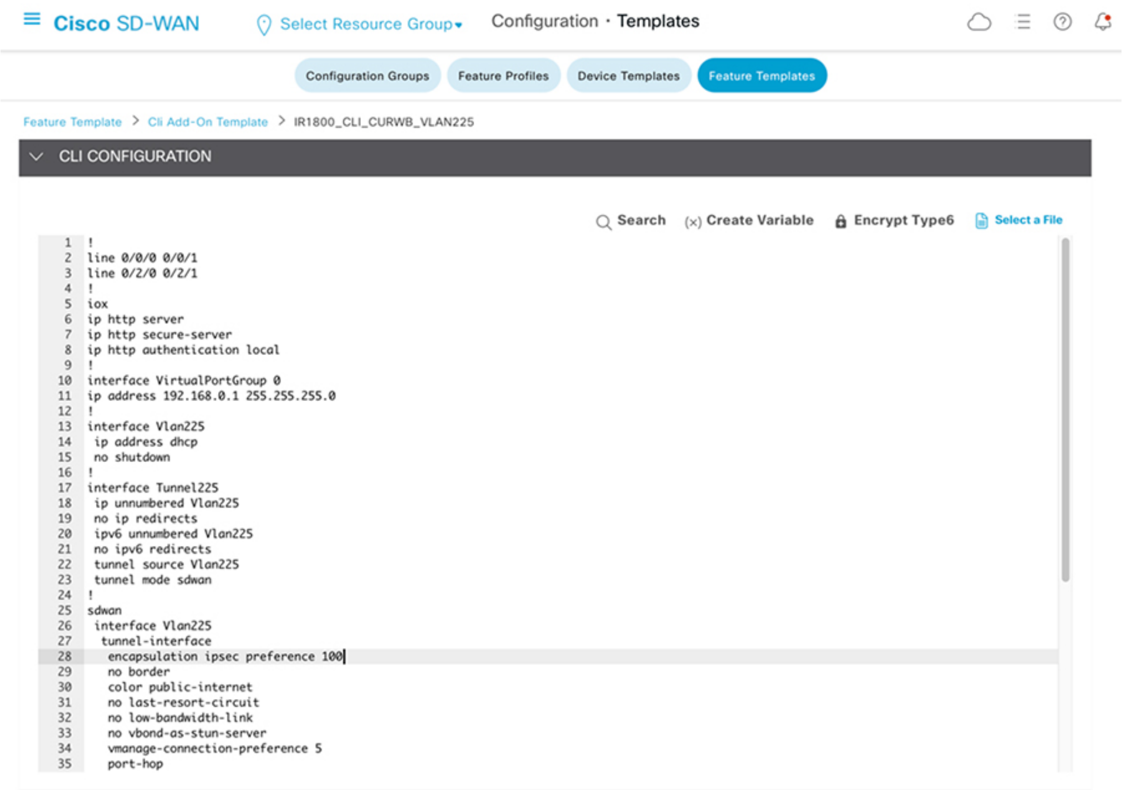
Cisco VPN Interface Ethernet VPN0_loop0

VPN Interface Cellular IR1835_VPN0_Cell0/4/0

VPN Interface Cellular IR1835_VPN0_Cell0/5/0

VPN Interface SVI IR_CURWB_V225

4. Create or modify a CLI Add-on template for the router. The CLI Add-on template will need to be used to specify the required VPN parameters for the SVI interface.

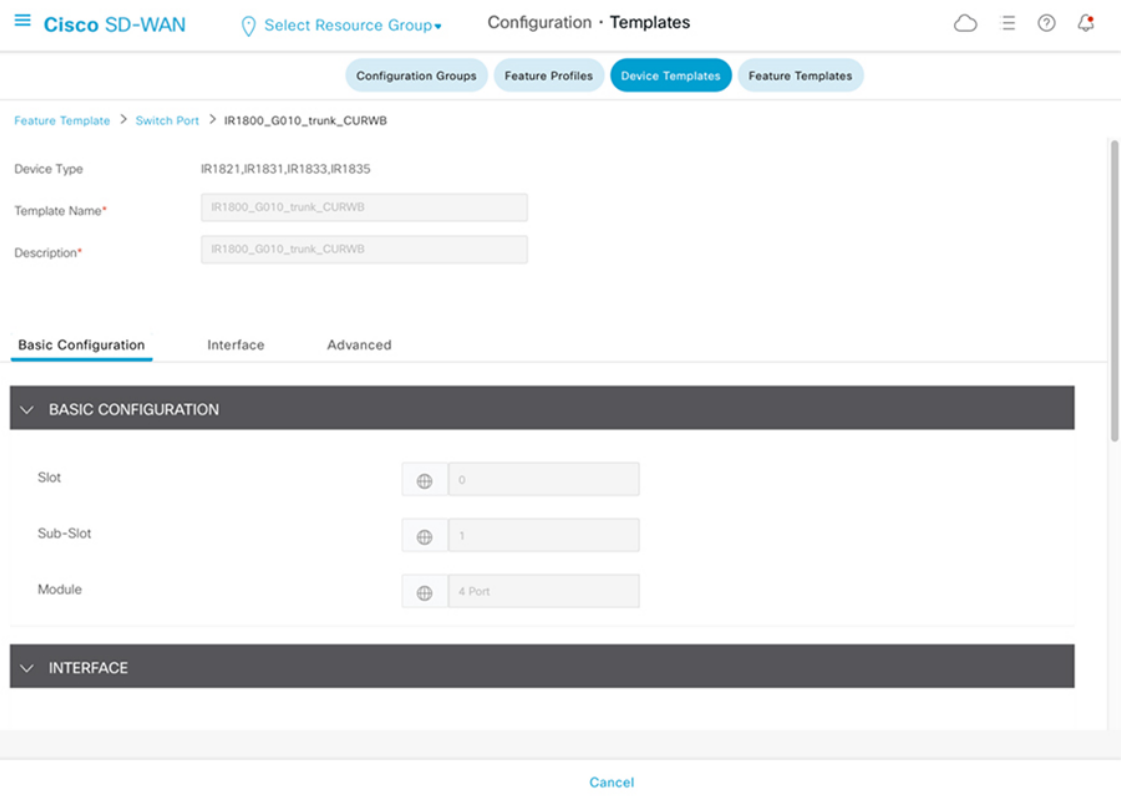


```
!
line 0/0/0 0/0/1
line 0/2/0 0/2/1
!
iox
ip http server
ip http secure-server
ip http authentication local
!
interface VirtualPortGroup 0
ip address 192.168.0.1 255.255.255.0
!
interface Vlan225
 ip address dhcp
 no shutdown
!
interface Tunnel225
 ip unnumbered Vlan225
 no ip redirects
 ipv6 unnumbered Vlan225
 no ipv6 redirects
 tunnel source Vlan225
 tunnel mode sdwan
!
sdwan
 interface Vlan225
  tunnel-interface
   encapsulation ipsec preference 100
   no border
   color public-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
```

5. The contents of the tested CLI template are listed below, including the ipsec preference of “100” which gives it priority over the other WAN interfaces that have a default value of “0”.

```
!

line 0/0/0 0/0/1

line 0/2/0 0/2/1

!

iox

ip http server

ip http secure-server

ip http authentication local

!

interface VirtualPortGroup 0

ip address 192.168.0.1 255.255.255.0

!

interface Vlan225

 ip address dhcp
 no shutdown
!
interface Tunnel225
 ip unnumbered Vlan225
 no ip redirects
 ipv6 unnumbered Vlan225
 no ipv6 redirects
 tunnel source Vlan225
 tunnel mode sdwan
!
sdwan
 interface Vlan225
  tunnel-interface
   encapsulation ipsec preference 100
   no border
   color public-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
```

A switch port feature template is created that will make the physical interface (GigabitEthernet0/1/0) on the router into a trunk port so it can carry VLAN225, and potentially other VLANs if required.



Device Type IR1821,IR1831,IR1833,IR1835

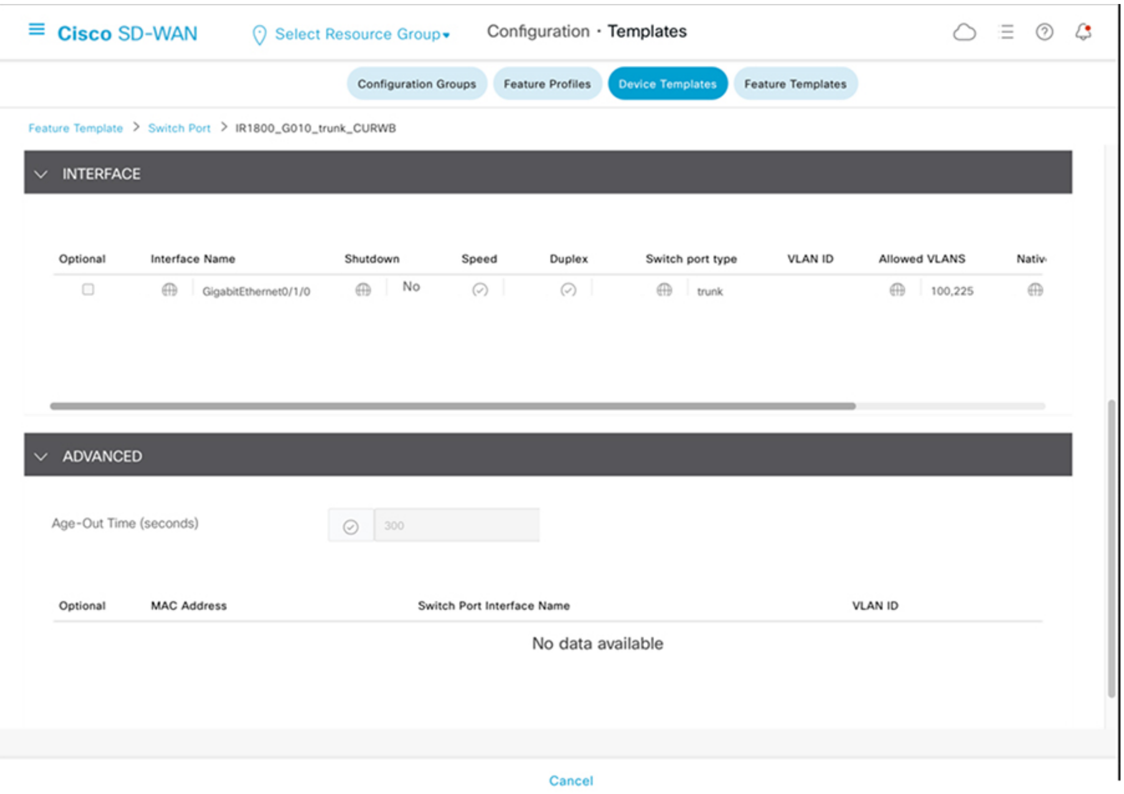
Template Name* IR1800_G010_trunk_CURWB

Description* IR1800_G010_trunk_CURWB

Slot 0

Sub-Slot 1

Module 4 Port



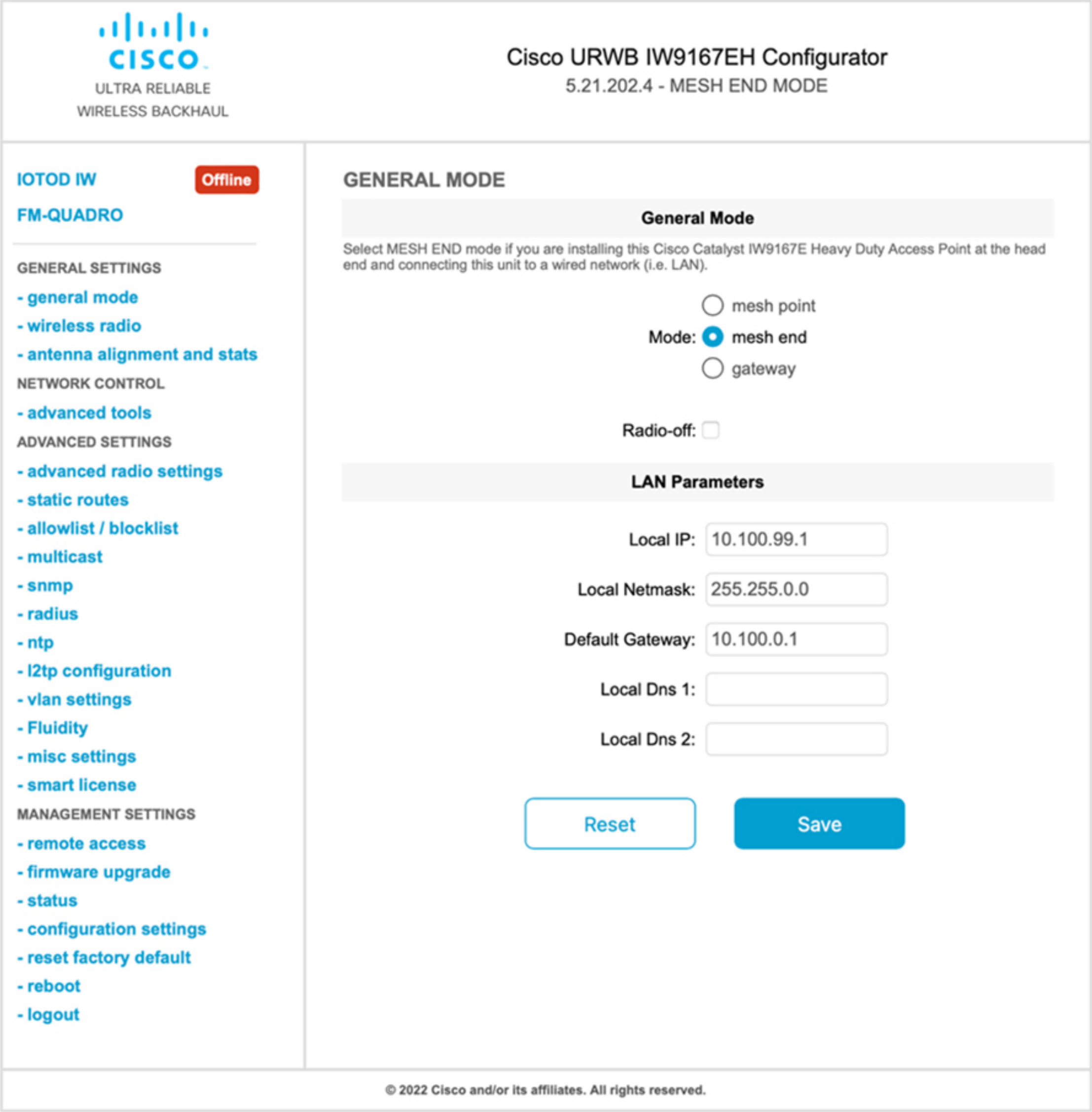
Optional	Interface Name	Shutdown	Speed	Duplex	Switch port type	VLAN ID	Allowed VLANS	Nativ
□	GigabitEthernet0/1/0	No			trunk		100,225	

Age-Out Time (seconds) 300

Optional	MAC Address	Switch Port Interface Name	VLAN ID

No data available

The screenshots that follow show the configuration for the two IW9167 radios – one connected to the IR1835 switchport, and the other at a fixed location connected to the upstream network. One radio is configured as mesh end, and the other as mesh point. A passphrase is configured to authenticate communication between radios, and VLAN trunking is also configured. Additional CURWB configuration details are beyond the scope of this documentation.



Cisco URWB IW9167EH Configurator

5.21.202.4 - MESH END MODE

GENERAL MODE

General Mode

Select MESH END mode if you are installing this Cisco Catalyst IW9167E Heavy Duty Access Point at the head end and connecting this unit to a wired network (i.e. LAN).

Mode: ○ mesh point ● mesh end ○ gateway

Radio-off: □

LAN Parameters

Local IP: 10.100.99.1

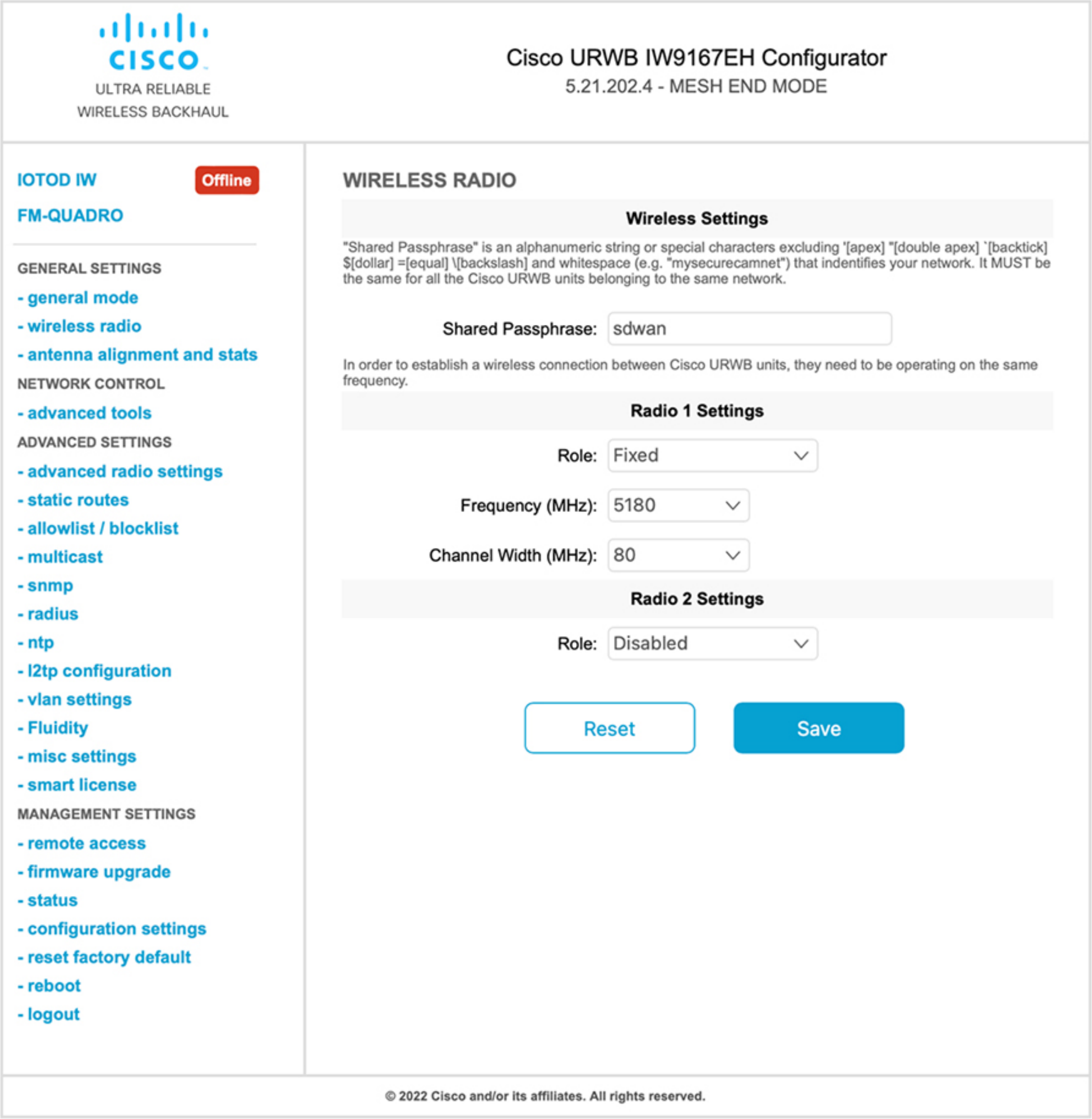
Local Netmask: 255.255.0.0

Default Gateway: 10.100.0.1

Local Dns 1:

Local Dns 2:

© 2022 Cisco and/or its affiliates. All rights reserved.



Cisco URWB IW9167EH Configurator

5.21.202.4 - MESH END MODE

WIRELESS RADIO

Wireless Settings

"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase: sdwan

In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.

Radio 1 Settings

Role: Fixed

Frequency (MHz): 5180

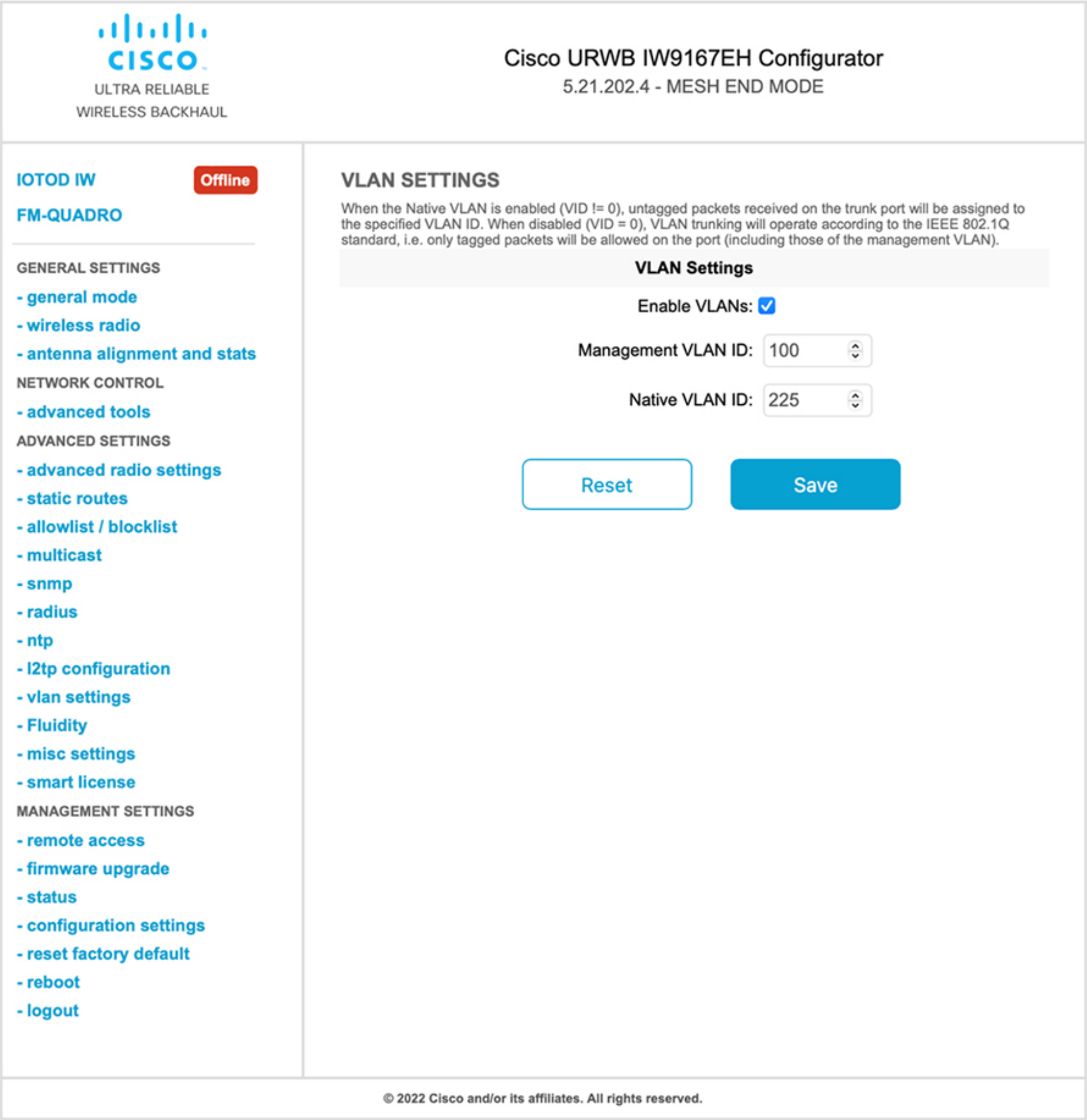
Channel Width (MHz): 80

Radio 2 Settings

Role: Disabled

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 24:



Cisco URWB IW9167EH Configurator

5.21.202.4 - MESH END MODE

VLAN SETTINGS

When the Native VLAN is enabled (VID != 0), untagged packets received on the trunk port will be assigned to the specified VLAN ID. When disabled (VID = 0), VLAN trunking will operate according to the IEEE 802.1Q standard, i.e. only tagged packets will be allowed on the port (including those of the management VLAN).

VLAN Settings

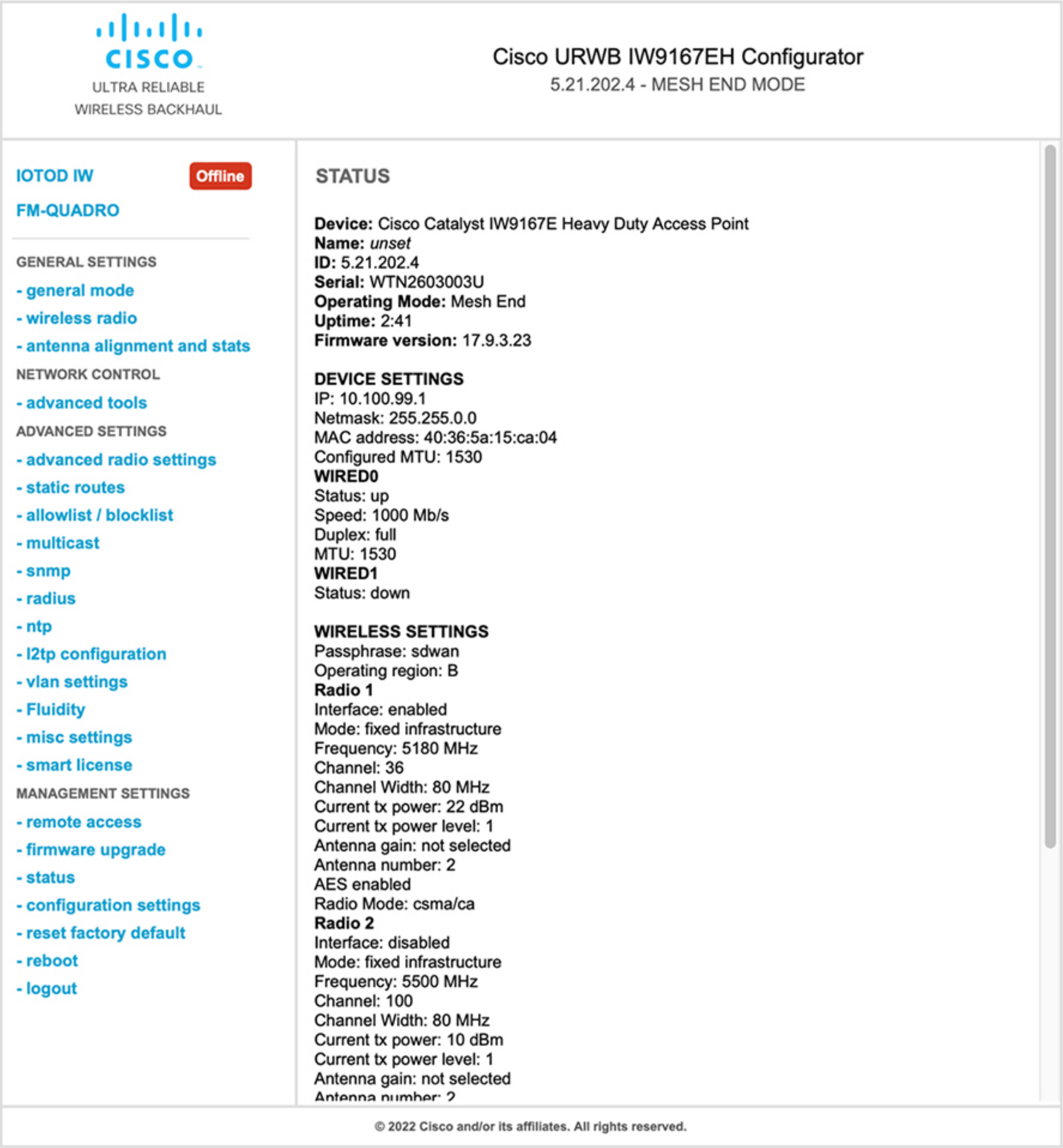
Enable VLANs: ☑

Management VLAN ID: 100

Native VLAN ID: 225

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 25:



Cisco URWB IW9167EH Configurator

5.21.202.4 - MESH END MODE

STATUS

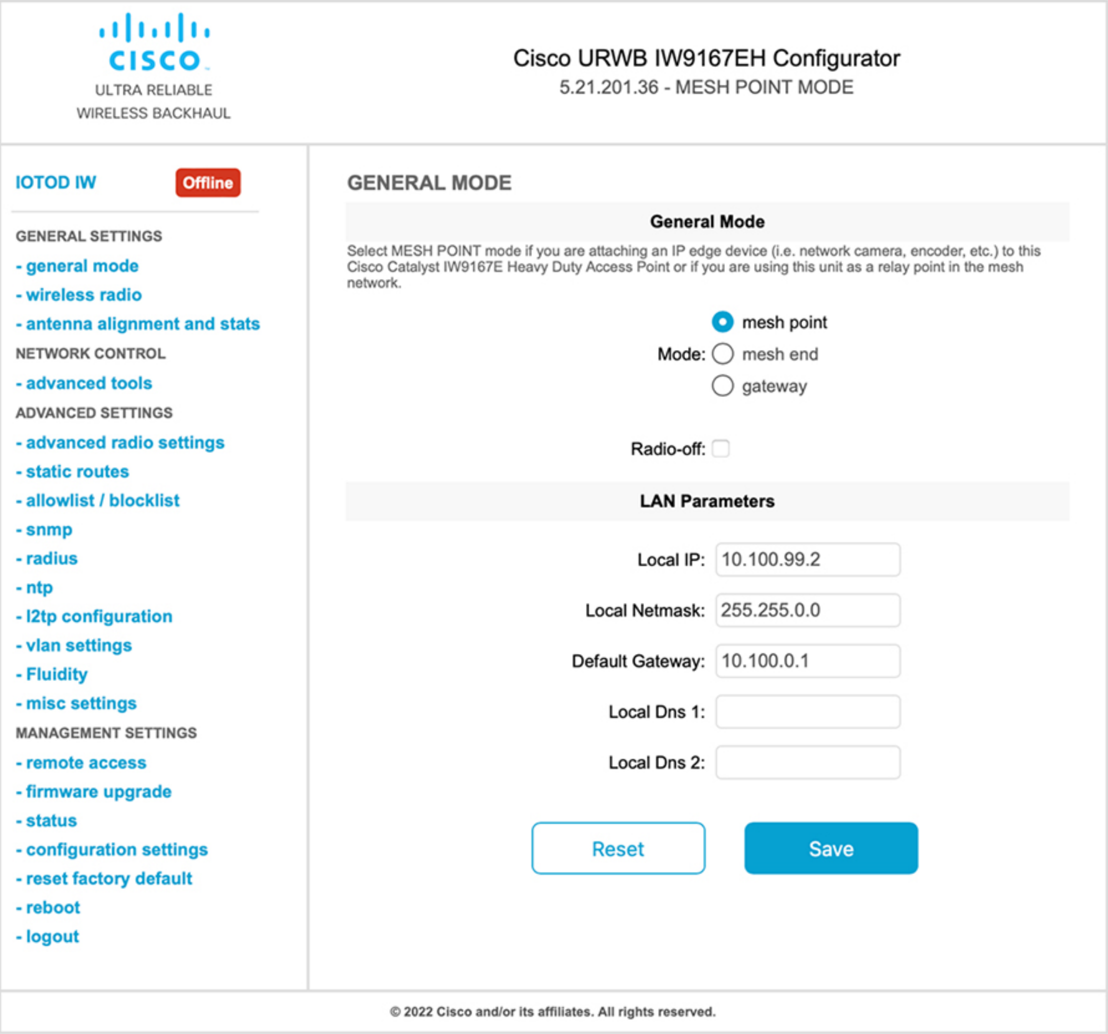
Device: Cisco Catalyst IW9167E Heavy Duty Access Point
Name: *unset*
ID: 5.21.202.4
Serial: WTN2603003U
Operating Mode: Mesh End
Uptime: 2:41
Firmware version: 17.9.3.23

DEVICE SETTINGS
IP: 10.100.99.1
Netmask: 255.255.0.0
MAC address: 40:36:5a:15:ca:04
Configured MTU: 1530
WIRED0
Status: up
Speed: 1000 Mb/s
Duplex: full
MTU: 1530
WIRED1
Status: down

WIRELESS SETTINGS
Passphrase: sdwan
Operating region: B
Radio 1
Interface: enabled
Mode: fixed infrastructure
Frequency: 5180 MHz
Channel: 36
Channel Width: 80 MHz
Current tx power: 22 dBm
Current tx power level: 1
Antenna gain: not selected
Antenna number: 2
AES enabled
Radio Mode: csma/ca
Radio 2
Interface: disabled
Mode: fixed infrastructure
Frequency: 5500 MHz
Channel: 100
Channel Width: 80 MHz
Current tx power: 10 dBm
Current tx power level: 1
Antenna gain: not selected
Antenna number: 2

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 26:



Cisco URWB IW9167EH Configurator

5.21.201.36 - MESH POINT MODE

GENERAL MODE

General Mode

Select MESH POINT mode if you are attaching an IP edge device (i.e. network camera, encoder, etc.) to this Cisco Catalyst IW9167E Heavy Duty Access Point or if you are using this unit as a relay point in the mesh network.

Mode: ● mesh point ○ mesh end ○ gateway

Radio-off: □

LAN Parameters

Local IP: 10.100.99.2

Local Netmask: 255.255.0.0

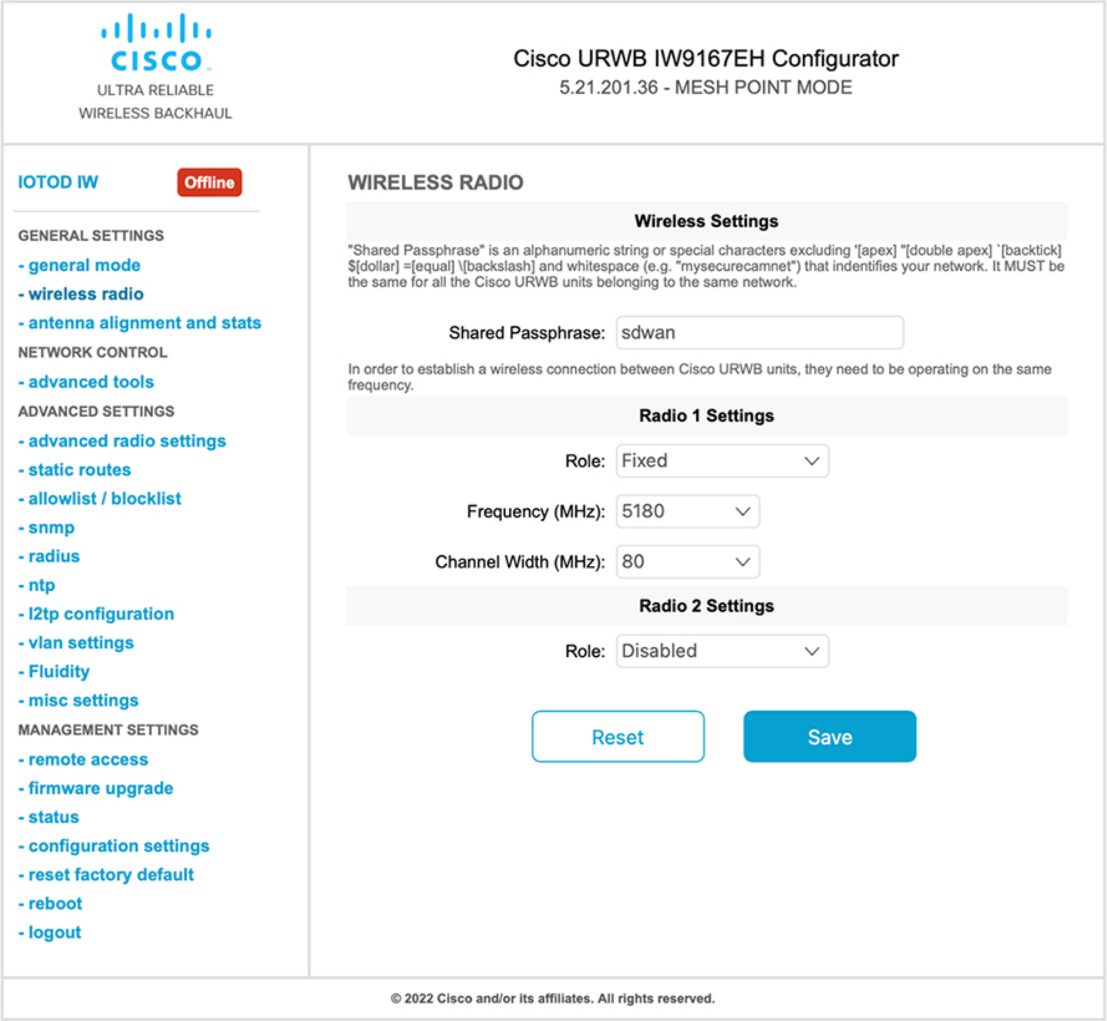
Default Gateway: 10.100.0.1

Local Dns 1:

Local Dns 2:

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 27:



Cisco URWB IW9167EH Configurator

5.21.201.36 - MESH POINT MODE

WIRELESS RADIO

Wireless Settings

"Shared Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $[dollar] =[equal] \[backslash] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Shared Passphrase: sdwan

In order to establish a wireless connection between Cisco URWB units, they need to be operating on the same frequency.

Radio 1 Settings

Role: Fixed

Frequency (MHz): 5180

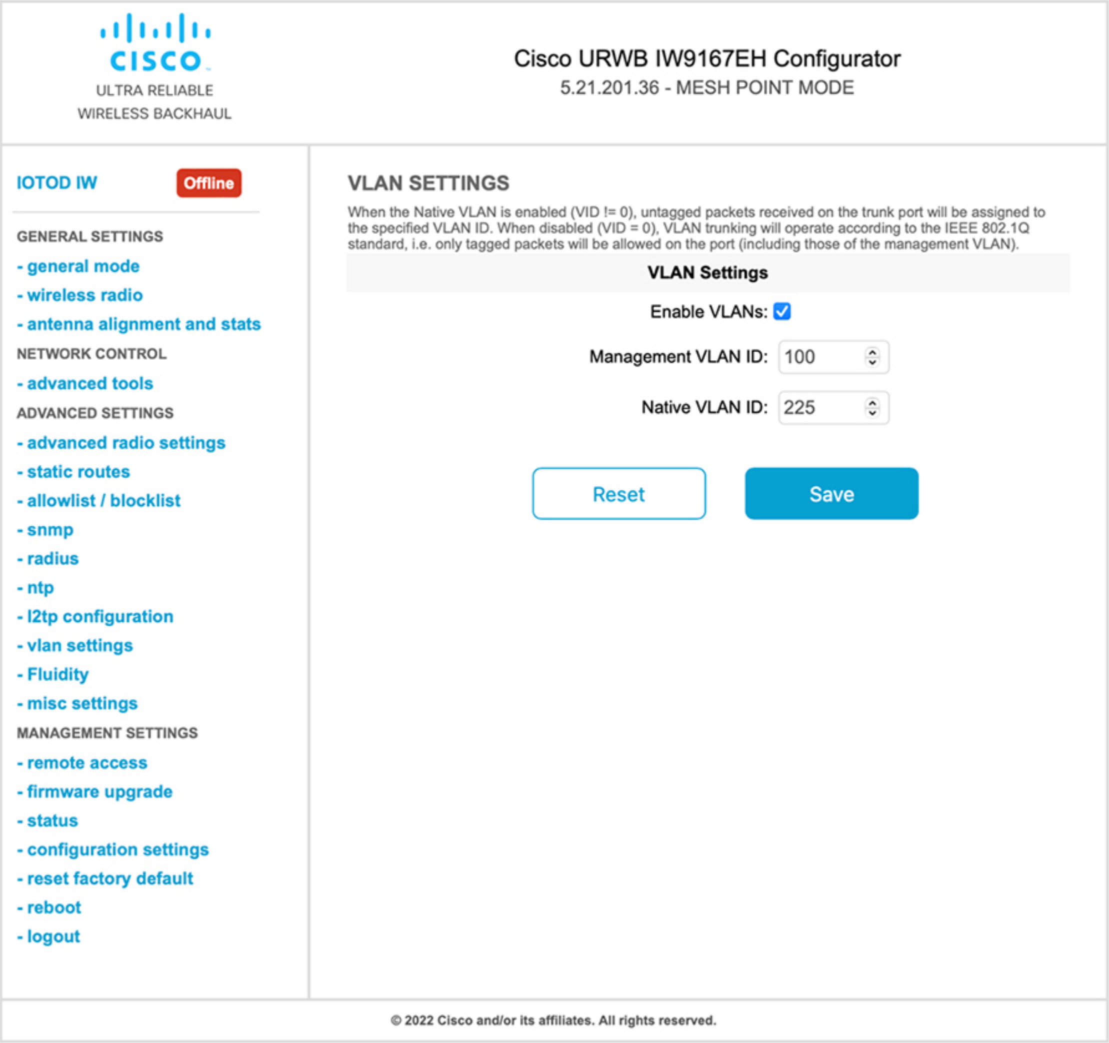
Channel Width (MHz): 80

Radio 2 Settings

Role: Disabled

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 28:



ULTRA RELIABLE
WIRELESS BACKHAUL

Cisco URWB IW9167EH Configurator
5.21.201.36 - MESH POINT MODE

VLAN SETTINGS

When the Native VLAN is enabled (VID != 0), untagged packets received on the trunk port will be assigned to the specified VLAN ID. When disabled (VID = 0), VLAN trunking will operate according to the IEEE 802.1Q standard, i.e. only tagged packets will be allowed on the port (including those of the management VLAN).

VLAN Settings

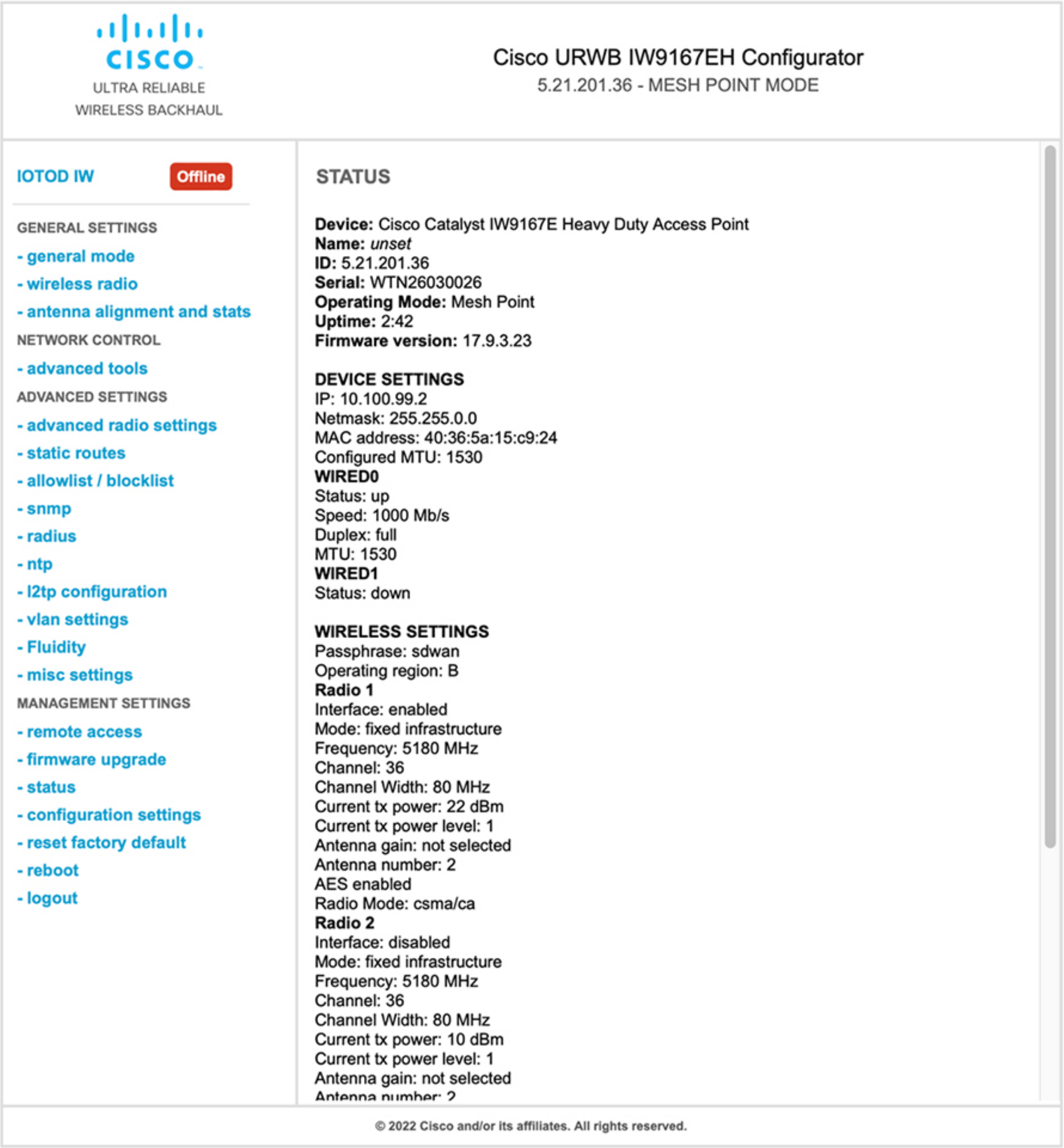
Enable VLANs: ☑

Management VLAN ID: 100

Native VLAN ID: 225

© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 29:



Cisco URWB IW9167EH Configurator
5.21.201.36 - MESH POINT MODE

STATUS

Device: Cisco Catalyst IW9167E Heavy Duty Access Point
Name: *unset*
ID: 5.21.201.36
Serial: WTN26030026
Operating Mode: Mesh Point
Uptime: 2:42
Firmware version: 17.9.3.23

DEVICE SETTINGS
IP: 10.100.99.2
Netmask: 255.255.0.0
MAC address: 40:36:5a:15:c9:24
Configured MTU: 1530
WIRED0
Status: up
Speed: 1000 Mb/s
Duplex: full
MTU: 1530
WIRED1
Status: down

WIRELESS SETTINGS
Passphrase: sdwan
Operating region: B
Radio 1
Interface: enabled
Mode: fixed infrastructure
Frequency: 5180 MHz
Channel: 36
Channel Width: 80 MHz
Current tx power: 22 dBm
Current tx power level: 1
Antenna gain: not selected
Antenna number: 2
AES enabled
Radio Mode: csma/ca
Radio 2
Interface: disabled
Mode: fixed infrastructure
Frequency: 5180 MHz
Channel: 36
Channel Width: 80 MHz
Current tx power: 10 dBm
Current tx power level: 1
Antenna gain: not selected
Antenna number: 2

Ignition Sense

Create a CLI Add-on template with the following configuration, and then add the feature template to the device template for the IR1800. This configuration will cause the IR1800 to monitor the voltage on the power input. When the detected voltage drops below 11.81V for 20 seconds, as would be the case if the vehicle is turned off and power is coming from the battery instead of the alternator, a 900-second timer is started after which the router will shut down. When the vehicle is started again, and input voltage exceeds 11.81V for 1 second, the router will boot up again.

```
!

ignition enable
ignition sense

ignition sense-voltage threshold 11 810

ignition off-timer 900

ignition battery-type 12v

!
```

Ignition Power Management

Create a CLI Add-on template with the following configuration, and then add the feature template to the device template for the IR1835. This configuration will cause the IR1835 to monitor the digital input connected to the vehicle ignition wire. When the ignition input is off a 900-second timer is started after which the router will shut down. When the vehicle is started again, and the ignition input is on the router, it will boot up.

```
!

ignition enable

ignition off-timer 900

ignition battery-type 12v

!
```

GPIO

Configure GPIO by creating a CLI Add-on template, adding the configuration below, and then adding the CLI Add-on template to the Device Template. In this example, an IR1101 with an IRM-1101-SPMI expansion module with Digitial IO ports is configured with pin 1 as an input that is triggered when it is closed (for example it contacts the ground on pin 5).

```
alarm contact 1 enable

alarm contact 1 description Expansion module Digital IO port 1

alarm contact 1 severity critical

alarm contact 1 trigger closed
```

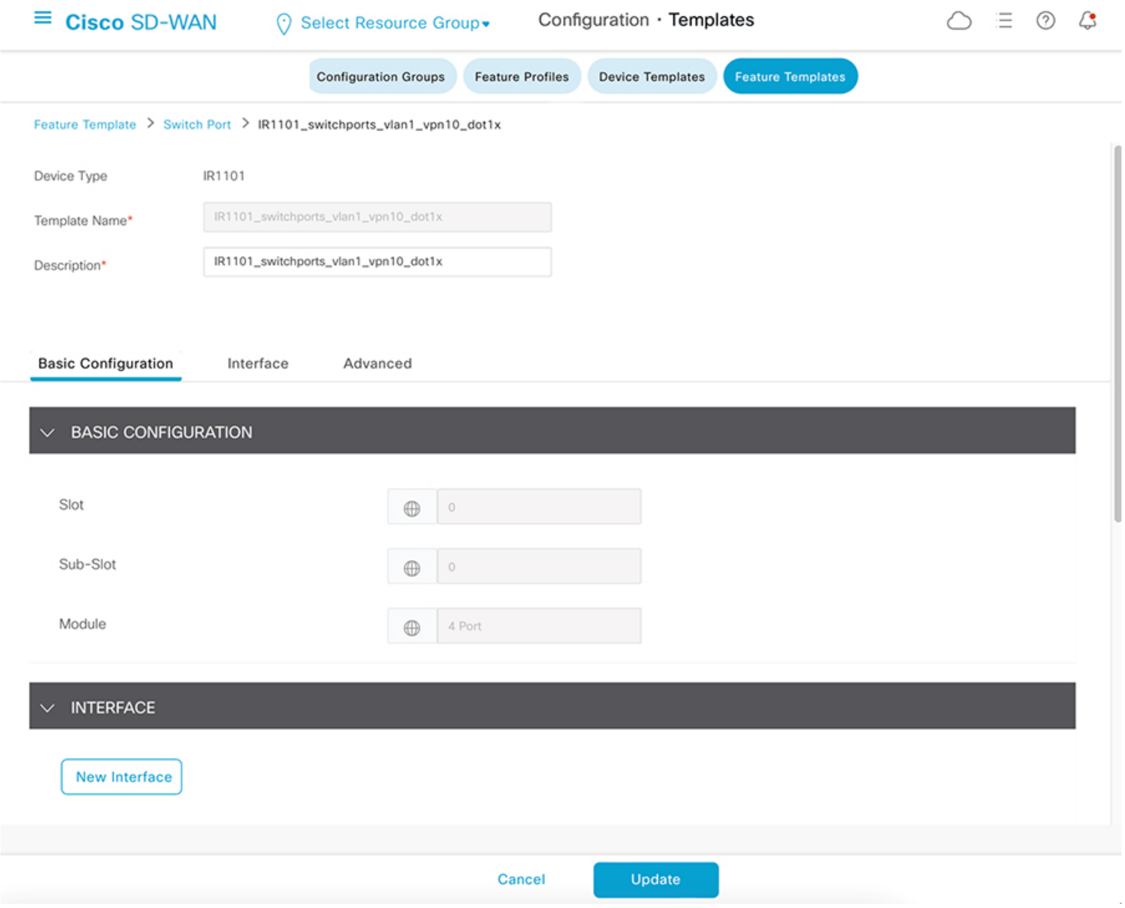
When the input on pin 1 is detected, it will trigger a SYSLOG message of severity CRITICAL.

```
Dec 12 17:51:57.729: %IOT_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External
alarm/digital IO port (Expansion module Digital IO port 1) asserted



IR1101-K9-FCW23090HYU#show alarm

Alarm contact 0:

   Not enabled.


Digital I/O 1:

   Description: Expansion module Digital IO port 1

   Status:      Asserted
   Application: Dry

   Severity:    critical

   Trigger:     Closed

   Voltage:     225mV

   Threshold:   1600mV

   Mode:        Input


IR1101-K9-FCW23090HYU#show facility-alarm status | i port 1


System Totals Critical: 4  Major: 2  Minor: 2


Source                     Time                   Severity      Description [Index]

------                     ------                 --------      -------------------



External alarm contact     Dec 12 2022 12:56:12   CRITICAL      Expansion module Digital
IO port 1 [1]
```

802.1X Authentication for LAN clients

1. Create a switchport template to enable each of the switchports on the router.

Figure 30:



Feature Template > Switch Port > IR1101_switchports_vlan1_vpn10_dot1x

Device Type IR1101

Template Name* IR1101_switchports_vlan1_vpn10_dot1x

Description* IR1101_switchports_vlan1_vpn10_dot1x

BASIC CONFIGURATION

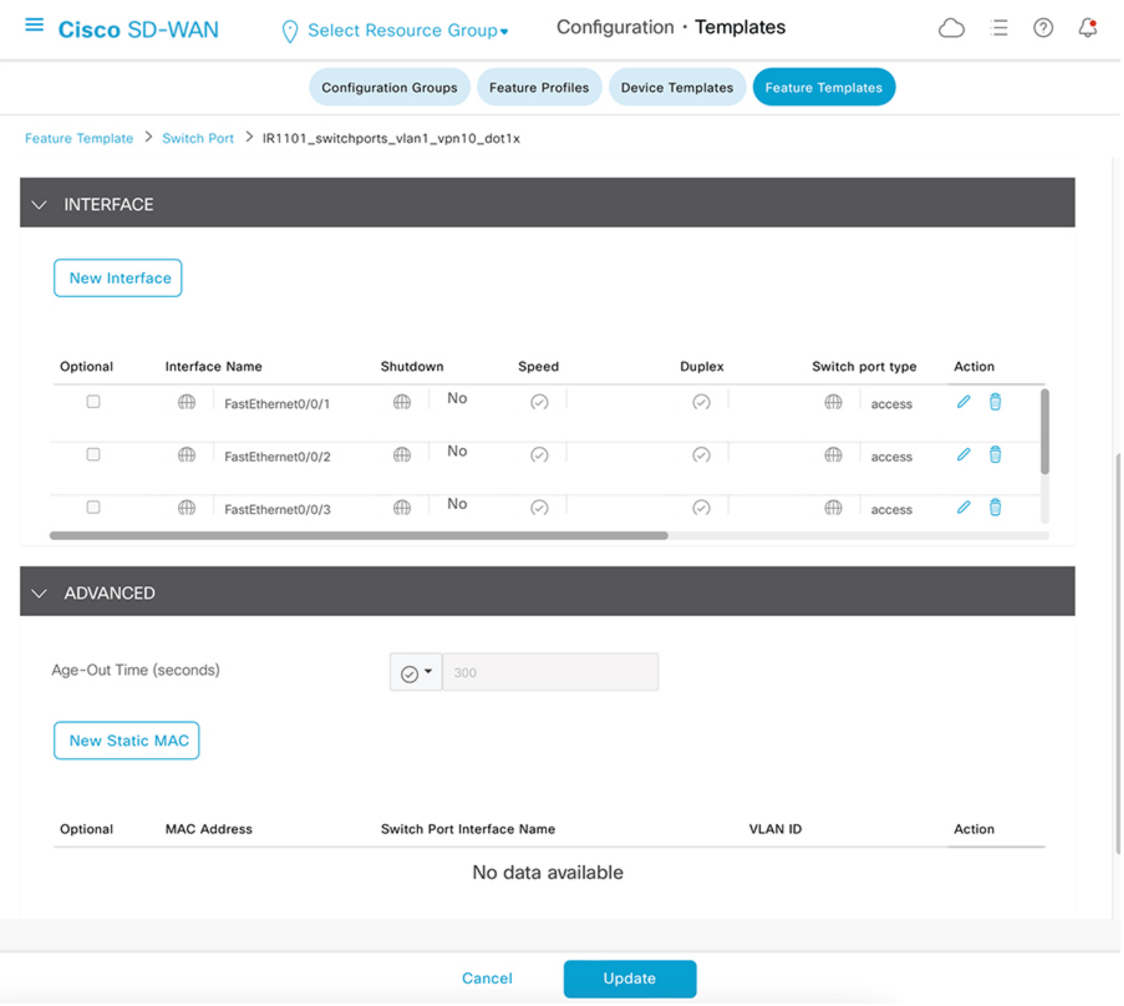
Slot 0

Sub-Slot 0

Module 4 Port

INTERFACE

Figure 31:



Feature Template > Switch Port > IR1101_switchports_vlan1_vpn10_dot1x

INTERFACE

New Interface

Optional	Interface Name	Shutdown	Speed	Duplex	Switch port type	Action
□	FastEthernet0/0/1	No	✓	✓	access	✎ 🗑
□	FastEthernet0/0/2	No	✓	✓	access	✎ 🗑
□	FastEthernet0/0/3	No	✓	✓	access	✎ 🗑

ADVANCED

Age-Out Time (seconds) ✓ ▾ 300

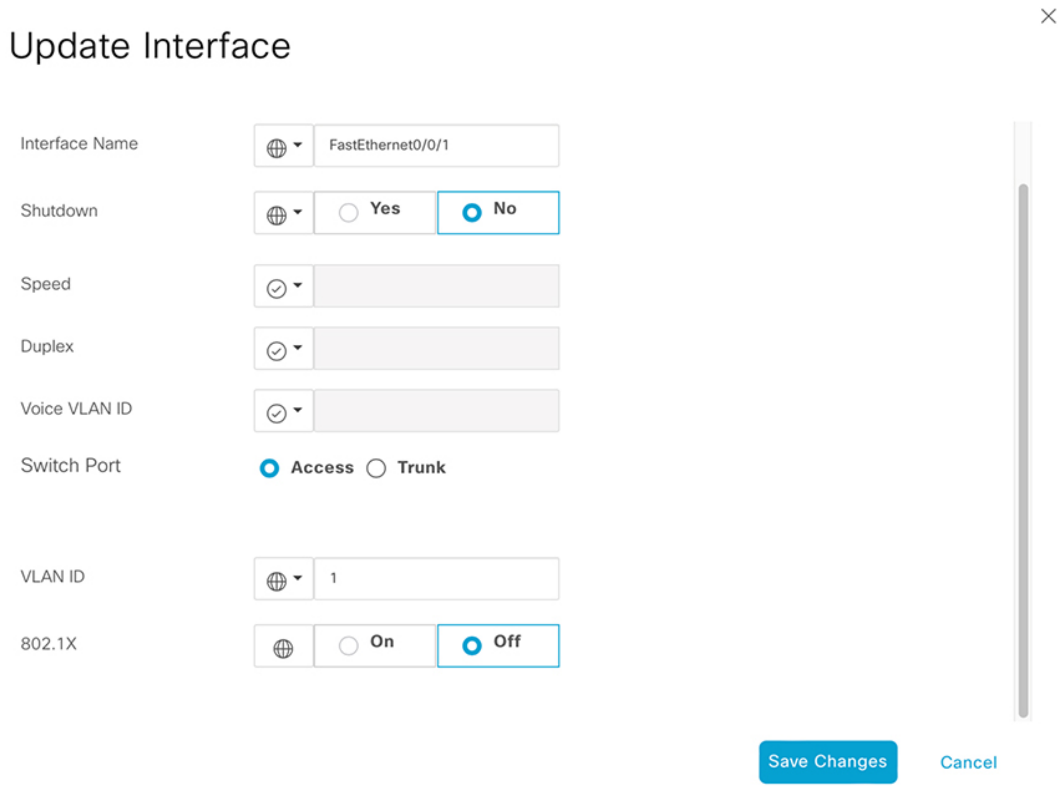
New Static MAC

Optional	MAC Address	Switch Port Interface Name	VLAN ID	Action

No data available

2. For each switchport (FastEthernet0/0/1, for example), click on the edit pencil icon button under **Action**. This will bring up a new window in which you can set the various parameters of the physical interface like the VLAN, speed, duplex, etc. Set 802.1X to **On**.

Figure 32:



Update Interface

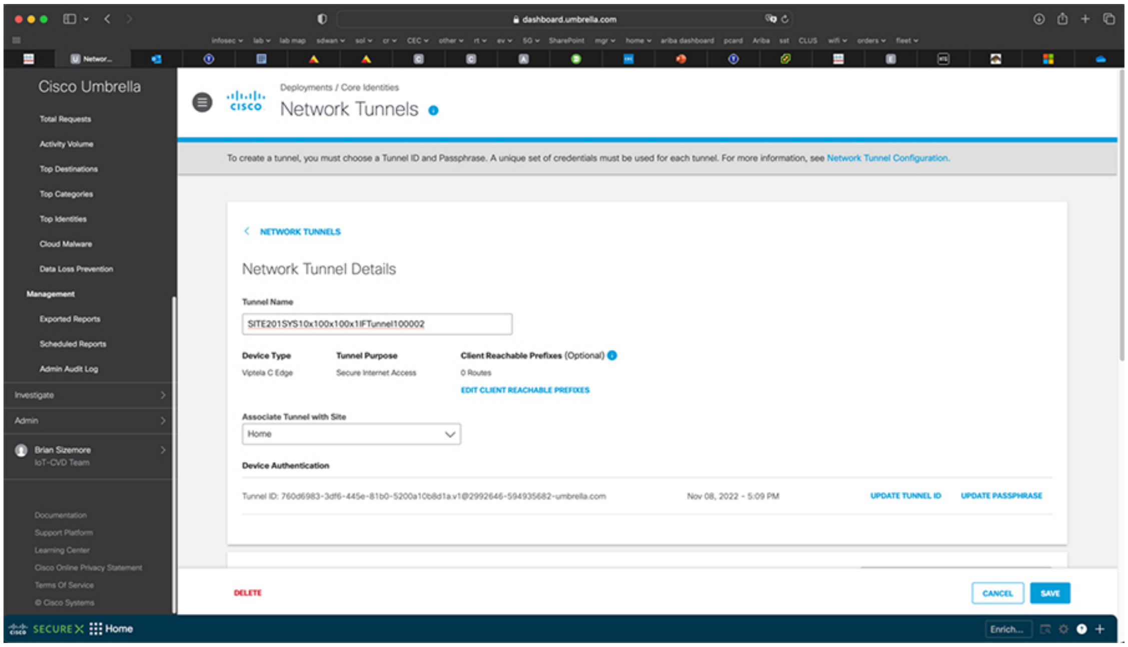
Interface Name	FastEthernet0/0/1
Shutdown	○ Yes ● No
Speed	
Duplex	
Voice VLAN ID	
Switch Port	● Access ○ Trunk
VLAN ID	1
802.1X	○ On ● Off

Note: Due to a bug (CSCwd83109), some 802.1x configuration must be manually added via CLI to the Add-on template in vManage version 20.10, as shown below.

```
!

line 0/0/0

line 0/2/0

!

interface FastEthernet0/0/3

dot1x pae authenticator

authentication port-control auto

!

interface FastEthernet0/0/4

dot1x pae authenticator

authentication port-control auto

!
```

Umbrella SIG

Figure 33:



Deployments / Core Identities

Network Tunnels

To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more information, see Network Tunnel Configuration.

< NETWORK TUNNELS

Network Tunnel Details

Tunnel Name

SITE201SYS10x100x100x1IFTunnel100002

Device Type	Tunnel Purpose	Client Reachable Prefixes (Optional)
Viptela C Edge	Secure Internet Access	0 Routes
		EDIT CLIENT REACHABLE PREFIXES

Associate Tunnel with Site

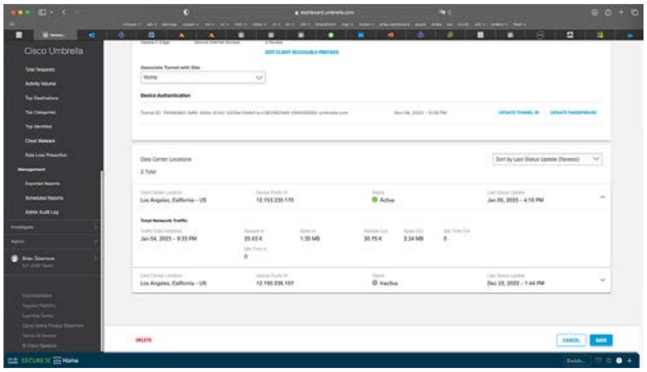
Home

Device Authentication

Tunnel ID: 760d6983-3df6-445e-81b0-5200a10b8d1a.v1@2992646-594935682-umbrella.com Nov 08, 2022 - 5:09 PM UPDATE TUNNEL ID UPDATE PASSPHRASE

DELETE CANCEL SAVE

Figure 34:



EDIT CLIENT REACHABLE PREFIXES

Associate Tunnel with Site

Home

Device Authentication

UPDATE TUNNEL ID UPDATE PASSPHRASE

Data Center Locations

2 Total

Sort by Last Status Update (Newest)

Los Angeles, California - US 12.153.239.170 Active Jan 06, 2023 - 4:16 PM

Total Network Traffic

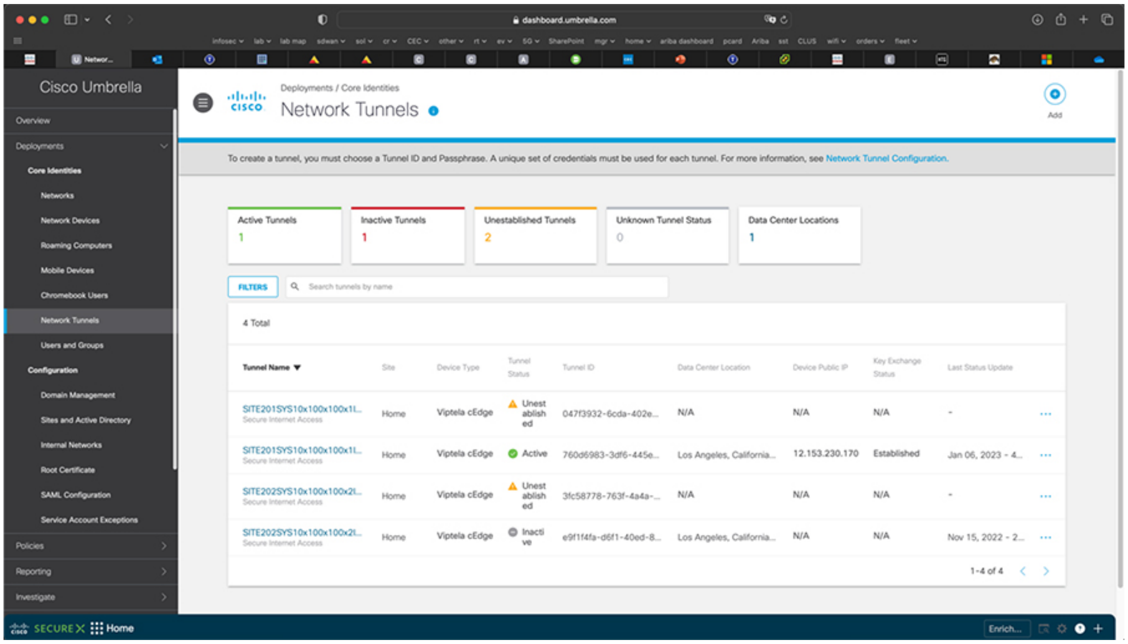
Jan 04, 2023 - 9:35 PM 25.63 K 1.35 MB 30.75 K 3.34 MB 0

0

Los Angeles, California - US 12.190.239.107 Inactive Dec 22, 2022 - 1:44 PM

DELETE CANCEL SAVE

Figure 35:



Deployments / Core Identities

Network Tunnels

To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more information, see Network Tunnel Configuration.

Active Tunnels	Inactive Tunnels	Unestablished Tunnels	Unknown Tunnel Status	Data Center Locations
1	1	2	0	1

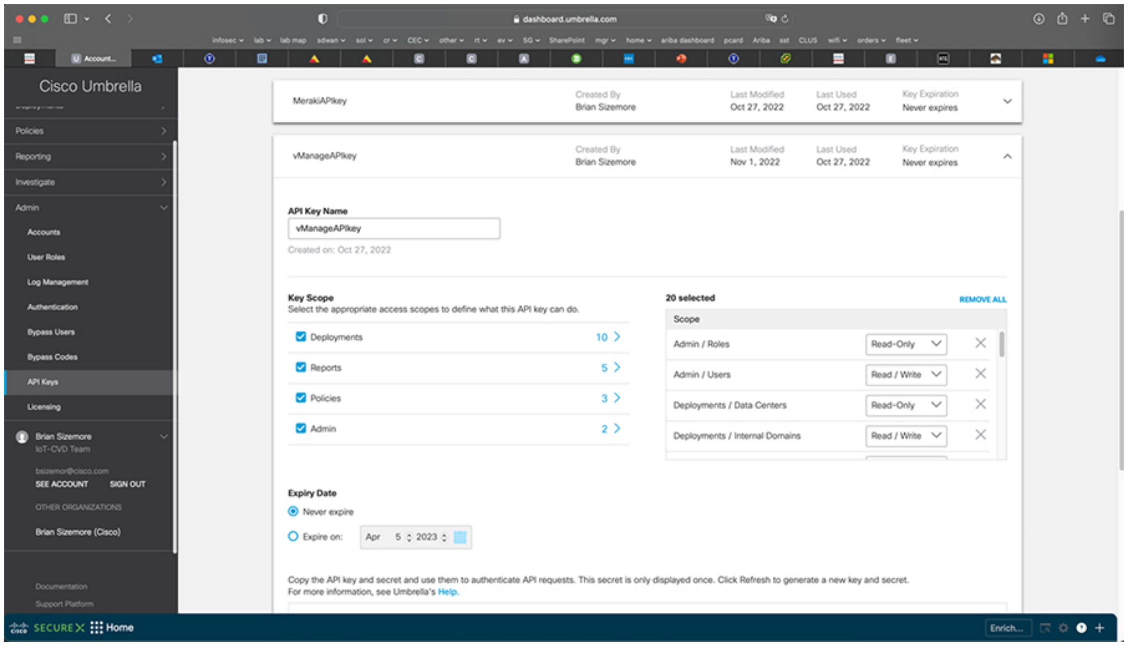
4 Total

Tunnel Name ▼	Site	Device Type	Tunnel Status	Tunnel ID	Data Center Location	Device Public IP	Key Exchange Status	Last Status Update
SITE201SYS10x100x100x1l... Secure Internet Access	Home	Viptela cEdge	Unestablished	047f3932-6cda-402e...	N/A	N/A	N/A	-
SITE201SYS10x100x100x1l... Secure Internet Access	Home	Viptela cEdge	Active	760d6983-3df6-445e...	Los Angeles, California...	12.153.230.170	Established	Jan 06, 2023 - 4...
SITE202SYS10x100x100x2l... Secure Internet Access	Home	Viptela cEdge	Unestablished	3fc58778-763f-4a4a-...	N/A	N/A	N/A	-
SITE202SYS10x100x100x2l... Secure Internet Access	Home	Viptela cEdge	Inactive	e9f1f4fa-d6f1-40ed-8...	Los Angeles, California...	N/A	N/A	Nov 15, 2022 - 2...

1-4 of 4

1. Begin by creating an **API key** in the Umbrella dashboard for vManage to use.

Figure 36:



	Created By	Last Modified	Last Used	Key Expiration
MerakiAPIkey	Brian Sizemore	Oct 27, 2022	Oct 27, 2022	Never expires
vManageAPIkey	Brian Sizemore	Nov 1, 2022	Oct 27, 2022	Never expires

API Key Name: vManageAPIkey

Created on: Oct 27, 2022

Key Scope

Select the appropriate access scopes to define what this API key can do.

- ☑ Deployments 10
- ☑ Reports 5
- ☑ Policies 3
- ☑ Admin 2

20 selected

Scope	
Admin / Roles	Read-Only
Admin / Users	Read / Write
Deployments / Data Centers	Read-Only
Deployments / Internal Domains	Read / Write

Expiry Date

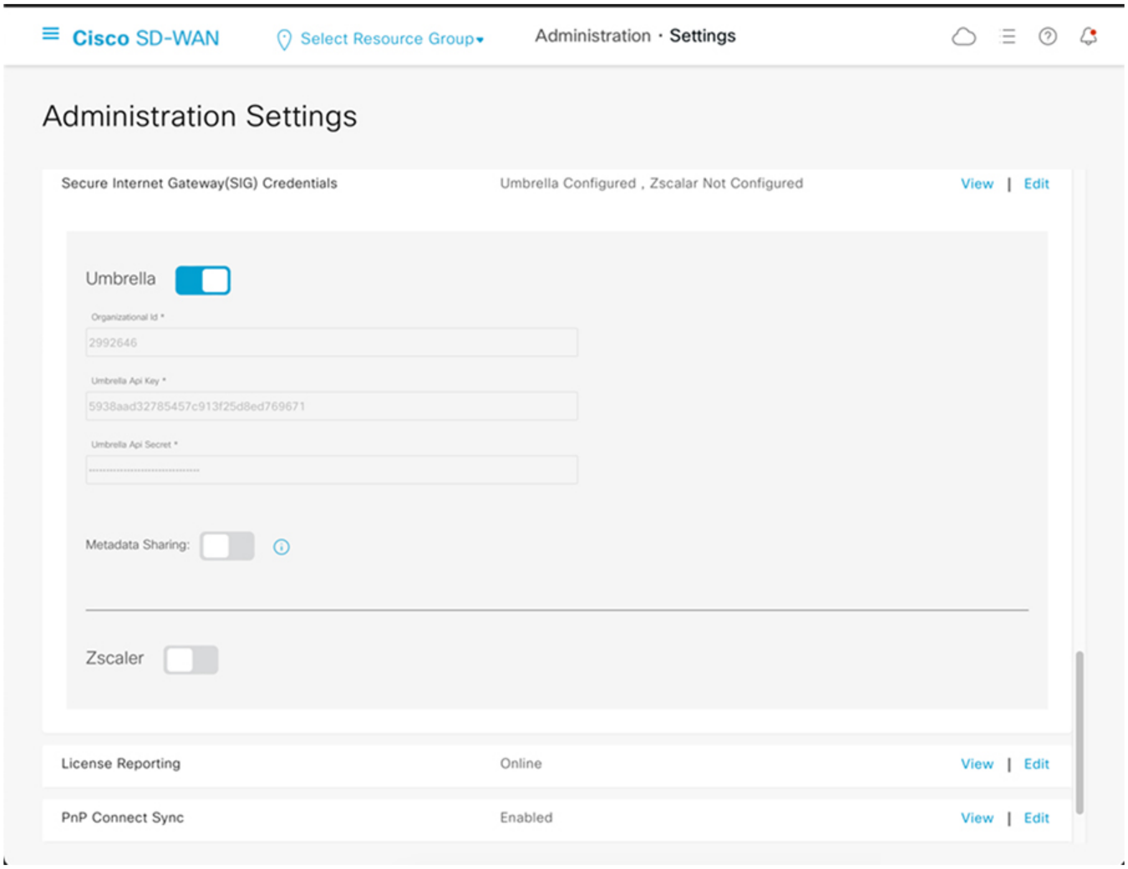
● Never expire

○ Expire on: Apr 5 2023

Copy the API key and secret and use them to authenticate API requests. This secret is only displayed once. Click Refresh to generate a new key and secret. For more information, see Umbrella's Help.

2. From vManage, add this Umbrella API key under the **Administration Settings > Secure Internet Gateway (SIG) Credentials**.

Figure 37:



Administration Settings

Secure Internet Gateway(SIG) Credentials — Umbrella Configured , Zscalar Not Configured — View | Edit

Umbrella: on

Organizational Id *
2992646

Umbrella Api Key *
5938aad32785457c913f25d8ed769671

Umbrella Api Secret *
••••••••••••••••••••••••••••••

Metadata Sharing: off

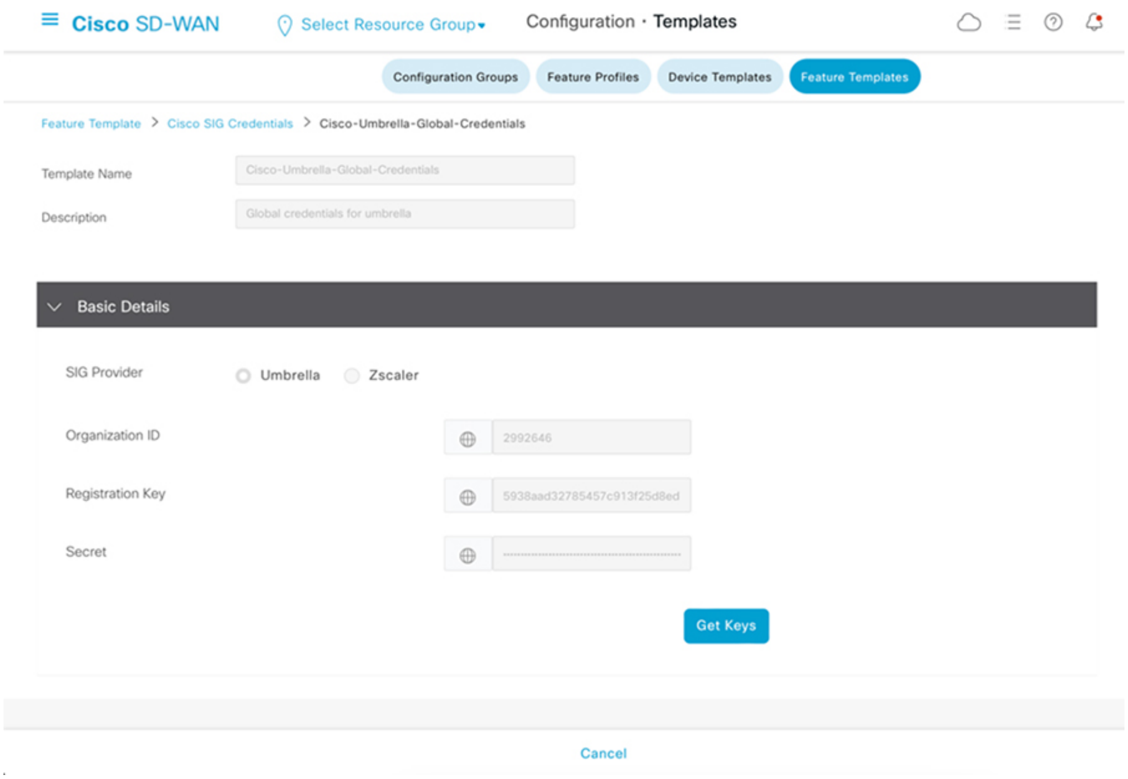
Zscaler: off

License Reporting — Online — View | Edit

PnP Connect Sync — Enabled — View | Edit

3. Create a Cisco SIG Credentials feature template, select **Umbrella** as the provider, and fill out the details from the Umbrella dashboard.

Figure 38:



Template Name: Cisco-Umbrella-Global-Credentials

Description: Global credentials for umbrella

SIG Provider: ○ Umbrella ○ Zscaler

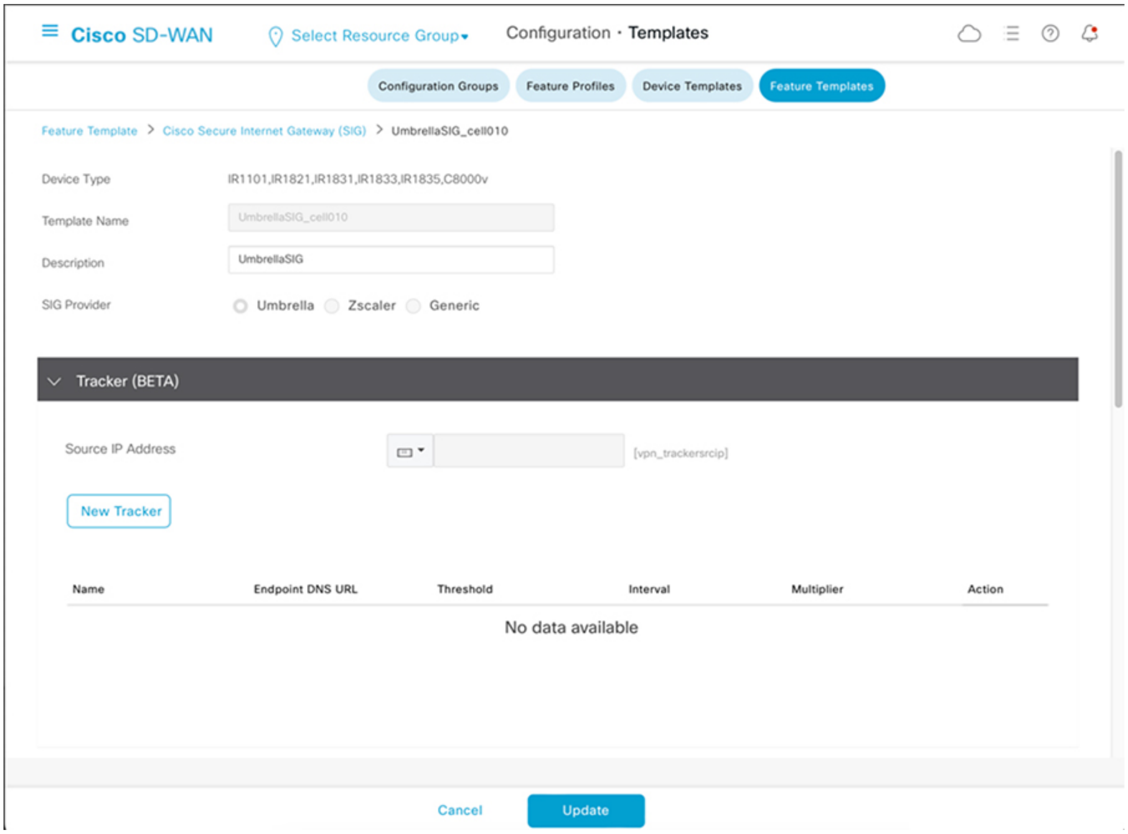
Organization ID: 2992646

Registration Key: 5938aad32785457c913f25d8ed

Secret: ··

4. Create a Cisco Secure Internet Gateway (SIG) feature template and add two IPsec tunnels (primary and backup).

Figure 39:



Device Type IR1101,IR1821,IR1831,IR1833,IR1835,C8000v

Template Name UmbrellaSIG_cell010

Description UmbrellaSIG

SIG Provider ○ Umbrella ○ Zscaler ○ Generic

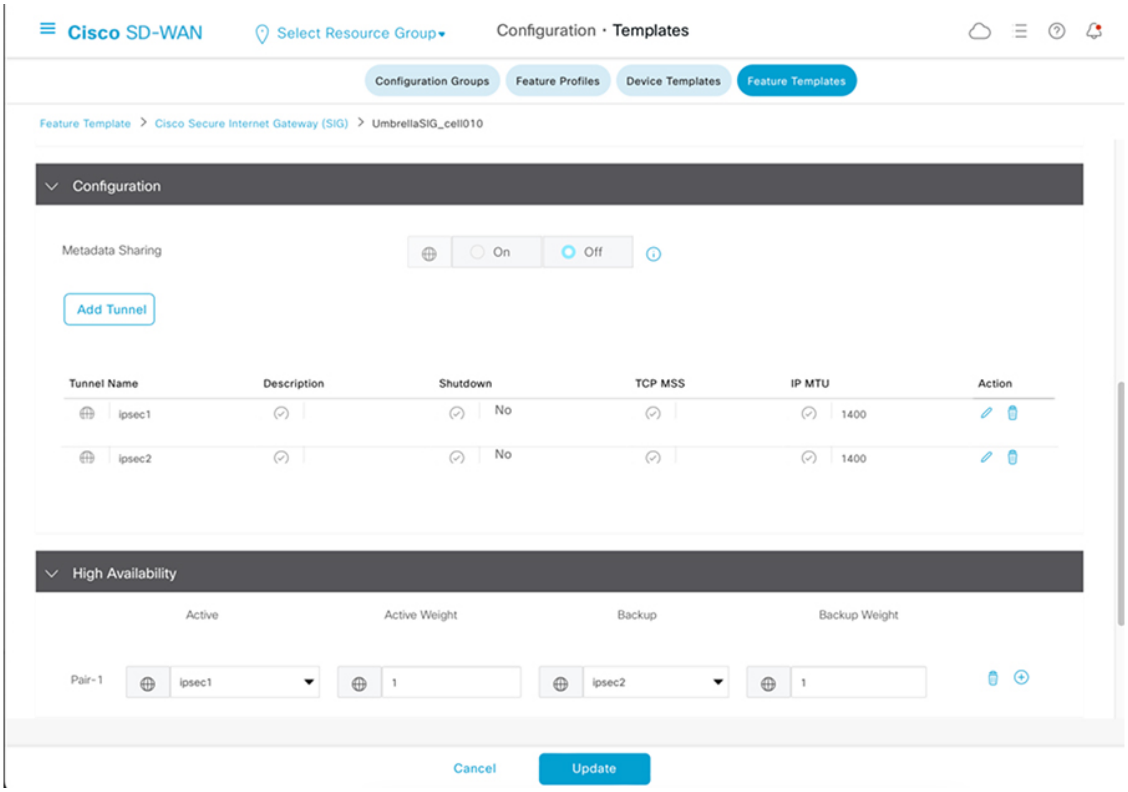
Tracker (BETA)

Source IP Address [vpn_trackersrcip]

Name	Endpoint DNS URL	Threshold	Interval	Multiplier	Action

No data available

Figure 40:



Feature Template > Cisco Secure Internet Gateway (SIG) > UmbrellaSIG_cell010

Configuration

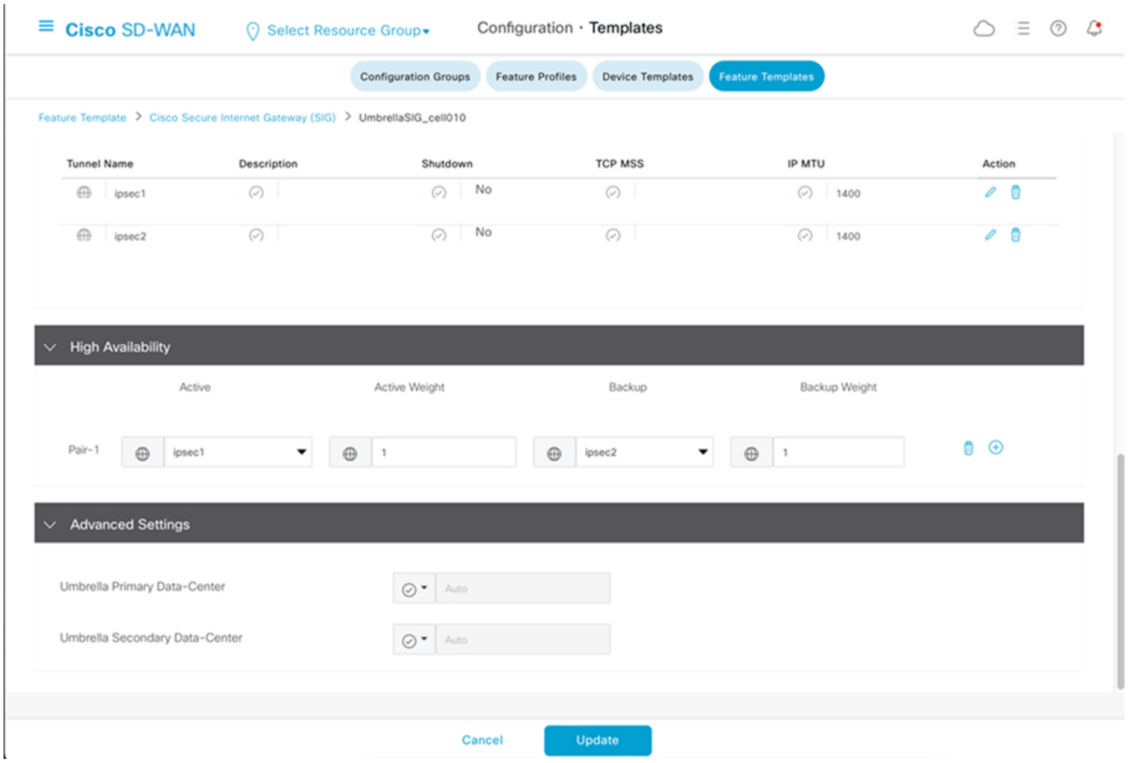
Metadata Sharing ○ On ● Off

Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		No		1400	
ipsec2		No		1400	

High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	ipsec1	1	ipsec2	1

Figure 41:



Feature Template > Cisco Secure Internet Gateway (SIG) > UmbrellaSIG_cell010

Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		No		1400	
ipsec2		No		1400	

High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	ipsec1	1	ipsec2	1

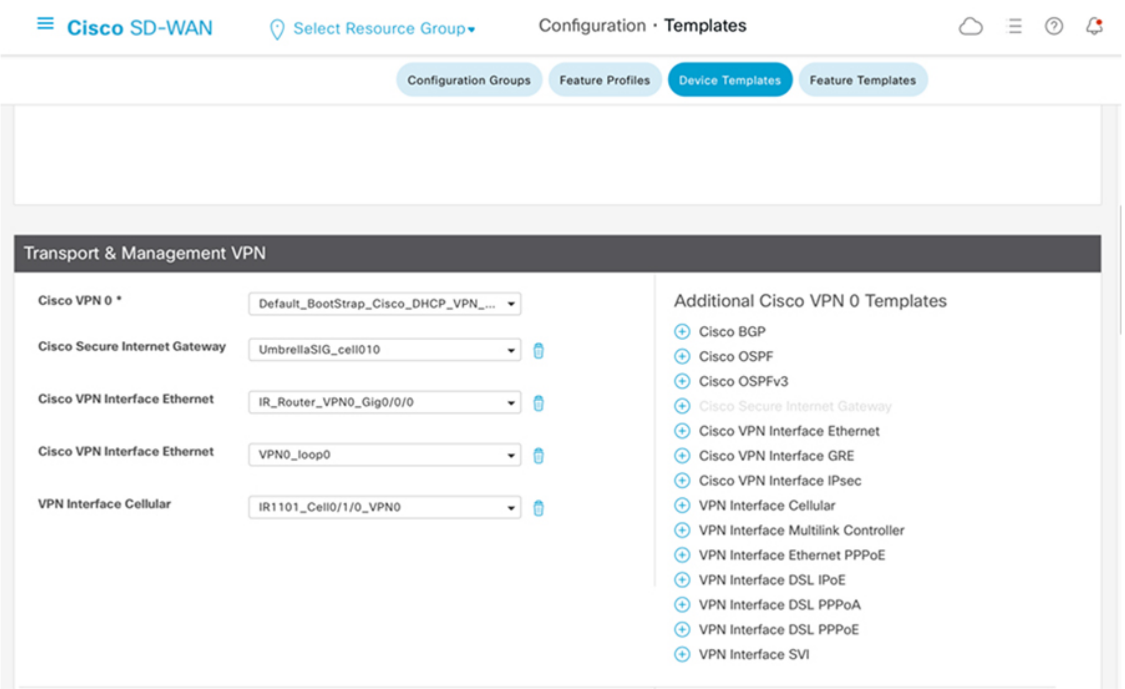
Advanced Settings

Umbrella Primary Data-Center: Auto

Umbrella Secondary Data-Center: Auto

5. In the Device Template, add the **Cisco Secure Internet Gateway template** under the **Transport & Management VPN** section.

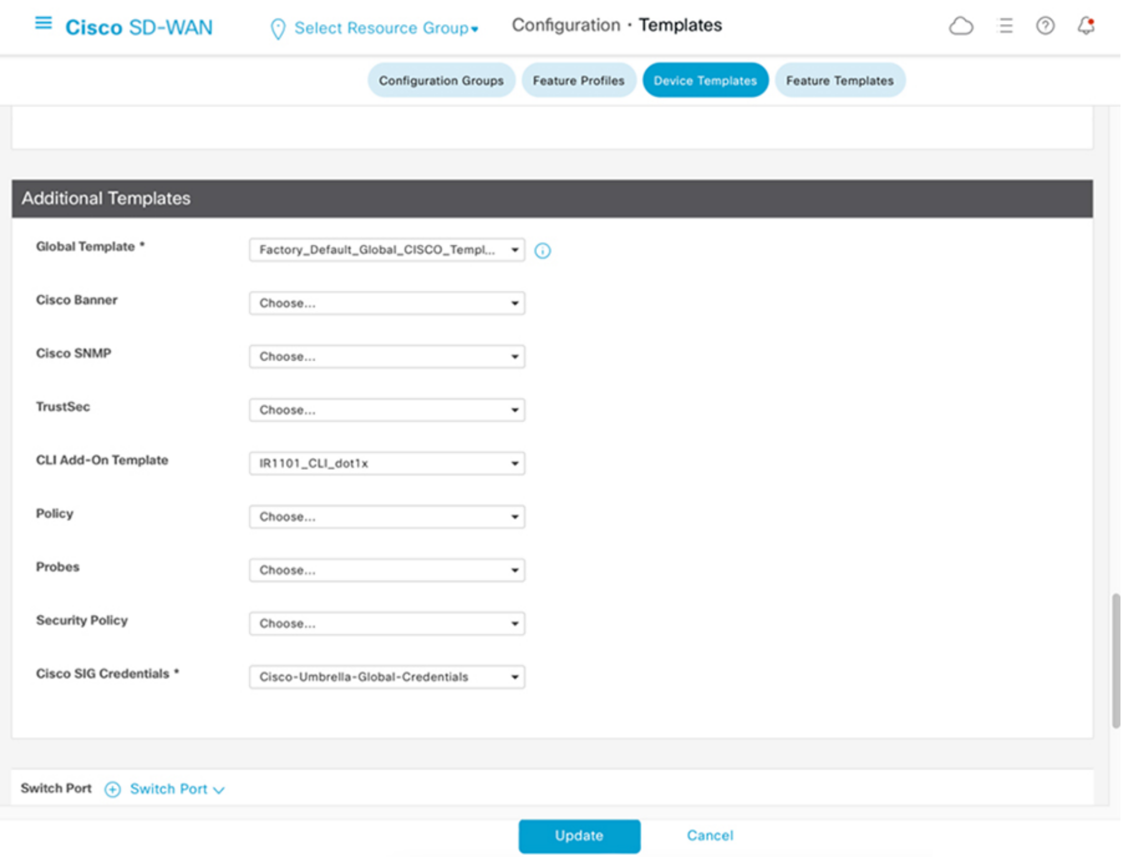
Figure 42:



Cisco VPN 0 *	Default_BootStrap_Cisco_DHCP_VPN_...
Cisco Secure Internet Gateway	UmbrellaSIG_cell010
Cisco VPN Interface Ethernet	IR_Router_VPN0_Gig0/0/0
Cisco VPN Interface Ethernet	VPN0_loop0
VPN Interface Cellular	IR1101_Cell0/1/0_VPN0

6. Also in the Device Template, add the **Cisco SIG Credentials template** under **Additional Templates**.

Figure 43:



Global Template * : Factory_Default_Global_CISCO_Templ...

Cisco Banner : Choose...

Cisco SNMP : Choose...

TrustSec : Choose...

CLI Add-On Template : IR1101_CLI_dot1x

Policy : Choose...

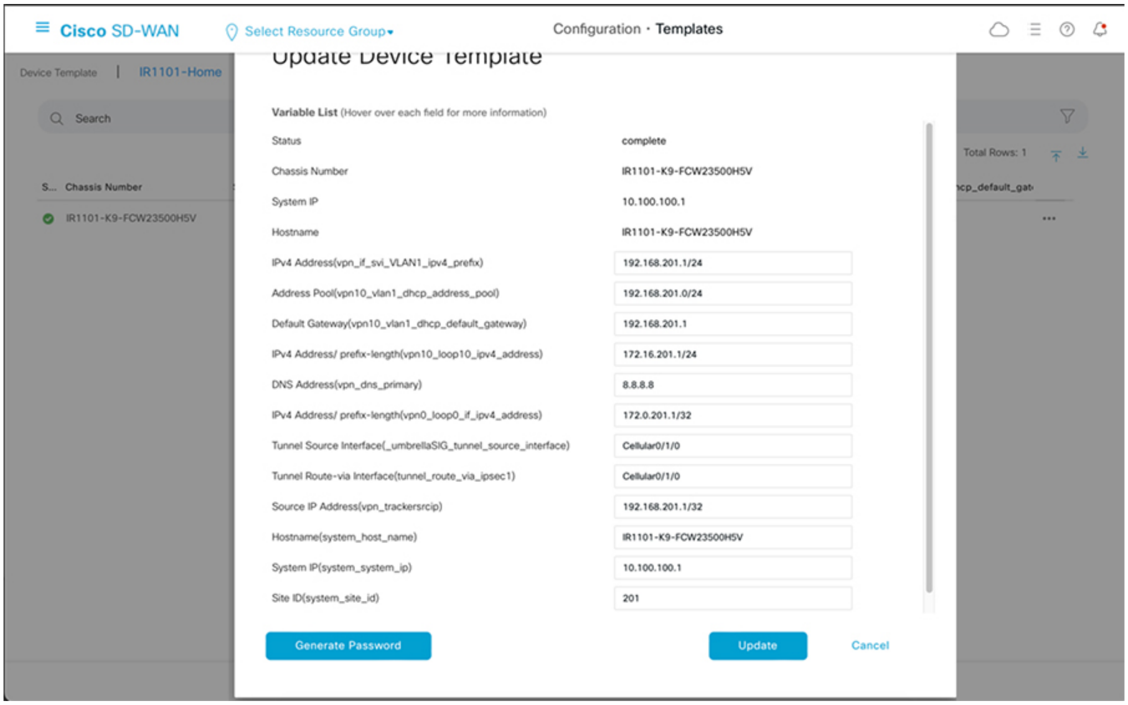
Probes : Choose...

Security Policy : Choose...

Cisco SIG Credentials * : Cisco-Umbrella-Global-Credentials

Note that in version 20.10, you cannot select a cellular interface as the source for the tunnel. Instead, you can use a variable for this value, and fill in the interface name (like “Cellular0/1/0”) for each router.

Figure 44:



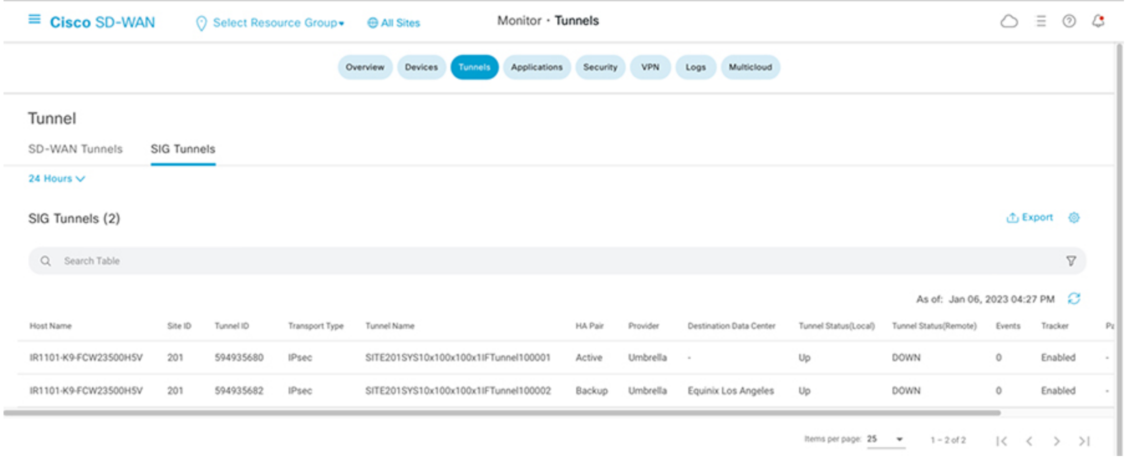
Update Device Template

Variable List (Hover over each field for more information)

Status	complete
Chassis Number	IR1101-K9-FCW23500H5V
System IP	10.100.100.1
Hostname	IR1101-K9-FCW23500H5V
IPv4 Address(vpn_if_svi_VLAN1_ipv4_prefix)	192.168.201.1/24
Address Pool(vpn10_vlan1_dhcp_address_pool)	192.168.201.0/24
Default Gateway(vpn10_vlan1_dhcp_default_gateway)	192.168.201.1
IPv4 Address/ prefix-length(vpn10_loop10_ipv4_address)	172.16.201.1/24
DNS Address(vpn_dns_primary)	8.8.8.8
IPv4 Address/ prefix-length(vpn0_loop0_if_ipv4_address)	172.0.201.1/32
Tunnel Source Interface(_umbrellaSIG_tunnel_source_interface)	Cellular0/1/0
Tunnel Route-via Interface(tunnel_route_via_ipsec1)	Cellular0/1/0
Source IP Address(vpn_trackersrcip)	192.168.201.1/32
Hostname(system_host_name)	IR1101-K9-FCW23500H5V
System IP(system_system_ip)	10.100.100.1
Site ID(system_site_id)	201

7. Verify that the tunnels come up from the **Monitor** > **Tunnels** page.

Figure 45:



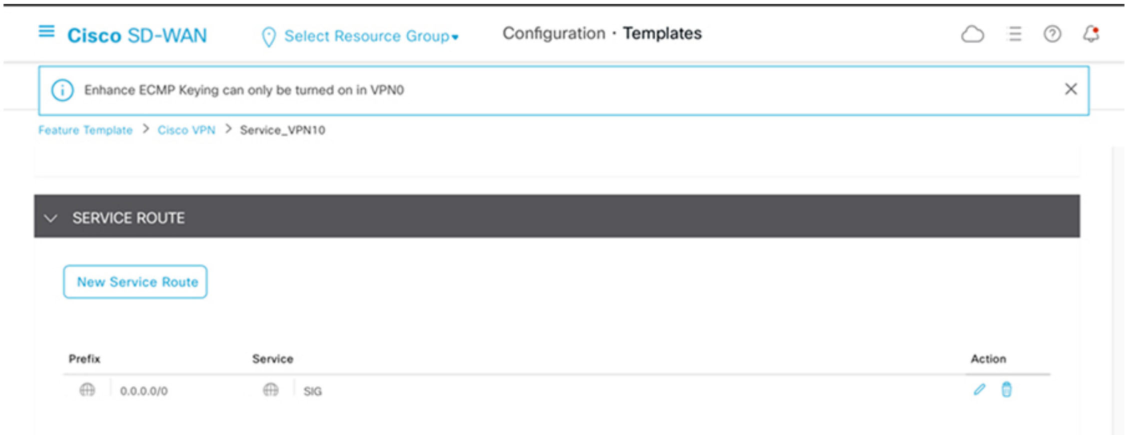
SIG Tunnels (2)

As of: Jan 06, 2023 04:27 PM

Host Name	Site ID	Tunnel ID	Transport Type	Tunnel Name	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)	Events	Tracker	Pa
IR1101-K9-FCW23500H5V	201	594935680	IPsec	SITE201SYS10x100x100x1IFTunnel100001	Active	Umbrella	-	Up	DOWN	0	Enabled	-
IR1101-K9-FCW23500H5V	201	594935682	IPsec	SITE201SYS10x100x100x1IFTunnel100002	Backup	Umbrella	Equinix Los Angeles	Up	DOWN	0	Enabled	-

8. You can also add a default **Service Route for SIG** to send data to **Umbrella** for processing.

Figure 46:


Cisco SD-WAN
Select Resource Group
Configuration · Templates
Feature Template > Cisco VPN > Service_VPN10
SERVICE ROUTE
New Service Route

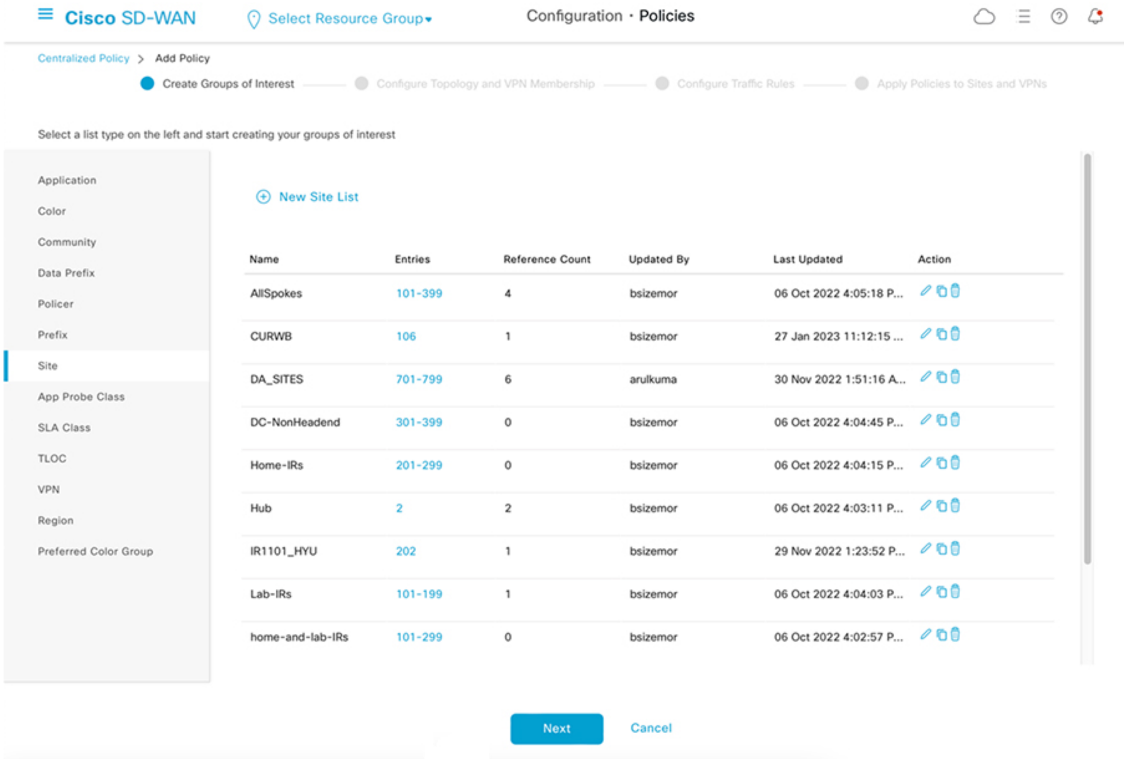
Enhance ECMP Keying can only be turned on in VPN0

Prefix	Service	Action
0.0.0.0/0	SIG	

Hub and Spoke Policy

1. Start by creating a new Centralized Policy.

Figure 47:

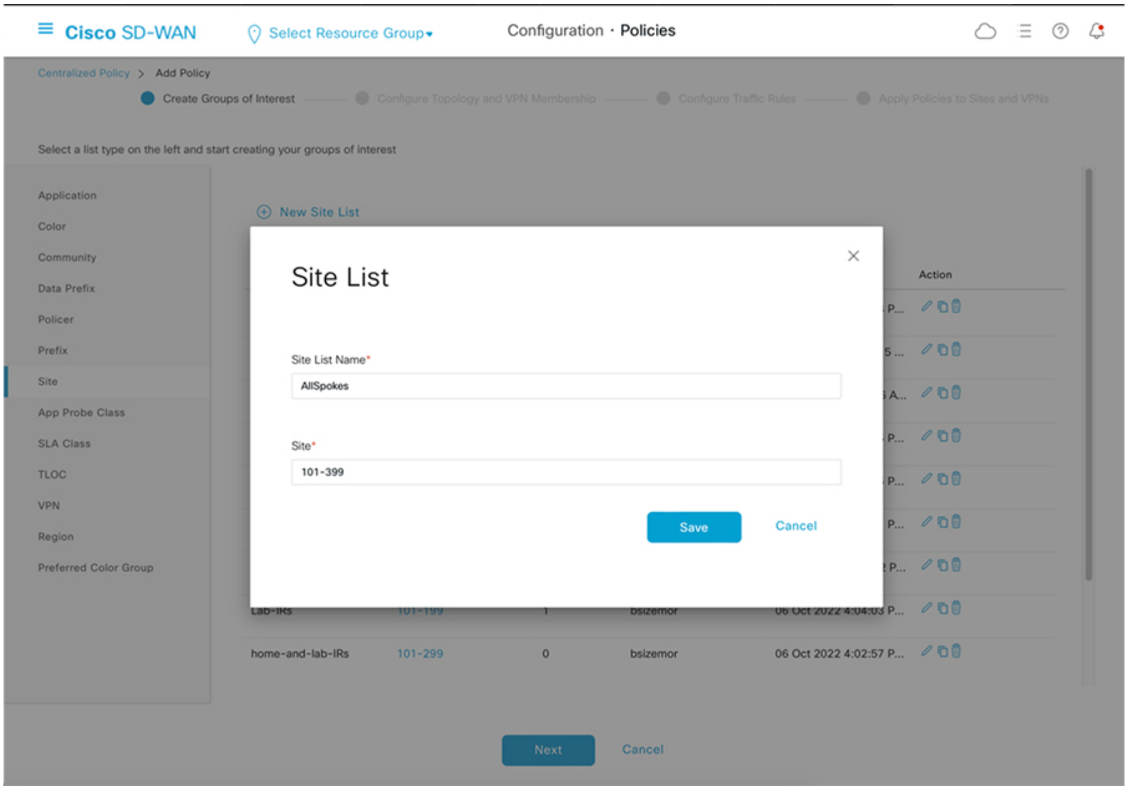


Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By	Last Updated	Action
AllSpokes	101-399	4	bsizemor	06 Oct 2022 4:05:18 P...	
CURWB	106	1	bsizemor	27 Jan 2023 11:12:15 ...	
DA_SITES	701-799	6	arulkuma	30 Nov 2022 1:51:16 A...	
DC-NonHeadend	301-399	0	bsizemor	06 Oct 2022 4:04:45 P...	
Home-IRs	201-299	0	bsizemor	06 Oct 2022 4:04:15 P...	
Hub	2	2	bsizemor	06 Oct 2022 4:03:11 P...	
IR1101_HYU	202	1	bsizemor	29 Nov 2022 1:23:52 P...	
Lab-IRs	101-199	1	bsizemor	06 Oct 2022 4:04:03 P...	
home-and-lab-IRs	101-299	0	bsizemor	06 Oct 2022 4:02:57 P...	

2. Next create two **Site Lists** – one for the hub, and one for the spokes. Add routers to the list based on Site ID, which can be a range like 100-399 for spokes, for example.

Figure 48:



Select a list type on the left and start creating your groups of interest

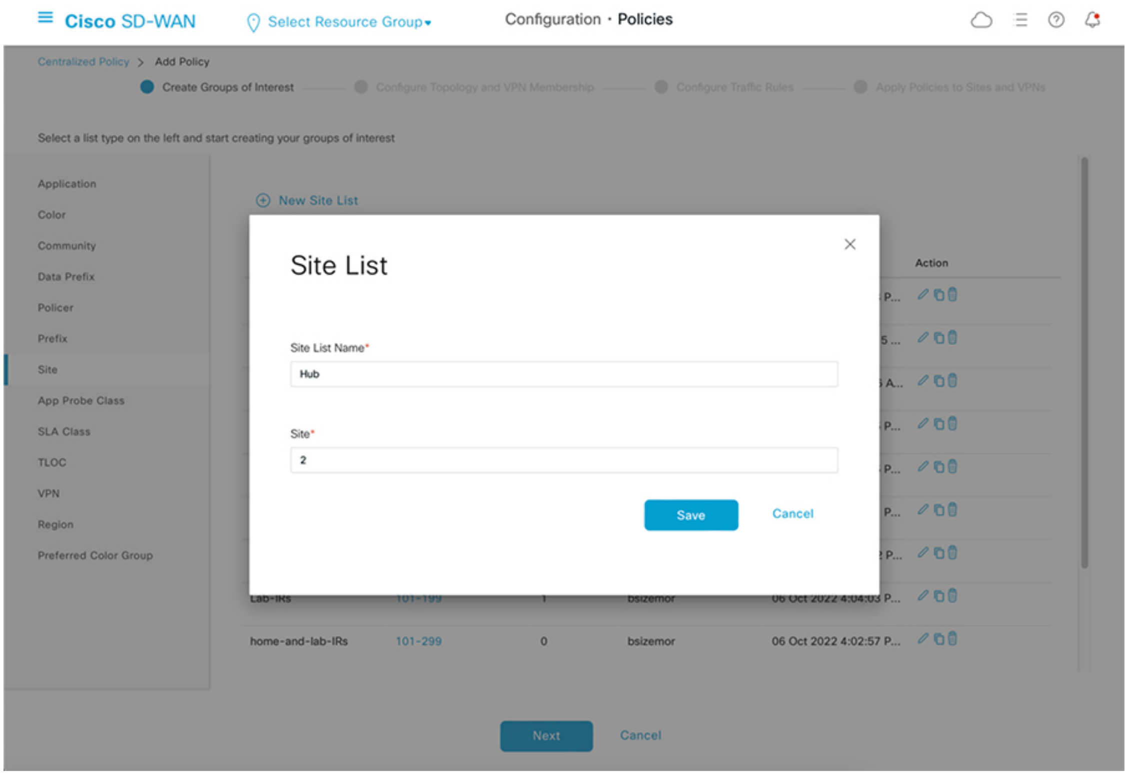
Site List

Site List Name*: AllSpokes

Site*: 101-399

Lab-IRs	101-199	1	bsizemor	06 Oct 2022 4:04:03 P...	
home-and-lab-IRs	101-299	0	bsizemor	06 Oct 2022 4:02:57 P...	

Figure 49:



Cisco SD-WAN · Select Resource Group · Configuration · Policies

Centralized Policy > Add Policy

● Create Groups of Interest — ● Configure Topology and VPN Membership — ● Configure Traffic Rules — ● Apply Policies to Sites and VPNs

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site
App Probe Class
SLA Class
TLOC
VPN
Region
Preferred Color Group

⊕ New Site List

Site List

Site List Name*
Hub

Site*
2

Save Cancel

Action

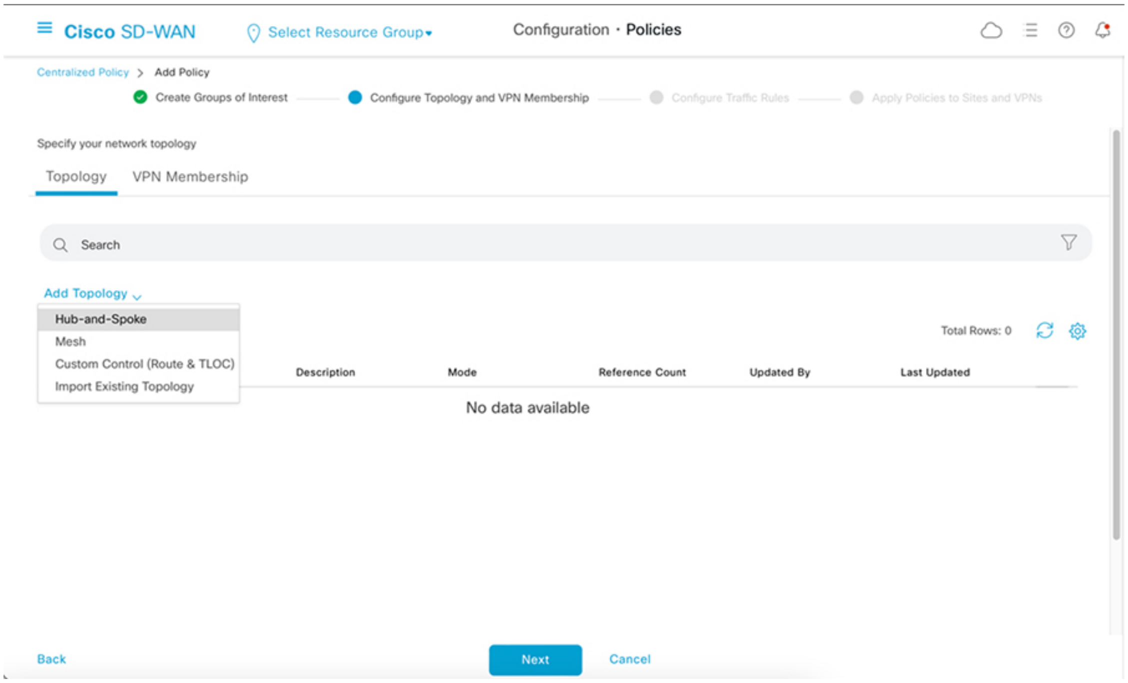
Lab-IRs 101-199 1 bsizemor 06 Oct 2022 4:04:03 P...

home-and-lab-IRs 101-299 0 bsizemor 06 Oct 2022 4:02:57 P...

Next Cancel

3. Next, add a Topology of type **Hub-and-Spoke.**

Figure 50:



Cisco SD-WAN · Select Resource Group · Configuration · Policies

Centralized Policy > Add Policy

✓ Create Groups of Interest — ● Configure Topology and VPN Membership — ● Configure Traffic Rules — ● Apply Policies to Sites and VPNs

Specify your network topology

Topology VPN Membership

Search

Add Topology
- Hub-and-Spoke
- Mesh
- Custom Control (Route & TLOC)
- Import Existing Topology

Total Rows: 0

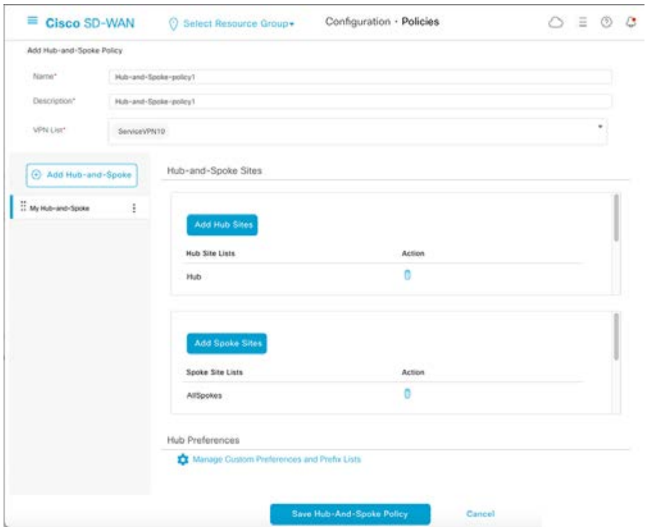
Description	Mode	Reference Count	Updated By	Last Updated

No data available

Back Next Cancel

4. Select the Hub and Spoke sites by selecting the **Site Lists** created earlier. Associate the policy with one or more Service VPNs.

Figure 51:



Add Hub-and-Spoke Policy

Name*: Hub-and-Spoke-policy1

Description*: Hub-and-Spoke-policy1

VPN List*: ServiceVPN10

Hub Site Lists	Action
Hub	

Spoke Site Lists	Action
AllSpokes	

Hub Preferences
Manage Custom Preferences and Prefix Lists
Save Hub-And-Spoke Policy
Cancel

5. Activate the policy.

Benchmark Data

Boot Time

Table 8: Time from power on to connectivity established over cellular

	Controller Mode	Autonomous Mode
IR1101 with P-LTEA-EA		6:28
IR1835 with P-LTEA-EA	6:04	5:40

Failover Performance

Table 9:

Scenario	Average failover time
Ethernet to Cellular (Last Resort)	7s
Cellular to Cellular (Active/active, ECMP Load Balancing)	7s
Cellular to Cellular (active/standby)	7s
Cellular to CURWB via Ethernet	7s

In all tests, the BFD timers were left with default values of 1000 milliseconds for hello interval, and multiplier of 7.

Memory Utilization – at idle

Routers configured with 4 Service VPNs and hub & spoke policy. There were no external devices connected to the service VPNs to generate data plane traffic beyond what is used for management by vManage servers.

	CPU	Memory
IR1101	25.6%	74.1%
IR1835	34.6%	41.0%