Connected Communities Infrastructure Solution Implementation Guide

Preface

This Cisco Connected Communities Infrastructure (CCI) Solution Release 2.1 Cisco Validated Design (CVD) Implementation Guide provides a comprehensive explanation of the Cisco Connected Communities Network infrastructure implementation, including Wi-Fi Access network, along with Smart Cities and Roadways vertical solution use cases such as Cisco Safety and Security, Cisco Smart Street Lighting, Supervisory Control and Data Acquisition (SCADA) Water, LoRaWAN Lighting, and Edge Computing.

This implementation document includes information about the solution architecture, possible deployment models, and guidelines for deployment. It also recommends best practices and potential issues when deploying the reference architecture.

Navigator

The document covers the following topics:

Chapter	Description
Implementation of CCI Access Networks, page 106	Describes implementation details of various access networks in CCI. It covers the implementation of the following access network and technologies: ■ Ethernet Access Network in Ring Topology ■ Cisco Resilient Mesh (CR-Mesh) Access Network ■ Dedicated Short Range Communications (DSRC) ■ LoRaWAN Access Network ■ Wi-Fi Access Network
Implementation of the Field Area Network, page 176	Describes the steps to implement Field Area Network for CR-Mesh. Explains the implementation in various places in the network, such as the headend network, onboarding Connected Grid Router (CGR) as gateway for CR-Mesh endpoints, and CR-Mesh network.
Implementing Remote Point-of-Presence (RPoP) Sites, page 234	Explains the detailed steps to implement the Remote Point-of-Presence (RPoP) network for connecting the remote LoRaWAN and CR-Mesh access network to the CCI Network headend infrastructure. **Note:** Although RPoP network can be used for connecting various other devices, only LoRaWAN and CR-Mesh have been validated.
VDSL Example, page 279	Describes the steps to implement vertical solution-specific Cisco application servers in the data center or headquarter site. Also covers the implementation of various partner applications (on-premises or cloud) required for Cities and Roadways verticals.
Implementing Network Security, page 363	Explains the detailed steps for implementing CCI network security such as macro- and micro-segmentation, Scalable Groups Tags (SGT)-based classification and propagation, policy enforcement, device or endpoints security, and Firepower.
Implementing CCI Network Quality of Service, page 401	Discusses the steps to deploy CCI network QoS on CCI fabric device and IE access rings.
Implementing CCI Network Multicast, page 416	Discusses steps to configure SD Access Multicast in a PoP site and between PoP sites.
Implementation of SCADA Communication with Multiple Backhaul Types and Protocols, page 434	Captures the detailed implementation steps and procedure of SCADA communication with multiple backhaul types and protocols. This implementation focused on Distributed Network Protocol 3 (DNP3) and MODBUS SCADA protocols.
FlashNet Lighting Use Case Implementation over LoRaWAN, page 514	Explains the detailed steps for implementing LoRaWAN-based FlashNet Lighting using Actility ThingPark Enterprise (TPE) as the network server.
Train to Trackside Roaming, page 537	Explains the detailed steps for secure onboarding of Axis cameras.
Train to Trackside Roaming, page 537	Describes how to extend network services out to a train network when a CCI network is being built out,
Caveats and Open Issues, page 557	Discusses CCI solution caveats and workarounds.
Appendix: Configuration Examples, page 558	Captures supplementary configurations used for the CCI network topologies validated in this CVD.

Audience

The audience for this guide comprises, but is not limited to, system architects, network/compute/systems engineers, field consultants, Cisco Solution Support specialists, and customers.

Readers should be familiar with networking protocols and IP Routing, basic network security and QoS, and be exposed to server virtualization using hypervisor and the Cisco Connected Communities Infrastructure (CCI) Solution architecture, which is described in the *Cisco Connected Communities Infrastructure CVD Solution Design Guide* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

Document Objective and Scope

This implementation guide provides a comprehensive details of Cisco Connected Communities Infrastructure (CCI) horizontal network infrastructure implementation leveraging the Cisco Digital Network Architecture Center (Cisco DNA Center) Software Defined Access (SD-Access) Fabric. The CCI solution horizontal access network infrastructure implementation is based on the *Cisco Software Defined Access Deployment Guid*e that can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.html

This document also provides details about implementing CCI vertical use cases such as cities safety and security and Cisco Smart Street Lighting and CCI overlay network use cases such as transportation/roadways intersection. While the implementation steps detailed in this document should be used as a reference for deploying other CCI vertical use cases, the detailed implementation of specific vertical use cases on the CCI network that are not validated in this solution is beyond the scope of this document.

This document covers example network underlay routing configurations and Multiprotocol Label Switching (MPLS) network backhaul configuration for the deployment models and network topologies validated in the solution. Detailed implementation of network routing protocols and configuring MPLS network backhaul is beyond the scope of this document.

Introduction

The Cisco CCI solution is a multi-service network architecture for a City Campus or a Metropolitan area and Roadways that leverages Cisco's Intent-Based Networking and SD-Access with Cisco DNA Center management to bring the latest developments in network segmentation, automation, and endpoint authentication.

The CCI solution architecture also includes ruggedized access network devices such as Cisco Industrial Ethernet (IE) Switches, Connected Grid Routers (CGR), Cisco Industrial Routers (IR), Cisco Long Range Wide Area Network (LoRaWAN) gateway, and the Cisco® IC3000 Industrial Compute Gateway along with other network infrastructure components to provide a scalable and secure network for CCI vertical solution use cases. The CCI solution implementation is based on the design recommended in the *Cisco Connected Communities Infrastructure Solution Design Guide* that can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html

This guide details the implementation of the Cisco CCI horizontal network, which includes the implementation of the CCI network underlay, shared services, backhaul network (Ethernet and MPLS), SD-Access Fabric overlay network, access networks like Ethernet Access Rings using Cisco IE switches and CR Mesh, and access technologies like DSRC and LoRaWAN.

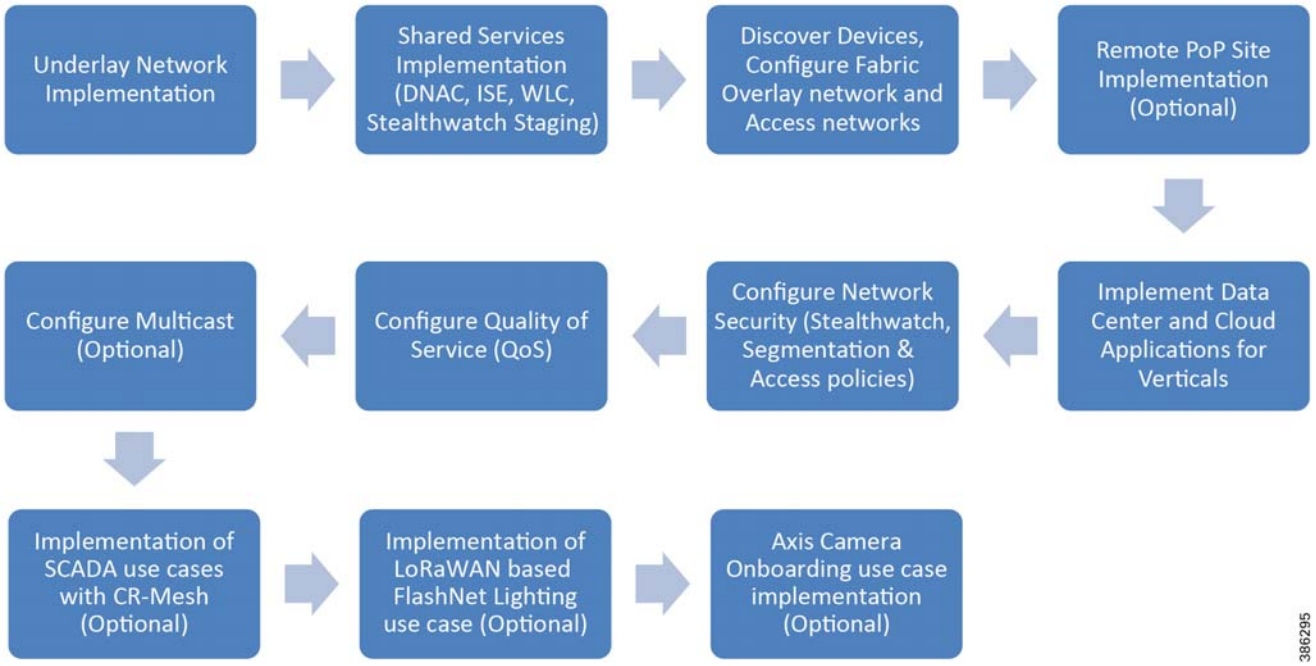
However, in some deployments of CCI, there could only be Remote Point-of-Presence (RPoP) sites comprised of CGR, IR1101, and IR1800 Series routers, and is typically connected to the Public Internet (a cellular network, for example), over which secure FlexVPN tunnels are established to the Headend in the CCI Headend network in the Demilitarized Zone (DMZ). Such RPoP-only CCI deployments, which do not require Cisco SD-Access, could be implemented by following the steps described in Implementing Remote Point-of-Presence (RPoP) Sites, page 234.

New Capabilities in CCI Release 2.1

- Cisco Ultra Reliable Wireless Backhaul (CURWB) for CCI backhaul and wireless access networks
- Enhanced Ethernet Access Ring & Provisioning
  - IE-3300 10G Access Ring in CCI PoPs
  - Daisy Chaining Automation of Extended and Policy Extended Nodes using Cisco DNA Center
  - REP Ring Automation using Cisco DNA Center
- Cisco CyberVision OT Device and Flow Detection
  - CyberVision Sensor deployment on IE-3400, IE-3300 10G and IR-1101 Platform
  - OT Device and Protocols (DNP3 and MODBUS) Flow Detection using Cisco Cyber Vision Center
- Enhanced End-to-End QoS design on IE3400 and IE3300 10G
- Enhanced Remote Point-of-Presence (RPoP) Management design
  - IR-1800 as RPoP gateway with multi-service and macro-segmentation at RPoP
  - RPoP Management Design using Cisco DNA Center and Cisco IoT Operations Dashboard (IoTOD)

This document also provides implementation details for overlaying CCI vertical use cases like Cities Safety and Security, Cisco Smart Street Lighting, SCADA use cases, LoRaWAN Lighting, and Rail and Roadways intersection on the CCI network. It is recommended to implement CCI network and vertical use cases, as depicted in Figure 1, which shows the flow of the material in this implementation guide:

Figure 1 CCI Solution Implementation Flow



The document addresses the implementation of the following CCI network horizontal and vertical use cases:

- CCI Underlay Network implementation for basic network (Layer 3) IP forwarding and connectivity.
- Implementation of shared services like Cisco DNA Center, Identity Service Engine (ISE), Cisco Wireless LAN Controller (WLC) and Cisco Prime Infrastructure (PI), Cisco CyberVision Center, DHCP, and DNS servers, as well as other shared IoT devices management applications such as Field Network Director (FND).
- Configuring Cisco SD-Access Fabric Site (Point-of-Presence aka PoP) as overlay network and Interconnection of the Fabric Sites leveraging Cisco DNA Center.
- Implementation of Cisco Industrial Ethernet switches—Cisco Industrial Ethernet (IE) 4000, Cisco Industrial Ethernet (IE) 5000, Cisco Catalyst Industrial Ethernet and Embedded Services 3300 and 3400 series switches—as fabric extended nodes, policy extended nodes, in Ethernet access network rings.
- Implementation of Cisco Unified Wireless Network (CUWN) Wi-Fi Mesh and SD Access Wireless Wi-Fi access networks.
- Implementation of headquarter site data center applications for vertical use cases and services on the fabric overlay network. It covers Cities Safety and Security, LoRaWAN, ThingPark Enterprise, and applications such as Certificate Authority (CA) services needed for Cisco Smart Street Lighting solution use cases along with Public Wi-Fi use cases.
- Deployment details for LoRaWAN in Remote PoP.
- Deployment details for Remote PoP over cellular network backhaul for multi-services and macro-segmentation.
- Deployment details for LoRaWAN in Remote PoP (optional).
- Implementation of end-to-end network security, which covers macro- and micro-segmentation of CCI networks using Virtual Networks (VNs) and Scalable Group Tags (SGT) and Scalable Group Access Control Lists (SGACL), network devices and endpoints security, and network firewall implementation in the DMZ and Stealthwatch.
- End-to-end network QoS implementation for traffic classification, prioritization, queuing, and policing.

- Implementation of multicast network forwarding in CCI. Enabling multicast in CCI is optional as it is needed if you want to implement any vertical use case which requires multicast traffic forwarding in CCI.
- Implementation of SCADA communication use cases with CR-Mesh network.
- Implementation of LoRaWAN-based FlashNet lighting use case.
- Axis camera Day 0 onboarding and Day N management in CCI.

Solution Network Topology and Addressing

This section, which discusses the various topologies used for solution validation and implementation, includes the following major topics:

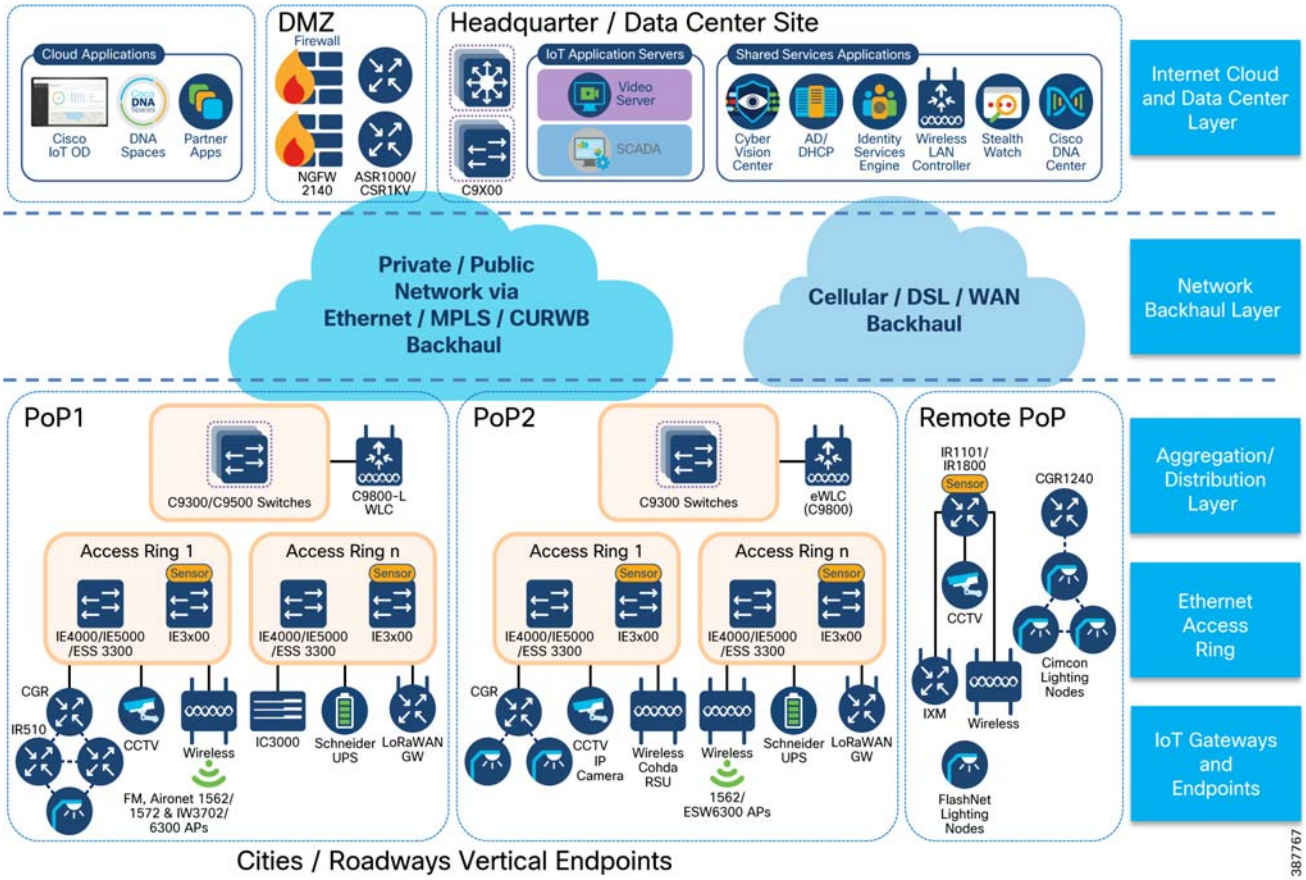
Deployment Topology Diagrams

This section describes the different deployment network topologies that have been validated in the CCI Solution Implementation.

High Level Solution Validation Topology

Figure 2 depicts the CCI high level validation topology, including the endpoints for vertical use cases validated in this solution implementation:

Figure 2 CCI High Level Solution Validation Topology



The multiple layers of topology include:

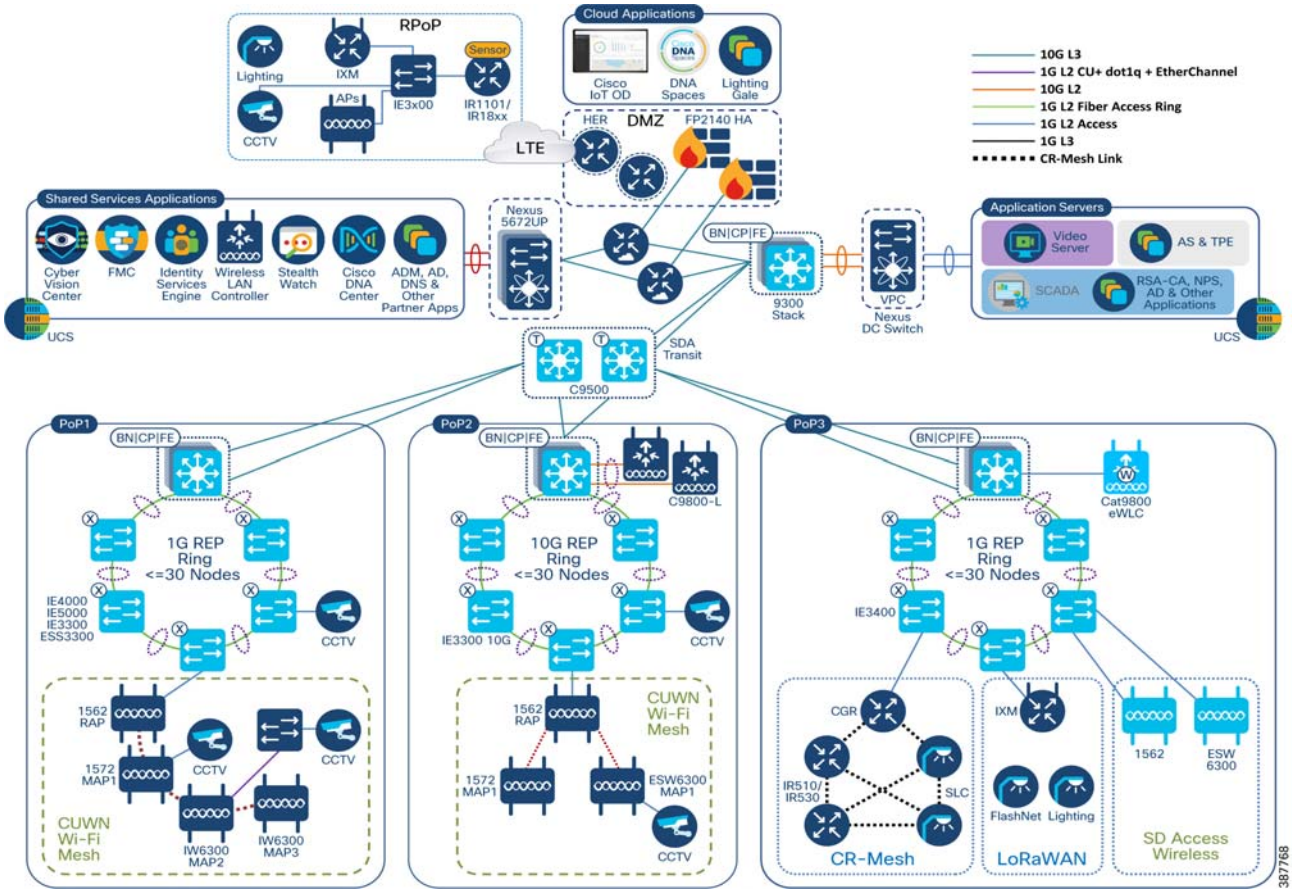
1. Internet Cloud and Data Center layer, which includes:
   - Network connectivity to Demilitarized Zone (DMZ) to access Internet/Applications on the cloud.
   - A Headquarter or Data Center Site (HQ/DC Site) aka Application Servers Site consisting of:
     - Application servers for hosting vertical specific applications needed on the CCI horizontal network
     - Shared services like Cisco DNA Center, ISE, DHCP, DNS servers, Stealthwatch Management Console (SMC) and Flow Collector (SFC), Cisco Cybervision Center, CURWB Global gateway along with other applications that are common to all vertical use cases like FND, Axis Device Manager (ADM) for both Cities and Transportation/Roadways.
2. Network backhaul layer interconnects PoPs and the Internet Cloud/Data Center layer with either the private enterprise Ethernet network or private MPLS network backhaul. Remote PoPs connect to the CCI network via cellular or private/public network backhaul.
3. Aggregation layer aggregates all PoPs traffic to the upper layers.
4. Ethernet access ring provides network access to gateways/endpoints validated in the solution.
5. Internet of Things (IoT) gateways and endpoints layer includes Access Points (AP) for Wi-Fi access, Curwb Access Points for Rail, access gateways based on access technologies (such as DSRC, LoRaWAN, and CR-Mesh) and their endpoints validated in this solution.

Solution Validation Topologies

Two deployment models of the CCI solution have been validated during this implementation:

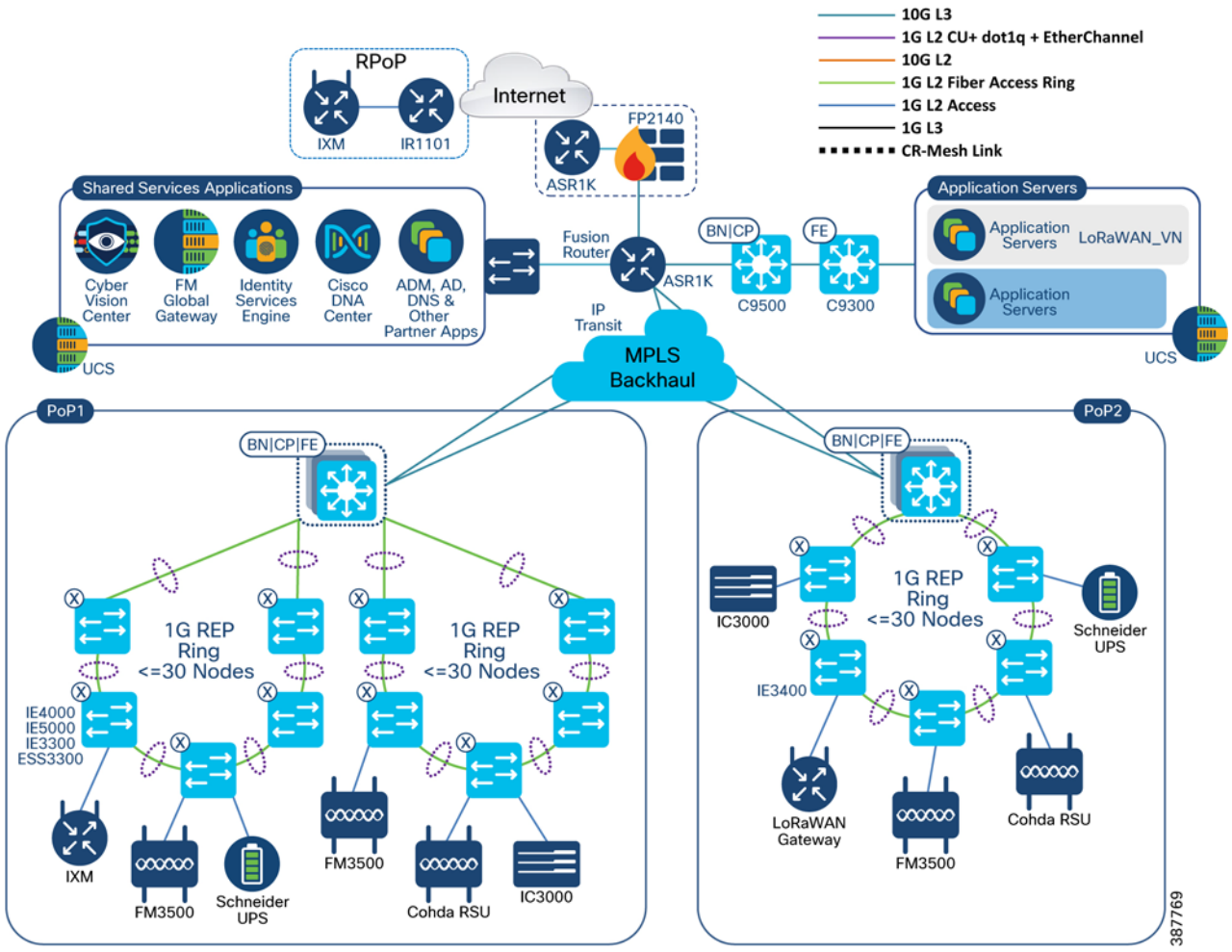
1. CCI network deployment topology with Cisco SD-Access Transit, henceforth referred to as SDA Transit interconnection of all sites. The validation is done over the Enterprise Ethernet Network backhaul (using Cisco Catalyst 9500 switches as the network core). This topology is depicted in Figure 3.
2. CCI network deployment topology with IP Transit interconnection of PoPs and headquarter sites with validation done over Private MPLS network backhaul, as shown in Figure 4.

Figure 3 SD-Access Transit with Enterprise Backhaul Network Topology



Note: In Figure 3, the PoP1 with C9500 SVL is also supported to connect IE switches to just the nearest Catalyst 9500 stack member. This could be likely when there is insufficient fiber pairs between the two physical locations where each stack member is housed, however in this case also a Port Channel is still used with single member link automated by DNA Center.

Figure 4 IP Transit with MPLS Backhaul Network Topology



Network topologies validated in this CVD include FlexVPN tunnels that are configured for securing the communication between the Cisco 1240 Connected Grid Router and the HER in Cisco Smart Street Lighting solution use cases implemented on the CCI network.

For more details about fabric device roles (B-Border, CP-Control Plane, E-Edge, T-Transit, X-Extended Node) in the network topology, refer to the *Cisco Connected Communities Infrastructure CVD Solution Design Guide*.

IP Addressing

This section captures the example IP addressing prefixes used in the solution lab topology, as shown in Figure 3.

Note: The IP addresses captured in this section are example IP addressing used only for the solution validation as internal sub-networks in the CVD lab. It provides a reference for selecting subnets for the solution implementation. It is recommended to choose private network prefixes/IP addressing scheme depending on the solution deployment and devices connected to the CCI network.

Addressing Convention followed in the IP Subnet Selection

Four prefixes are used in the network subnet for the network topology (where **X** is the site ID chosen for a PoP site/ transit site and the underlay network devices, if any).

- **192.0.X. YY**–Devices Loopback IP addresses prefix

- **172.10.X. YY**—Virtual Network (VN) subnets prefix
- **192.168.X. YY**—Fabric Overlay Border Handoff Network prefix
- **192.100.X. YY**—Fabric Extended Nodes IP Pool prefix

Table 1 Example IP Addressing Prefixes and Convention Followed

Prefix	Purpose	Component(s) Connected by the Subnet	Sample IP Address
192.0.X. YY / 32	Loopback addresses for all the devices in the network topology.	PoP1 Site - Cisco Catalyst 9500 SVL	192.0.160.11
		PoP2 Site - Cisco Catalyst 9300	192.0.150.11
		PoP3 Site - Cisco Catalyst 9300	192.0.120.11
		RPoP1 Site - Cisco IR1101	192.168.200.25
	All fabric and non-fabric devices in the network.	HQ/DC Site - Cisco Catalyst 9300	192.0.140.11
		SDA Transit Node 1: Cisco Catalyst 9500	192.0.130.11
		SDA Transit Node 1: Cisco Catalyst 9500	192.0.130.12
172.10.X. YY/24	IP Subnet used in Virtual Networks (VRF) for endpoints/hosts data	PoP1 Site Safety and Security IP Camera	172.10.80.11
		PoP2 Site Safety and Security IP Camera	172.10.100.11
		PoP3 Site Safety and Security IP Camera	172.10.90.11
		RPoP1 Site Safety and Security	172.10.25.21
192.168.X.YY/24	Global Prefix used by Cisco DNA Center for Border Hand-off configuration to the Fusion Router, in case of IP Transit.	Cisco DNA Center Border Handoff Subnet	192.168.80.0/30
			192.168.90.0/30
			192.168.100.0/30
		PoP1 Site - Cisco Catalyst 9500 SVL	192.168.80.1
		PoP2 Site - Cisco Catalyst 9300	192.168.100.1
		PoP3 Site - Cisco Catalyst 9300	192.168.90.1
		Fusion Router	192.168.70.2
192.100.X.YY/24	Global IP Prefix used for Extended Nodes in the network	PoP1 Site Extended Nodes IP Pool	192.100.80.0/24
		PoP2 Site Extended Nodes IP Pool	192.100.100.0/24
		PoP3 Site Extended Nodes IP Pool	192.100.90.0/24
10.10.100.0/24 10.10.201.0/24	Shared Services (SS) Network Prefix	Cisco DNA Center	10.10.201.202 (subnet in SS)
		Cisco ISE	10.10.100.55
		DHCP/DNS Server	10.10.100.20
		Field Network Director (FND)	10.10.100.11
		CUWN WLC (C9800-40)	10.10.100.188
		Cisco Prime Infrastructure (PI)	10.10.100.65
		Cisco Stealthwatch Management Controller (SMC)	10.10.100.75
		Cisco Stealthwatch Flow Collector (SFC)	10.10.100.85

Note: Refer to IP Addressing of Solution Components, page 558 for more details about IP addresses, including IP addresses used for underlay network connectivity for the network topologies, as shown in Figure 3, Figure 4, and Figure 19.

Solution Virtual Networks and Scalable Groups

In the CCI implementation, a Virtual Network (VN) is used for a vertical service. This macro-segmentation provides complete separation between services. One VN can communicate with another only by leaking routes between the VRF at the fusion router. Table 2 provides an example list of VNs used in the CCI solution validation.

Example VNs for the Cities and Roadways applications include Safety and Security, Cisco Smart Street Lighting, Iteris, Schneider, and LoRaWAN. Further micro-segmentation within a virtual network is possible by using Scalable Group Tags (SGT). Table 2 also provides an example list of SGTs for micro-segmentation of the VN.

Table 2 Example Virtual Networks and Scalable Groups Used in the CCI Solution

Services	Virtual Network (VN) Name	Purpose	Scalable Groups
Cities Safety and Security Service	SnS_VN	VN, including all subnets defined for Cities Safety and Security Camera and Servers data traffic	SnS_Cameras SnS_Servers CCI_SSID1_SnS_VN CCI_SSID2_SnS_VN
Cities Smart Street Lighting Service	Lighting_VN	VN, including all subnets defined for CIMCON street lighting vertical services data traffic	Lighting_Gateways Lighting_Servers
Iteris	Iteris_VN	VN, including all subnets defined for Iteris traffic	Iteris
Roadways	Roadways_VN	VN, including all subnets defined for Schneider and Roadways traffic	Schneider
LoRaWAN	LoRaWAN_VN	VN, including all subnets defined for LoRaWAN traffic	LoRaWAN

Solution Components

This section covers the Cisco hardware and software component version validated in this CCI solution implementation for CCI horizontal network and CCI vertical-specific use cases implementation such as Cities Safety and Security and Street Lighting and Roadways for the system validation topology, as shown in Figure 2.

It also captures the CCI vertical solution partner hardware and software components along with other third-party applications validated in this implementation.

Table 3 and provide the list of Cisco components and the corresponding version validated in the CCI Horizontal Network and Cities Safety and Security vertical use case applications:

Table 3 Cisco Hardware and Software Versions Validated in this CVD

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
C9300-24UX	Cisco SD-A Fabric in a Box Switch	IOS-XE 17.6.1	PoP site aggregation/distribution layer switch
C9500-16X	Network Aggregation Switches	IOS-XE 17.6.1	Core switch for enterprise Ethernet network backhaul and fusion router in IP Transit
IE-4000-4GS8GP4G-E IE-4000-8GS4G-E	Access Rings Industrial Ethernet IE4000 Switches as Extended and Non-extended Nodes in PoP (fabric) sites	15.2 (8)E	Ruggedized access switch in PoP rings
IE-5000-12S12P-10G	Access Rings Industrial Ethernet IE5000 Switches as Extended and Non-extended Nodes in PoP (fabric) sites	15.2 (8)E	Ruggedized access switch in PoP rings
IE-3300-8P2S-E IE-3300-8T2S-E IE-3400-8T2S IE-3400-8P2S-A ESS-3300-CON IE-3300-8U2X IE-3300-8T2X	Access Rings Industrial Ethernet IE3x00 Switches as non-extended nodes in PoP (fabric) sites	IOS-XE 17.6.1	Ruggedized access switch in PoP rings
DN2-HW-APL	Cisco DNA Center Appliance	2.3.2.1	Centralized, Single Pane of Glass network management for Cisco's intent-based network with foundation controller and analytics platform
ASR1006-X	Cisco Aggregation Services Routers 1006-X (HER and Fusion Router)	16.9.5	Fusion Router in IP Transit topology with MPLS network backhaul
Firepower2140	Firewall (Firepower Intelligence Threat Defense)	7.1	Firewall
Nexus 5672UP	Headend Data Center network switch	7.3 (3) N1(1)	DC switches
UCS-C220-M5	Unified Computing System (UCS)	3.1.3c	Computing server for hosting applications
WS-C3850-24U-L	DMZ Layer 2 switch	16.12.1	--

Table 3 Cisco Hardware and Software Versions Validated in this CVD (continued)

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
IR1101-A-K9	Remote PoP Aggregation Router with Cellular Backhaul	17.6.1	Ruggedized 5G Ready, modular, dual active LTE-capable (two cellular networks for WAN redundancy) ISR
IR1835-A-K9	Remote PoP Aggregation Router with Cellular Backhaul	17.6.1	Ruggedized high-performance, 5G routers in a modular design that support private LTE, Wi-Fi6, and Gigabit Ethernet
C9800-40-K9 C9800-L-C-K9 C9800 Embedded on C9300	Wireless LAN Controller	IOS-XE 17.6.1	Wireless LAN Controller for CUWN (in the case of 9800-40, 9800-L)
AIR-AP1562E-D-K9 AIR-AP1572EAC-D-K9	Cisco Aironet Outdoor Access Points	IOS-XE 17.6.1	Outdoor 802.11ac APs
ESW6300 IW3702-2E-UXK9	Cisco Industrial Access Points	IOS-XE 17.6.1	Outdoor 802.11ac APs

.

Table 4 Cisco Software Applications Validated in this CVD

Software Application	Role in CCI	Software/Firmware Version	Remarks
Cisco ISE Virtual Appliance	Authentication & Policy Server	3.0.4	AAA Server
CSR1000V as Virtual Appliance	Cloud Service Router 1000V as fusion routers	17.6.1	Fusion router in SDA transit topology
Cisco CyberVision Center and Sensors	Network Sensors and Applications	4.0.1	IT and OT Network Visibility Sensor and application

Table 5 and Table 6 provide the list of Cisco components and its version validated for the Street Lighting solution on the CCI network for the Cities vertical.

Table 5 Cisco Hardware and Software Components for Cisco Smart Street Lighting Solution with CR-Mesh

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
CGR1240	Connected Grid Router (CGR) for CR Mesh	15.9(3)M2	Mesh Gateway
CGM-WPAN-FSK-NA	Wireless 6Low FSK Module for CR Mesh	5.7 (27)	CR-Mesh RF module
CGM-WPAN-OFDM-FCC	Wireless 6Low PAN ORDM Module for CR Mesh	6.2.19	CR-Mesh RF module

Table 6 Cisco Software Applications Validated for Cisco Smart Street Lighting Solution with CR-Mesh

Software Application	Role in CCI	Software Release Version	Remarks
CSR1000V	Cloud Service Router 1000V - Head End Router (HER)	17.6.1	Virtual CSR1KV Appliance
Field Network Director (FND) Virtual Appliance (OVA)	Network Management Server for IoT gateways and endpoints	4.6	--
Cisco Prime Network Registrar (CPNR) Virtual Appliance (OVA)	DHCPv6 Server for Connected Grid Endpoints (CGE)	9.1.2	Centralized DHCPv6 Server for CGE
Cisco IR510 CR Mesh Gateway	Wireless 6Low Gateway for CR Mesh	6.2.19	CR Mesh Gateway Module
Cisco IR530 Range Extender	Range extender for CR Mesh network, providing longer reach between WPAN endpoints	6.2.19	CR Mesh Range Extender Module

Table 7 and Table 8 provide the list of CIMCON components and its version validated for the Street Lighting solution on the CCI network for the Cities vertical along with other third-party applications used in this solution implementation:

Table 7 CIMCON Hardware Component for Cisco Smart Street Lighting Solution

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
iSLC3100-7P-C	Street Light Controller (SLC)	3.0.32_EXT	Lighting node

Table 8 CIMCON and Third Party Software Components for Cisco Smart Street Lighting Solution

Software Application	Role in CCI	Software/Firmware Version	Remarks
LightingGale (LG) on AWS Cloud	Street Lighting Management Application	5.1.2.41	Cloud lighting management application
Communication Module Firmware on SLC	CR-Mesh Firmware (CGE)	2.0.15	Communication module, including CIMCON application middleware
Hypervisor for Computing Servers	VMware Hypervisor	ESXi 6.5	Third party
Certificate Authority Server as a Virtual Machine	RSA Certificate Authority (CA)	Windows Server 2016	Third party
Certificate Authority Server as a Virtual Machine	ECC Certificate Authority (CA) for CGE	Windows Server 2016	Third party
Active Directory and AAA Server as a Virtual Machine	Active Directory (AD) and Network Policy Server	Windows Server 2016	Third party

Table 9 Hardware Components and Versions for LoRaWAN Solution

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
IXM-LPWA-900-16-K9	Cisco Wireless Gateway for LoRaWAN which operates on the subsets of 902 - 928 MHz ISM frequencies	2.0.32	--
IXM-LPWA-800-16-K9	Cisco Wireless Gateway for LoRaWAN which operates on the subsets of 863 - 870 MHz ISM frequencies	2.0.32	--

Table 10 Software Components and Versions for LoRaWAN Solution

Software	Role in CCI	Software/Firmware Version	Remarks
ACT-ENT-OCP-SM	ThingPark Enterprise (TPE) - LoRaWAN Enterprise On-Prem network server software, up to 10 gateways, 2,000 sensors, and 3 standard data flows Annual Subscription	5.2.2.5 (OVA version 4.6)	--
ACT-ENT-OCP-MD	ThingPark Enterprise (TPE) - LoRaWAN Enterprise On-Prem network server software, up to 50 gateways, 10,000 sensors, and 5 standard data flows Annual Subscription	5.2.2.5 (OVA version 4.6)	--
ACT-ENT-OCP-LG	ThingPark Enterprise (TPE) - LoRaWAN Enterprise On-Prem network server software, up to 100 gateways, 20,000 sensors, and 20 standard data flows Annual Subscription	5.2.2.5 (OVA version 4.6)	Not tested in this release
LRR	Packet Forwarder for LoRaWAN	2.4.85	Available from LoRaWAN Enterprise On-Prem network server dashboard

Table 11 Hardware Components and Versions for LoRaWAN based FlashNet Use Case implementation

Hardware	Role in CCI	Firmware Version	Remarks
FRE220-NEMA	FlashNet light	3498(FRE220NEMA_b_Q85_5min)	--

Table 12 Software Components and Versions for LoRaWAN based FlashNet Use Case implementation

Software	Role in CCI	Software/Firmware Version	Remarks
inteliLIGHT control software	Management of FlashNet lights	2.2.11	--
AS platform	Cloud application for integration with ThingPark Enterprise (TPE)	3923	--

Table 13 Hardware Components and Versions for Axis Cameras Use Case Implementation

Hardware Model	Role in CCI	Software/Firmware Version	Remarks
AXIS P3717-PLE	Axis cameras	10.1.0	--
AXIS Q6075-E	Axis cameras	10.0.2	--

Table 14 Software Components and Versions for Axis Cameras Use Case Implementation

Hardware Model/Software	Role in CCI	Software/Firmware Version	Remarks
AXIS Device Manager (ADM)	Axis Camera Management	5.09.042	--

Note: Make sure to install licenses for each of the products in the CCI solution. Refer to the respective product's installation/licensing guide for more details on product license activation.

Table 15 CURWB Components

Trackside Network Function	CURWBCURWB Platform	Version	CURWB Role	CVD Verified
Trackside Radio	FM 3500	9.3	Mesh Point/Mesh End	Yes
Train Radio[1]	FM 4500	9.3	Mobile Radio	Yes
Trackside Gateway	FM 1000	1.3.1	Mesh End/Global Gateway (no radio function)	Yes
Datacenter Gateway	FM 10000	2.0.1	Global Gateway	Yes
Antenna	FM Tube, Panel	N/A	Trackside/Tunnel antenna	No
Device Provisioning	Configurator, RACER	N/A	Local or Cloud provisioning	Yes
Network Monitoring	Monitor	N/A	Network Monitoring	No

1. The Train Radio is not part of the trackside infrastructure. The FM 4500 resides on the train to communicate with the FM 3500 on the trackside.

Underlay Network Implementation

The underlay network is defined by the switches and router in the network that are used to deploy the SD-Access network. In CCI, the underlay must establish IP connectivity via the use of a routing protocol. Instead of using arbitrary network topologies and protocols, the underlay implementation for SD-Access uses a well-designed Layer 3 foundation inclusive of the campus edge switches (also known as a routed access design), to ensure performance, scalability, and high availability of the network. Before the Cisco DNA Center can discover and manage the fabric devices, it must have this underlay network to reach them. This section covers the example configurations for implementing underlay network for CCI when CCI PoPs are interconnected via either Enterprise Ethernet backhaul or MPLS backhaul.

Note: Underlay network and routing configurations discussed in this section are example configurations used in the solution validation for the network topologies, as shown in Figure 3 and Figure 4 only. Depending on the CCI network deployment, you can choose to implement either of or both the network backhauls.

This section includes the following major topics:

Configuring Enterprise Ethernet Network Underlay

Ethernet as a backhaul, is one of the enterprise networks backhaul deployment methods that can be implemented in CCI horizontal network, as shown in Figure 3. The underlay network connectivity between shared services and all devices in each PoP site (including HQ/DC site) is provided through the backhaul network. The underlay network configuration is a basic network connectivity prerequisite for implementing the fabric overlay network for the CCI solution using the Cisco DNA Center.

Many protocols are available to configure IP routing, but in this implementation EIGRP is used as an example routing protocol for configuring underlay network connectivity and IP routing across PoP Sites and shared services. Cisco DNA Center uses Border Gateway Protocol (BGP) as the routing protocol when a border node connects to an IP transit, which means the configuration co-exists with the underlay configuration.

Configuring Cisco Catalyst 9300 Switch Stack for Fabric-in-a-Box

In the CCI Solution, all fabric/PoP sites leverage the Cisco Catalyst 9300 switch stack as an aggregation/distribution layer switch for aggregating traffic from access rings. Switch stack ensures redundancy. A stack of Cisco Catalyst 9300 switches appears to the operator and the rest of the network as one single switch, making it easier to manage and configure. Newer switch models add stateful failover capability, providing similar behavior as a chassis with dual supervisors in case of a failure or the need to update software on the stack.

Cisco Catalyst 9300 switch stack configuration is the initial step for provisioning a PoP site network (along with redundancy) for the access rings network and backhaul network connectivity network in the CCI topology. Refer to the following URL for configuring Cisco Catalyst 9300 switches in a stack:

- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/stck_mgr_ha/b_176_stck_mgr_ha_9300_cg/managing_switch_stacks.html

Configuring Cisco Catalyst 9500 Switches StackWise Virtual for Fabric-in-a-Box

Alternatively, Cisco Catalyst 9500 Series switches can be used as PoP sites aggregation/distribution layer switch for aggregating traffic from access rings in CCI. Cisco Catalyst 9500 platform StackWise Virtual (SVL) technology allows the clustering of two physical switches, that are geographically separated, together into a single logical entity. The two switches operate as one; they share the same configuration and forwarding state. This technology allows for enhancements in all areas of network design, including high availability, scalability, management, and maintenance.

Cisco Catalyst 9500 switch SVL configuration is the initial step for provisioning a PoP site network (along with redundancy) for the access rings network and backhaul network connectivity network in the CCI topology.

StackWise Virtual domain is elected as the central management point for the entire system when accessed via management IP or console. The switch acting as the single management point is referred to as the SV active switch. The peer chassis is referred to as the SV standby switch. The SV standby switch is also considered a hot-standby switch, since it is ready to become the active switch and it takes over all functions of active switch when active switch fails.

When the Catalyst 9500 SVL is used in the role of the Fabric-in-a-Box (FiaB) (Border + Control Plane + Edge), the connection to a Transit Site (for example, SD Access Transit switches) must be done with interfaces configured as a switchport trunk. A Switched Virtual Interface (SVI) is used for the Layer 3 configuration.

Conversion to StackWise Virtual Mode

Refer to the section "How to Configure Cisco StackWise Virtual" for configuring Cisco Catalyst 9500 switches in a SVL Mode at the following URL:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/ha/b_176_ha_9500_cg/configuring_cisco_stackwise_virtual.html

Configure Layer 3 on Ethernet Backhaul Network

Cisco Catalyst 9500 switches are used to provide the Ethernet network backhaul for interconnecting PoP sites and Shared Services, and Data Center applications in the HQ PoP Site, as shown in Figure 3. The following configuration provides an example configuration to enable Cisco Catalyst 9500 switches for the underlay network routing (Layer 3) for the network topology, as shown in Figure 3.

Configure the Layer 3 interface for the underlay network on Cisco Catalyst 9500 switches:

Example Interfaces Configuration on Cisco Catalyst 9500-1 (Transit Site)

1. Loopback interface is configured on the device for Cisco DNA Center discovery:

```
interface Loopback0
 ip address 192.0.30.11 255.255.255.255
 !
```

2. Configure an interface as a trunk to a PoP Site Cisco Catalyst 9300 stack:

```
interface TenGigabitEthernet1/0/3
 description Connected to C9300-20-STACK on port TE 1/1/1
 switchport mode trunk
!
```

3. Configure an SVI interface (example: VLAN 200) for underlay reachability between Fusion Router 1 and Cisco Catalyst 9300 stack, which is FiaB:

```
interface Vlan200
 ip address 20.20.20.1 255.255.255.252
!
```

4. Configure Layer 3 Port Channel between C9500 switches in Transit sites. On 9500-1:

```
interface TenGigabitEthernet1/0/1
no switchport
no ip address
channel-group 13 mode active
end
!
interface TenGigabitEthernet1/0/2
no switchport
no ip address
channel-group 13 mode active
end
```

```
!
interface Port-channel13
description Port Channel interface to C9500-R-2
no switchport
ip address 130.130.130.1 255.255.255.252
end
```

5. EIGRP routing protocol is configured between fusion routers and Cisco Catalyst 9300 stack network devices to form neighbors:

```
router eigrp 2000
 network 120.120.120.0 0.0.0.3   # PoP Site C9300 Stack underlay network subnet
 network 120.120.122.0 0.0.0.3   # HQ/DC Site P2P underlay network subnet
 network 130.130.130.0 0.0.0.3   # Between C9500 switches in Transit Site
 network 192.0.130.11 0.0.0.0
 eigrp router-id 192.0.130.11
```

Note: EIGRP is chosen as an example routing protocol for the underlay network routing configuration. Refer to the Cisco Connected Communities Infrastructure Design Guide for more details on recommended routing protocol for the underlay network routing configuration.

Example Interfaces Configuration on 9500-2 (Transit Site)

1. Loopback is configured on the device for Cisco DNA Center discovery:

```
interface Loopback0
 ip address 192.0.30.12 255.255.255.255
!
```

2. Configure an interface on 9500-2 as a trunk to the Cisco Catalyst 9300 stack:

```
interface TenGigabitEthernet2/0/3
 description Connected to C9300-20-STACK on port TE 2/1/1
 switchport mode trunk
!
```

3. Configure an SVI interface (for example, VLAN201) for underlay reachability between Fusion Router 2 and the Cisco Catalyst 9300 stack which is FiaB:

```
interface Vlan201
 ip address 20.20.21.1 255.255.255.252
!
```

4. Configure Layer 3 Port Channel between 9500 switches in Transit sites. On 9500-1:

```
interface TenGigabitEthernet1/0/1
no switchport
no ip address
channel-group 13 mode active
end
!
interface TenGigabitEthernet1/0/2
no switchport
no ip address
channel-group 13 mode active
end

!
interface Port-channel13
description Port Channel interface to C9500-R-2
no switchport
ip address 130.130.130.1 255.255.255.252
end
```

5. EIGRP routing configuration between fusion routers and Cisco Catalyst 9300 stack network devices to form neighbors:

```
router eigrp 2000
   network 120.120.120.0 0.0.0.3   # PoP Site C9300 Stack underlay network subnet
   network 120.120.122.0 0.0.0.3   # HQ/DC Site P2P underlay network subnet
   network 130.130.130.0 0.0.0.3   # Between C9500 switches in Transit Site
   network 192.0.130.11 0.0.0.0
   eigrp router-id 192.0.130.11
```

Example Interfaces Configuration on 9500-2 (Transit Site)

1. Loopback is configured on the device for Cisco DNA Center discovery:

```
interface Loopback0
ip address 192.0.130.12 255.255.255.255
!
```

2. Configure an interface on 9500-2 as a trunk to the Cisco Catalyst 9300 stack:

```
interface TenGigabitEthernet2/0/3
description Connected to C9300-20-STACK on port TE 2/1/1 switchport mode trunk
!
```

3. Configure an SVI interface (Example VLAN201) for underlay reachability between Fusion Router 2 and the Cisco Catalyst 9300 stack which is FiaB:

```
interface Vlan201
ip address 120.120.121.1 255.255.255.252
!
```

Configure Layer 3 Port Channel between C9500 switches in Transit sites. On C9500-2:

```
   interface TenGigabitEthernet1/0/1
    no switchport
    no ip address
    channel-group 13 mode active
   end
   !
   interface TenGigabitEthernet1/0/2
    no switchport
    no ip address
    channel-group 13 mode active
   end

!
interface Port-channel13
 description Port Channel interface to C9500-R-2
 no switchport
 ip address 130.130.130.2 255.255.255.252
end
```

4. EIGRP routing configuration between fusion routers and Cisco Catalyst 9300 stack network devices to form neighbors:

```
router eigrp 2000
    network 120.120.121.0 0.0.0.3     #PoP Site C9300 Stack underlay point-to-point network subnet
    network 120.120.123.0 0.0.0.3     #HQ/DC site underlay point-to-point network
    network 130.130.130.0 0.0.0.3     #Between C9500 switches underlay point-to-point network
    network 192.0.130.12 0.0.0.0
```

```
 eigrp router-id 192.0.130.12
```

Configure Layer 3 on Fabric-in-a-Box

An example Layer 3 routing configuration on the PoP site network device Cisco Catalyst 9300 stack or 9500 SVL to reach fusion routers and shared services network:

1. Loopback interface on the Cisco Catalyst 9300 stack for Cisco DNA Center discovery:

```
interface Loopback0
 ip address 192.0.20.11 255.255.255.255
!
```

2. Configure interfaces on the Cisco Catalyst 9300 stack as trunk ports to fusion routers:

```
interface TenGigabitEthernet1/1/1
 description Connected to 9500-1 Fusion Router on port TE 1/0/3
 switchport mode trunk
!
interface TenGigabitEthernet2/1/1
  description Connected to 9500-2 Fusion Router on port TE 2/0/3
  switchport mode trunk
!
```

3. Configure an SVI interfaces (example: VLAN200 and VLAN201) on the Cisco Catalyst 9300 stack to reach fusion routers:

```
interface Vlan200           #For reaching the Fusion router 9500-1
 ip address 20.20.20.2 255.255.255.252
!
interface Vlan201           #For reaching the Fusion router 9500-2
 ip address 20.20.21.2 255.255.255.252
```

4. Configure EIGRP neighbors between Cisco Catalyst 9300 Stack and Cisco Catalyst 9500 switches (fusion routers):

```
router eigrp 2000
 network 20.20.20.0 0.0.0.3
 network 20.20.21.0 0.0.0.3
 network 192.0.20.11 0.0.0.0
 eigrp router-id 192.0.20.11
```

Note: The above are the example configurations for the PoP1 site, as shown in Figure 3. The same has to be applied for all the PoP sites, including the HQ/DC site, to reach the shared services network so that devices can be successfully discovered in the Cisco DNA Center.

Configuring Shared Services Network Connectivity

For all the network devices in a PoP site and fusion routers to reach the shared services network, configure the basic underlay routing between the fusion routers and shared services network. Refer to Figure 3 for the physical topology between the fusion router, Nexus, and the shared services network.

1. A pair of Nexus 5672UP switches in the HQ/DC site connecting to application servers is used for connecting the Cisco DNA Center appliance and the Cisco UCS server where other shared services applications are hosted. The following configuration provides an example configuration (Layer 3) on the Nexus switches for configuring the shared services network to Cisco Catalyst 9500 switches as fusion routers, as shown in Figure 3.

   Nexus Switch-1 Configurations

   a. Configure an SVI interface (example: shared service VLAN1000) in Nexus-1 to reach the shared services network:

```
interface vlan 1000       # Vlan interface to reach Shared Services
```

```
 ip address 10.10.100.4 255.255.255.0
 no shut
!
```

b. Configure interface for connectivity to Cisco DNA Center appliance enterprise network interface:

```
interface Ethernet 1/6
 description Connected to Cisco DNA Center enterprise interface
 switchport mode trunk
 switchport trunk allowed vlan 1000
!
```

c. Configure interface for connectivity to CSR1KV:

```
interface Ethernet 1/22
 description Connected to CSR1KV on port TE1/0/6
 switch port mode trunk
 speed 1000
!
```

Nexus Switch-2 Configurations

a. Configure an SVI interface (VLAN1000) in Nexus-2 to reach the shared services network:

```
interface vlan 1000       # Vlan interface to reach Shared Services
 ip address 10.10.100.5 255.255.255.0
 no shut
!
```

b. Configure Nexus-2 interface for connectivity to the CSR1KV:

```
interface Ethernet 1/22
 description Connected to CSR1KV on port TE2/0/6
 switch port mode trunk
 speed 1000
!
```

2. Configure Cisco CSR1000V (fusion routers) to reach the shared services network.

a. For the shared services network (10.10.100.X), configure sub interfaces to reach Cisco DNA Center, DHCP, DNS, and ISE.

On Fusion Router 1:

```
interface GigabitEthernet2
 description Connected to Nexus5K-1 on Port Eth1/5
 no ip address
 negotiation auto
 cdp enable
 no mop enabled
 no mop sysid
end

!
interface GigabitEthernet2.1000
 encapsulation dot1Q 1000
 ip address 10.10.100.202 255.255.255.0
 ipv6 address 2001:DB8:16:110::120/64
 ipv6 enable
end
```

On Fusion Router 2:

```
interface GigabitEthernet2
 description Connected to Nexus5K-2 on Port Eth1/5
 no ip address
 negotiation auto
 cdp enable
 no mop enabled
 no mop sysid
end

!
interface GigabitEthernet2.1000
 encapsulation dot1Q 1000
 ip address 10.10.100.203 255.255.255.0
 ipv6 address 2001:DB8:16:110::121/64
 ipv6 enable
end
```

b. Cisco CSR1000v routers are configured as default routers for the shared services subnet with Next Hop Redundancy using the HSRP protocol. Configure HSRP to create gateway redundancy between the fusion routers for the shared services subnet. Example HSRP configuration on fusion routers:

On Fusion Router 1:

```
interface GigabitEthernet2.1000
standby version 2
standby 10 ip 10.10.100.201
standby 10 priority 105
standby 10 preempt delay minimum 120
!
```

On Fusion Router 2:

```
interface GigabitEthernet2.1000
standby version 2
standby 10 ip 10.10.100.201
standby 10 preempt delay minimum 120
!
```

3. Add the shared services network in the underlaying EIGRP routing configuration on both fusion routers, as shown in the example below.

```
router eigrp 2000
  network 10.10.100.0 0.0.0.255
```

Once the underlay routing configuration is complete for the Catalyst 9300 FiaB and fusion routers, the connectivity to the shared services (Cisco DNA, ISE, DHCP, WLC, Prime, etc.) network must be verified.

Transit Control Plane (C9500-1) IP Routing Verification:

```
C9500-30-CP1#show ip route eigrp
<Snip>


10.0.0.0/8is variably subnetted, 8 subnets, 2 masks
D 10.10.100.0/24[90/3328] via 120.120.122.2, 4d03h, Vlan300
[90/3072] via 120.120.120.2, 5w0d, Vlan200
D 10.10.201.0/24[90/3072] via 120.120.122.2, 6w1d, Vlan300

120.0.0.0/8is variably subnetted, 15 subnets, 2 masks
D 120.120.121.0/30[90/3072] via 130.130.130.2, 3w0d, Port-channel13
[90/3072] via 120.120.124.2, 3w0d, Vlan202
[90/3072] via 120.120.120.2, 3w0d, Vlan200
D 120.120.123.0/30[90/3072] via 130.130.130.2, 3w0d, Port-channel13
[90/3072] via 120.120.122.2, 3w0d, Vlan300
```

```
D 120.120.125.0/30[90/3072] via 130.130.130.2, 3w0d, Port-channel13
[90/3072] via 120.120.124.2, 3w0d, Vlan202
[90/3072] via 120.120.120.2, 3w0d, Vlan200
D 120.120.127.0/30[90/3072] via 130.130.130.2, 3w0d, Port-channel13
[90/3072] via 120.120.126.2, 3w0d, Vlan206
D 120.120.129.0/30[90/3072] via 130.130.130.2, 3w0d, Port-channel13
[90/3072] via 120.120.128.2, 3w0d, Vlan208
```

FiaB IP Routing Verification:

```
C9300-R-Stack#sh ip route
<snip>

[170/8192] via 120.120.121.1, 4d03h, Vlan201
[170/8192] via 120.120.120.1, 4d03h, Vlan200
10.0.0.0/8is variably subnetted, 9 subnets, 2 masks
[170/26906624] via 120.120.121.1, 1d22h, Vlan201
[170/26906624] via 120.120.120.1, 1d22h, Vlan200
D 10.10.100.0/24[90/3584] via 120.120.125.1, 4d03h, Vlan203
[90/3584] via 120.120.121.1, 4d03h, Vlan201
```

Ping Devices in Shared Services:

```
C9300-R-Stack#ping 10.10.100.201 #Fusion Router's Gateway Type escape sequence to abort.

Sending 5, 00-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

After successfully verifying the underlay connectivity from the Catalyst 9300 FiaB to the shared services, the edge fabric can start being provisioned.

Configuring Network Underlay for MPLS Backhaul Network

In addition to a Layer 3 enterprise network deployment, an edge fabric site can also be connected to the data center fabric site through an MPLS backhaul network. This network could be deployed by the city operator or a separate service provider. In either case, the fabric border device will act as a customer edge (CE) router and the connecting router in the MPLS core will act as the provider edge (PE) router. For this testing, a Layer 3 Virtual Private Network (L3VPN) was implemented. Explaining the differences in MPLS implementations is outside the scope of this document. This implementation is one of many ways a service provider can separate one customer's traffic from another.

Many ways exist for configuring a VRF-aware routing protocol between a PE and CE, but, in this implementation, eBGP was used. Cisco DNA Center only supports BGP as the routing protocol when a border node connects to an IP transit, which means the configuration can be combined with the underlay configuration. When the Catalyst 9300 is used in the role of the FiaB (Border + Control Plane + Edge), the connection to the PE must be done with an interface configured as a switchport trunk. An SVI is used for the Layer 3 configuration. For resiliency, another port on a different stack member can be connected to a different PE router.

Example Catalyst 9300 Configuration:

```
Interfaces:
    interface TenGigabitEthernet2/1/7
     switchport mode trunk
    !
    interface Vlan100
     ip address 10.1.1.9 255.255.255.248
```

```
!
interface Loopback0
 ip address 100.0.0.5 255.255.255.255
```

BGP Configuration:

```
router bgp 65002
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 10.1.1.14 remote-as 100
 !
 address-family ipv4
  bgp aggregate-timer 0
  network 100.0.0.5 mask 255.255.255.255
  neighbor 10.1.1.14 activate
 exit-address-family
 !
```

Example Provider Edge Configuration:

VRF Definition:

```
vrf definition cci-roadways
 rd 20:20
 !
 address-family ipv4
  route-target export 20:20
  route-target import 20:20
 exit-address-family
```

Physical Interface:

```
interface GigabitEthernet0/0/5
 service instance 20 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 21
```

Bridge Domain Interface:

```
interface BDI21
 vrf forwarding cci-roadways
 ip address 10.1.1.14 255.255.255.248
 ip mtu 9216
```

BGP Configuration:

```
router bgp 100
 address-family ipv4 vrf cci-roadways
    redistribute connected
    neighbor 10.1.1.9 remote-as 65002
    neighbor 10.1.1.9 activate
  exit-address-family
```

Note: Example VRF configuration is shown above for one VN. The configuration must be repeated if you add more VNs in the network.

Once the routing configuration is on the Catalyst 9300 FiaB and provider edge, connectivity to the shared services (Cisco DNA, ISE, DHCP, etc.) must be verified.

Provider Edge Verification:

```
X23-ASR920-6#sh ip bgp vpnv4 vrf cci-roadways summ
<snip>
```

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.2        4        65003     719     723      356    0    0 01:53:37        3
10.1.1.9        4        65002     772     793      356    0    0 02:02:04        3
```

FiaB Verification:

- Check Routing:

```
c9300-fabric2#sh ip bgp summ
<snip>
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.14       4          100     876     855      811    0    0 02:15:14       27
```

- Ping devices in shared services:

```
c9300-fabric2#ping 10.0.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

c9300-fabric2#ping 10.0.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

After successfully verifying the underlay connectivity from the Catalyst 9300 FiaB to the shared services, the edge fabric can start being provisioned.

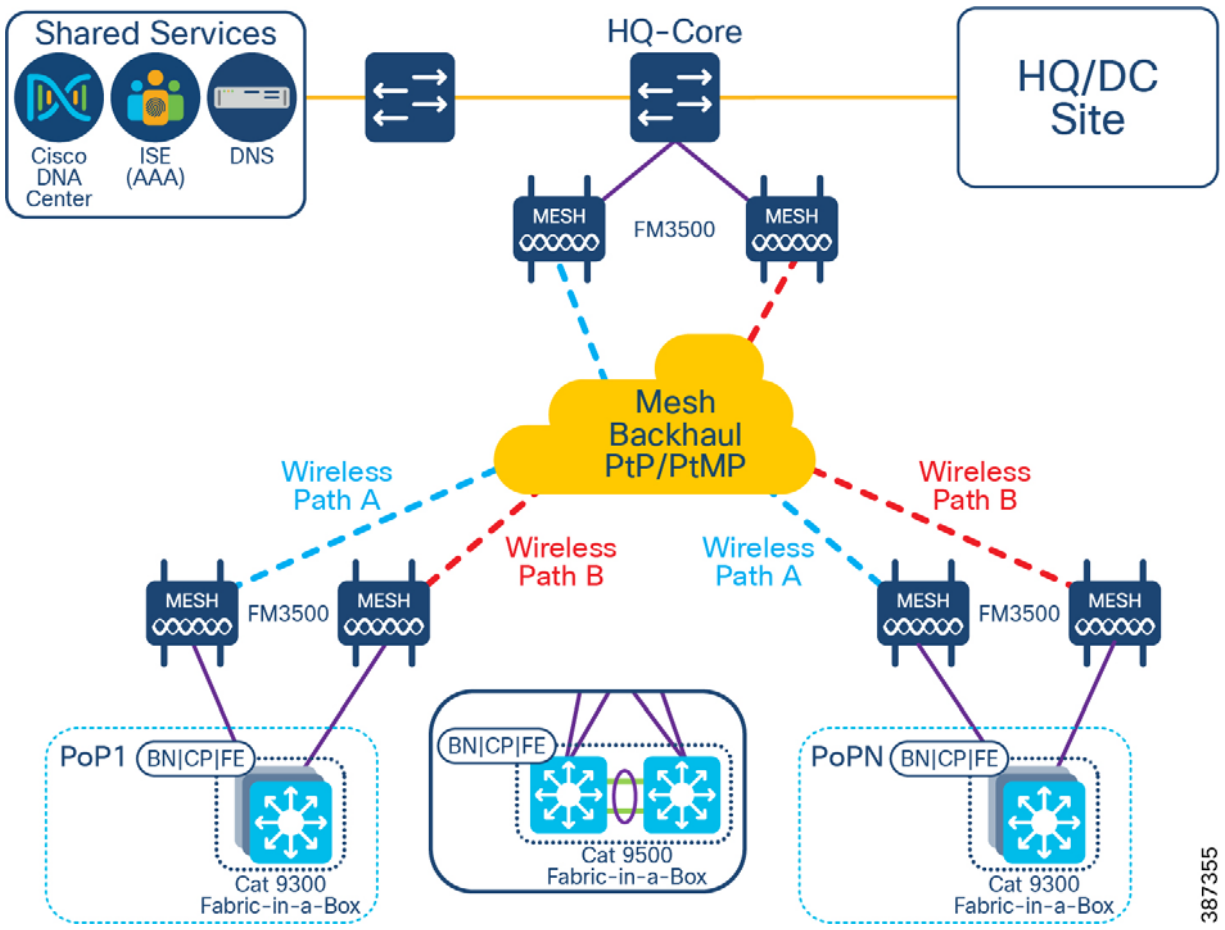
Cisco Ultra-Reliable Wireless Backhaul

Backhaul

When using Cisco Ultra-Reliable Wireless Backhaul (CURWB) in the backhaul to connect edge PoPs to the headquarters, it will takes on the role of underlay. Because the links act as invisible wires between the PoPs and the headquarters, they can be used as an SD Transit. However, because they are wireless devices, additional consideration and configuration is needed for deployment. The inherent challenges in an RF environment necessitate, a complete site survey is required before deploying the CURWB radios. Details of the site survey are outside the scope of this document. Using two different RF paths to provide higher throughput and resiliency for each PoP site is recommended. Configuring the radios prior to the physical installation is also recommended.

An example testbed is depicted below.

Figure 5 Multiple Wireless Backhaul Paths



In this deployment, two wireless paths are used to provide higher throughput and resiliency. Each PoP uses a routing protocol supporting Equal Cost Multipath (ECMP) which enables load balancing between the links. The effectiveness of the load balancing is dependent on the type of traffic and the load balancing algorithm chosen in the PoP border switch.

Plug-ins

Plug-ins are the licenses installed on the radios that enable specific features. The plug-ins needed to enable the fixed infrastructure will depend on the model chosen, the throughput needed, and whether the radios are in bridge mode or point-to -multipoint mode. The radios will also require the VLAN plug-in to enable the correct VLAN processing and AES to secure the wireless traffic. Enable MPLS fast failover is enabled by installing the TITAN plug-in.

CURWB Configuration

The radios can be configured in three different ways: 1) through RACER, 2) using the built-in web configuration tool, and 3) using the CLI. RACER and the CLI permit full configuration of all the options compared to the web configuration tool. RACER is the preferred tool for configuration because of the ability to manage all the CURWB radios' configurations in a single dashboard.

General and Wireless Settings

Each radio is configured to operate in a specific mode based on its role in the network. In this deployment, the radios at the headquarters are configured as Mesh Ends and the radios installed at the PoP sites are Mesh Points. The Mesh End radio is responsible for connecting the mesh network to the LAN connected backbone. Because the radios are configured as part of the network underlay, the management interface on all the Mesh Ends and Mesh Points must be configured in the same subnet. The configured passphrases must also match on the Mesh End and all its associated Mesh Points. This passphrase must be different from the other Mesh End and its Mesh Points, ensuring that the wireless networks are kept separate.

Figure 6 Mesh End Wireless Path A - General

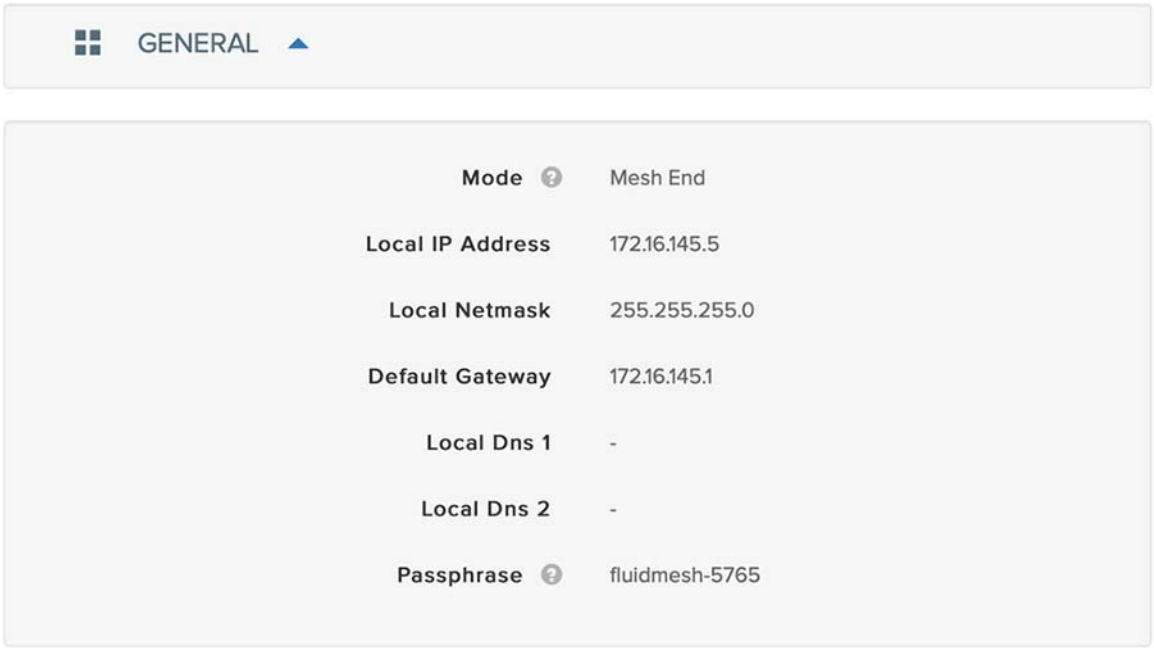


Figure 7 Mesh End Wireless Path B - General

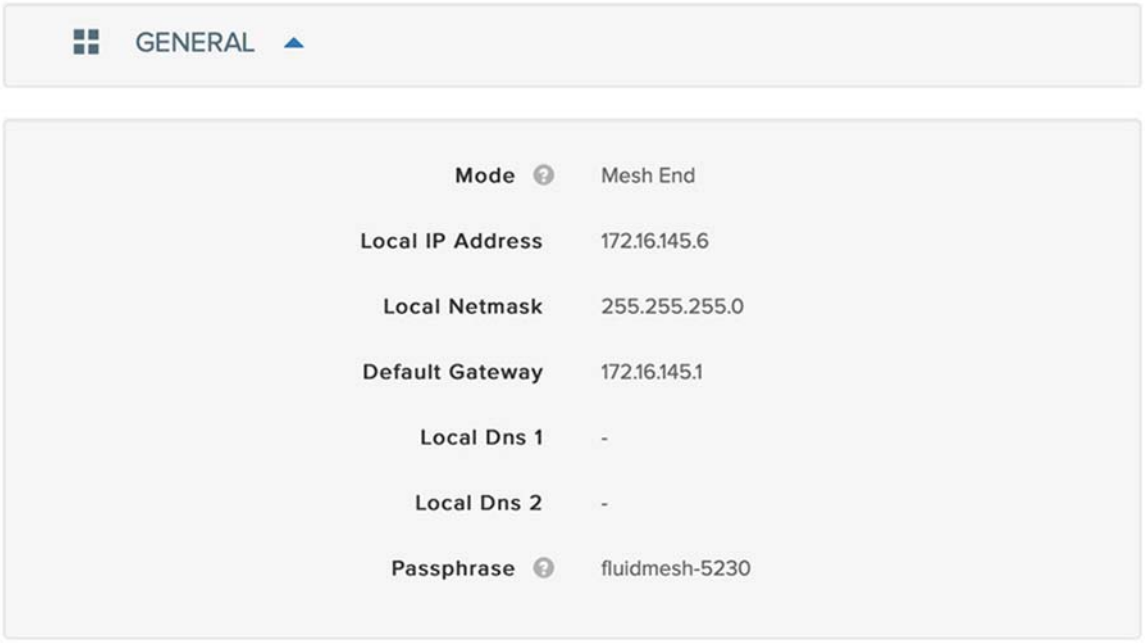


Figure 8 Mesh Point Wireless Path A – General

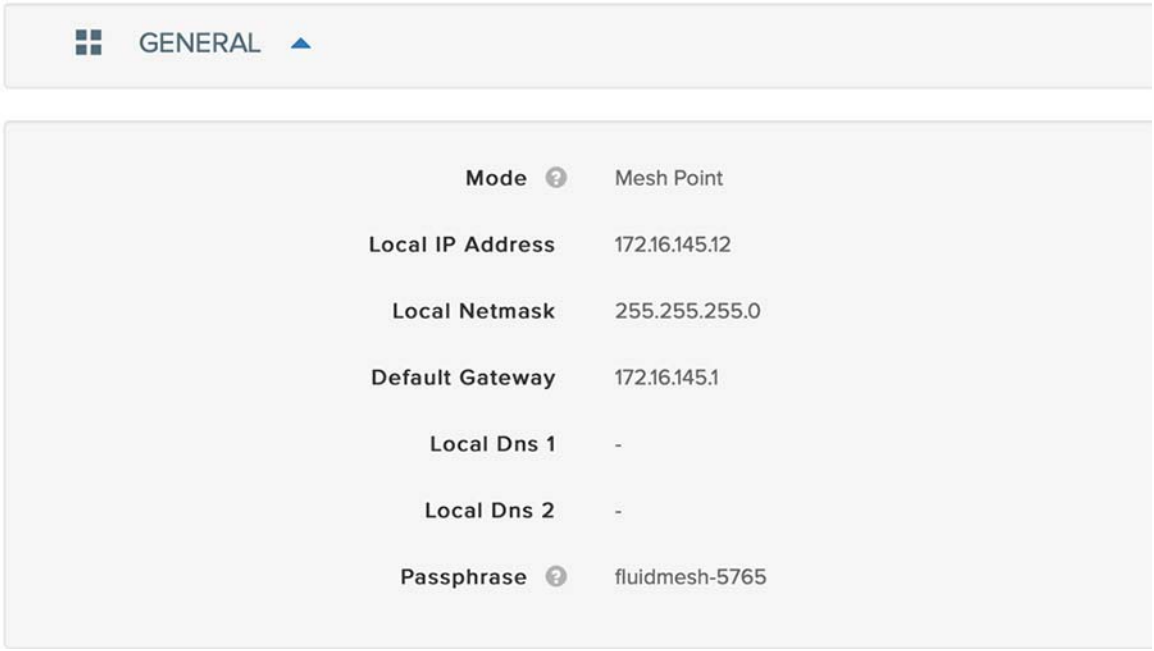
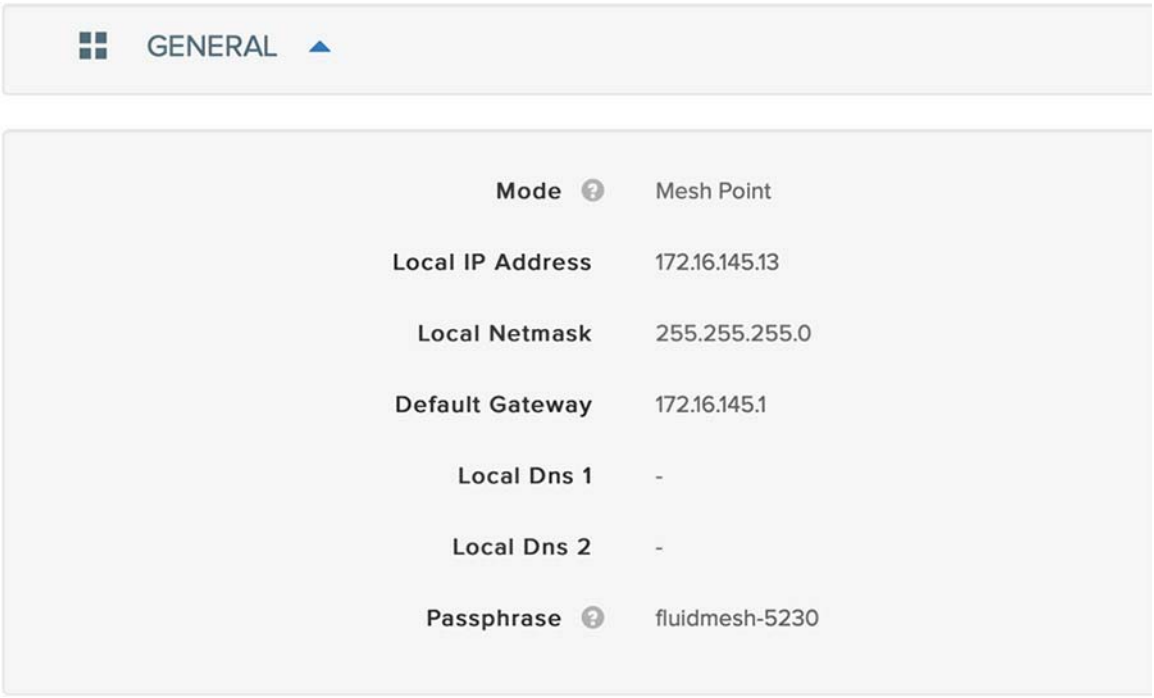


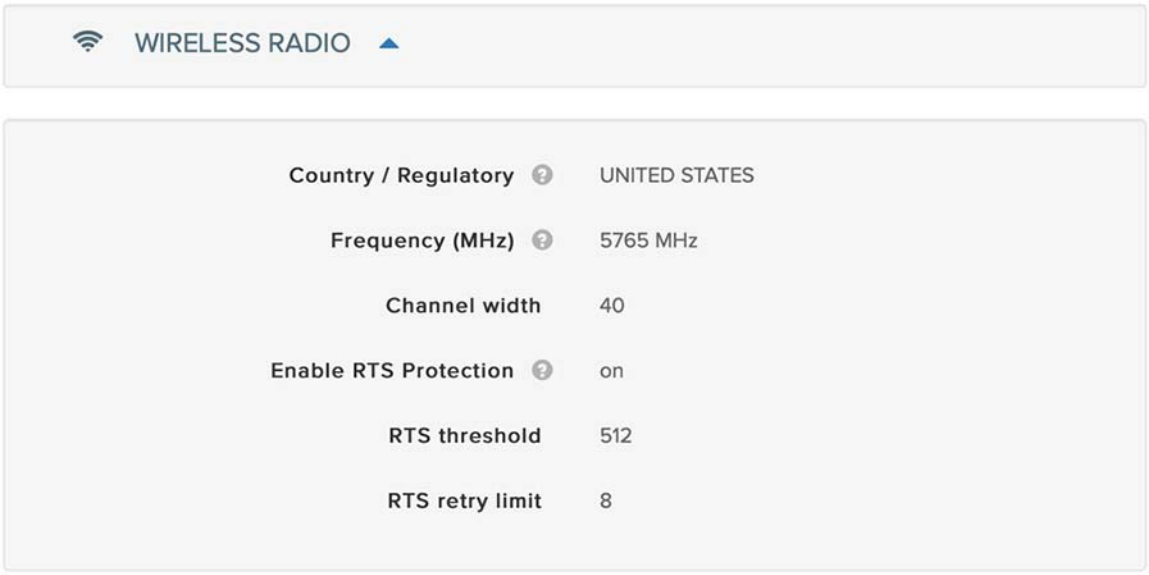
Figure 9 Mesh Point Wireless Path B – General



The wireless part of the radio is a separate configuration, and each path is configured on a separate non-overlapping frequency as determined by the site survey. Because the radios are operating in Point –to-Multipoint mode, there is the chance that Mesh Points could communicate at the same time causing a collision. The FM3200 can operate in Time

Division Multiple Access (TDMA) mode which increases efficiency in the communication by reducing collisions, but the FM3500 can only operate in Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mode. To reduce collisions, it is necessary to enable RTS/CTS on the FM3500 Mesh End radios.

Figure 10 Mesh End/Mesh Point – Wireless Radio



Because the Mesh Ends communicate with numerous PoP sites, they are also configured using FluidMAX. This allows the unit configured as “Master” (Mesh End in this case) to dictate the operating frequency to the radio units configured as “Slave” (Mesh Points).

Note: In the Advanced Radio Settings UI shown below, the Primary is called Master and the Secondary is called Slave. This feature cannot be configured in RACER for the FM3500, it can only be configured using the web Configurator, or the CLI.

Advanced Radio Settings

Figure 11 FluidMAX Primary/Master

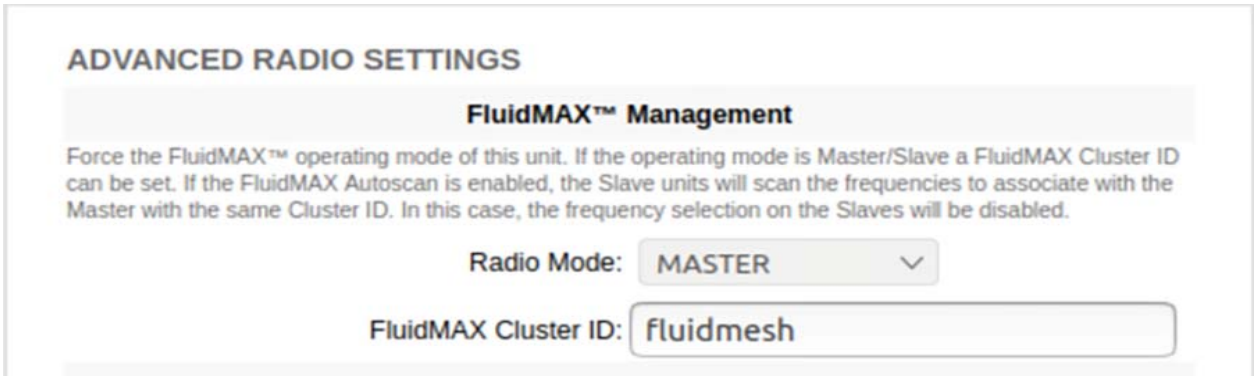
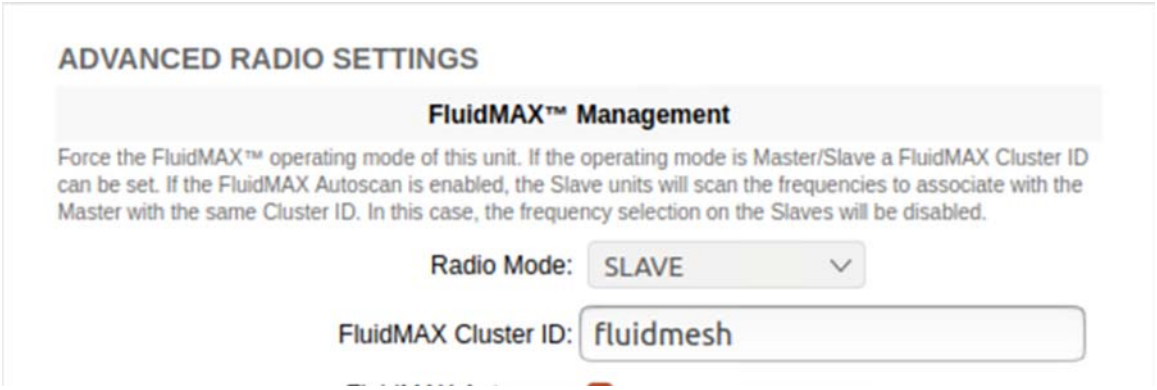


Figure 12 FluidMAX Secondary/Slave



Multicast

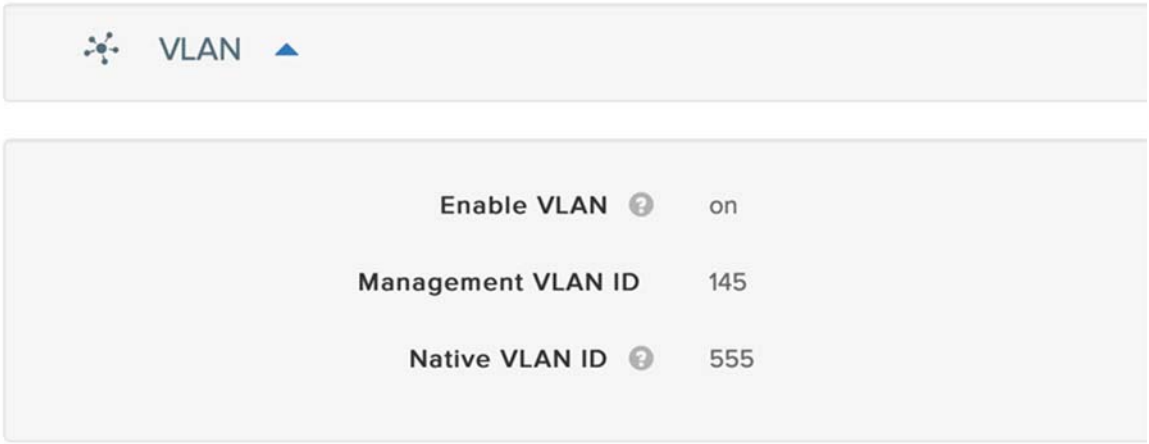
For this deployment, EIGRP was used as the underlay routing protocol which uses the well-known standard reserved multicast address 224.0.0.10. To forward these messages to the other radios, the Mesh Ends must be configured with multicast routes. The below configuration will send below sends the EIGRP update messages to all units in the mesh network.

Figure 13 Multicast

VLAN

Because the radios are all in the underlay network, the management VLAN can be configured as common across all the radios. The other configurable option for VLANs in the radio is the native VLAN. The native VLAN should must be configured the same on the Mesh End and Mesh Points while using the PoP border node to set the desired native VLAN. This ensures that any untagged packets coming into the wireless network do not inadvertently leave the radio with a VLAN tag. In the below examples below, VLAN 145 is used for management and VLAN 555 is used as the native VLAN. Note, VLAN 555 is not being used elsewhere in the network. Note that if the native VLAN is set to 0, any untagged traffic will be dropped.

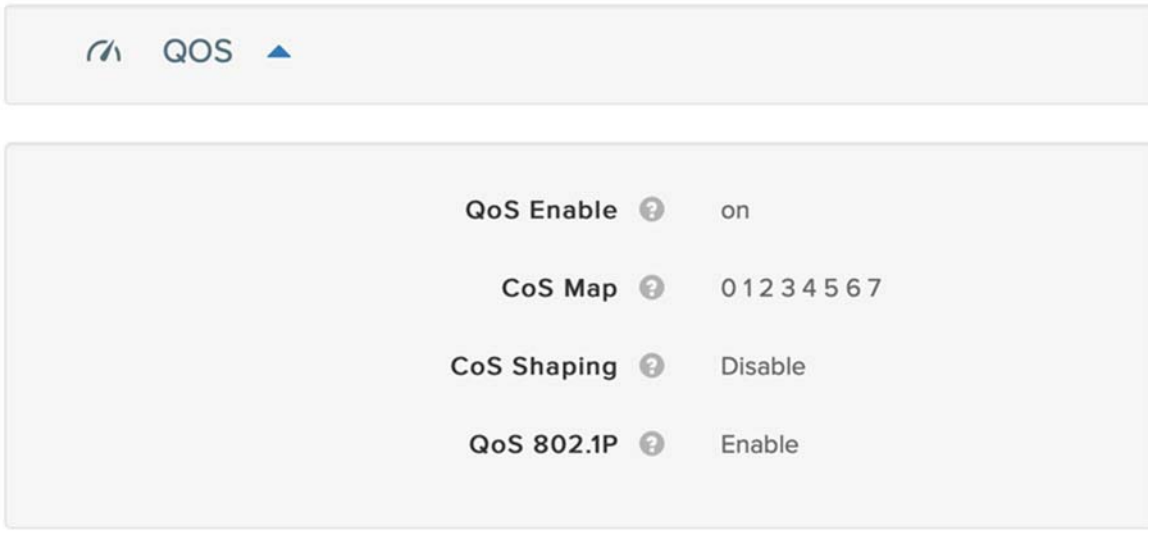
Figure 14 VLAN Configuration



QoS

QoS can only be enabled through the RACER configuration or CLI, not using the web Configurator. Enableing QoS on the radio and leaving the marking and queueing to the connected switch is recommended. Enable this configuration on all Mesh Ends and Mesh Points. When enabling 802.1P, the CURWB radio will inspects the COS value in the VLAN header as opposed to the DSCP value in the Layer 3 header.

Figure 15 QoS Configuration



Infrastructure Configuration

Headquarters

Using multiple parallel wireless paths will increases throughput and resiliency. Each radio network is therefore treated as a separate network path to a PoP site. In this deployment, wireless path A is assigned to VLAN 200 and wireless path B is assigned to VLAN 201. Each radio is connected to a trunk port that disallows the other PoP VLAN. The MTU is also configured for the maximum size that the radios can pass. The MTU is also required on the SVI because EIGRP sends updates up to the maximum size allowed on the link. VLAN 145 is included to enable management of the radios.

Wireless Path A

```
interface TenGigabitEthernet1/0/3
 description connected to FM-3500 5.1.29.7
 switchport trunk allowed vlan 1,145,200
 switchport mode trunk
 mtu 2044
```

Wireless Path B

```
interface TenGigabitEthernet1/0/4
 description connected FM-3500 5.0.156.233
 switchport trunk allowed vlan 1,145,201
 switchport mode trunk
 mtu 2044
```

Each VLAN has an associated SVI for Layer3 reachability.

```
interface Vlan145
 ip address 172.16.145.1 255.255.255.0
interface Vlan200
 ip address 10.5.1.1 255.255.255.0
 ip mtu 2044
interface Vlan201
```

```
 ip address 10.5.2.1 255.255.255.0
 ip mtu 2044
```

VLAN 200 and 201 are added to EIGRP to form neighbors with the other PoP sites connected wirelessly.

```
router eigrp 20
 network 10.5.1.0 0.0.0.255
 network 10.5.2.0 0.0.0.255
```

PoP Site

At each PoP site, the VLAN for each wireless path must be configured. For sites with dual paths, this is VLAN 200 and 201. The interfaces facing the radio must also be set as trunks. When using the 9x00 as the border node, the MTU can be configured system wide for 2044.

```
system mtu 2044
PoP Interface Configuration
interface TenGigabitEthernet1/0/23
 switchport mode trunk
interface TenGigabitEthernet1/0/24
 switchport mode trunk
interface Vlan200
 ip address 10.5.1.5 255.255.255.0
interface Vlan201
 ip address 10.5.2.5 255.255.255.0
```

Cisco DNA-C also requires a loopback for onboarding and management.

```
interface Loopback0
 ip address 100.0.0.9 255.255.255.255
```

The underlay subnets are then added to the EIGRP process.

```
router eigrp 20
 network 10.5.1.0 0.0.0.255
 network 10.5.2.0 0.0.0.255
 network 100.0.0.9 0.0.0.0
```

Looking at the EIGRP neighbors will confirms the underlay is functioning correctly.

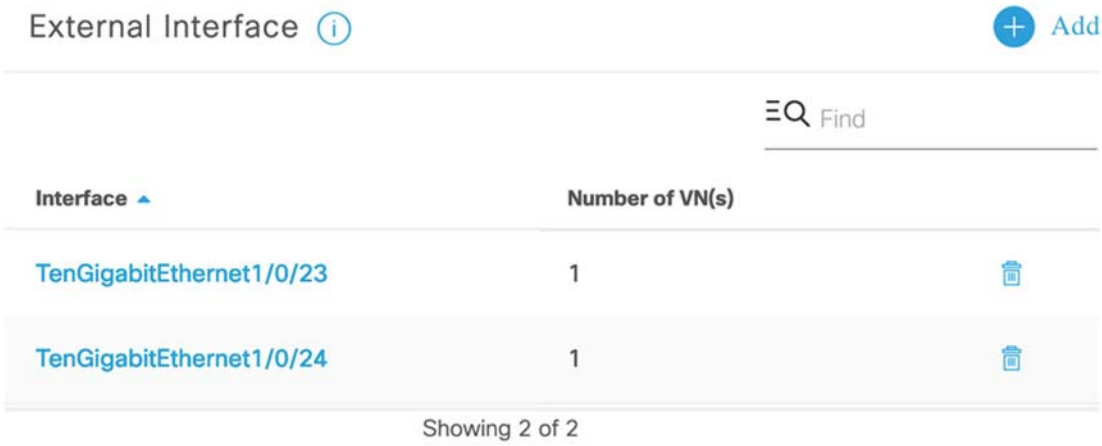
```
EIGRP-IPv4 Neighbors for AS(20)
H   Address                 Interface              Hold   Uptime     SRTT   RTO     Q     Seq
                                                          (sec)                     (ms)
Cnt    Num
4   10.5.1.1                Vl200                    12      02:46:59    1       100       0
1760951
5   10.5.2.1                Vl201                    11      03:18:41    1       100       0
1760950
```

After the underlay network is functional and all required configuration for discovery is in place, the Discovery workflow can be used to onboard the device.

Cisco DNA-C Configuration

Onboarding and provisioning the newly-discovered switch is the same process as a wired switch and requires no special configuration to support the CURWB connection. After provisioned to the fabric site, the border interfaces must be configured if an IP Transit is used. Each interface facing the CURWB radio is used as the External Interface.

Figure 16 Border External Interfaces



Because the PoP switch is connected to the headquarters through Layer2, each VLAN configured for a VN must be unique at the headquarters site.

Figure 17 Border Interface-1 VN Configuration

Figure 18 Border Interface-2 VN Configuration

Through the use of multiple interfaces, the routing protocol can be configured for fast failover and load balancing. Bidirectional Failure Detection (BFD) is configured on the interfaces and within the BGP instance for the VRF associated with the VN. Load balancing is achieved using the maximum-paths command. The routing protocol is dependent on having multiple interfaces to achieve these additions.

Edge PoP External SVI:

```
interface Vlan3020
 description vrf interface to External router
 vrf forwarding Transportation
 ip address 172.16.18.5 255.255.255.252
 no ip redirects
 ip route-cache same-interface
 bfd interval 100 min_rx 100 multiplier 3                    <<<<<<< Enable BFD
interface Vlan3021
 description vrf interface to External router
 vrf forwarding Transportation
 ip address 172.16.18.13 255.255.255.252
 no ip redirects
```

```
 ip route-cache same-interface
 bfd interval 100 min_rx 100 multiplier 3                                    <<<<<<< Enable BFD
```

Edge PoP BGP Address Family

```
router bgp 6006
 address-family ipv4 vrf Transportation
  bgp aggregate-timer 0
  network 172.16.17.16 mask 255.255.255.248
  network 172.16.18.4 mask 255.255.255.252
  network 172.16.18.12 mask 255.255.255.252
  aggregate-address 172.16.17.16 255.255.255.248 summary-only
  redistribute lisp metric 10
  neighbor 172.16.18.6 remote-as 65001
  neighbor 172.16.18.6 update-source Vlan3020
  neighbor 172.16.18.6 fall-over bfd                                          <<<<<<< Enable BFD
  neighbor 172.16.18.6 activate
  neighbor 172.16.18.6 weight 65535
  neighbor 172.16.18.14 remote-as 65001
  neighbor 172.16.18.14 update-source Vlan3021
  neighbor 172.16.18.14 fall-over bfd                                       <<<<<<< Enable BFD
  neighbor 172.16.18.14 activate
  neighbor 172.16.18.14 weight 65535
  maximum-paths 2                                                                    <<<<<<<
Install multiple routes in routing table
```

BFD Neighbor table

```
show bfd neighbors
IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
172.16.18.6                             2/2          Up        Up        Vl3020
172.16.18.14                            4/3          Up        Up        Vl3021
```

IP Routing table with multiple paths

```
show ip route vrf Transportation
      10.0.0.0/24 is subnetted, 2 subnets
B        10.0.1.0 [20/0] via 172.16.18.14, 00:03:01
                  [20/0] via 172.16.18.6, 00:03:01
B        10.5.1.0 [20/0] via 172.16.18.14, 00:03:01
                  [20/0] via 172.16.18.6, 00:03:01
```

The headquarters core switch needs the complementary configuration on the interfaces and BGP address family configuration. Upon completion, multiple paths will be available for traffic between the Edge PoP and headquarterss which can be used for load balancing and failover.

Implementation of CCI Shared Services

This section covers the implementation of services common to all fabric sites (PoPs) in CCI network, also called shared services. Shared services like Cisco DNA Center, ISE, Centralized Wireless LAN Controller (WLC), DHCP, and DNS, along with other CCI vertical-specific applications such as FND and Fog Director, must be reachable from each fabric/PoP site underlay network and overlay VN provisioned using the Cisco DNA Center.

This section includes the following major topics:

Cisco DNA Center Installation and Initial Configuration

Cisco DNA Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center provides a centralized management dashboard for complete control of the CCI horizontal network.

Cisco DNA Center, which is a dedicated hardware appliance powered through a software collection of applications, processes, services, packages, and tools, is the centerpiece for Cisco® Digital Network Architecture (Cisco DNA™). This software provides full automation capabilities for provisioning and change management, reducing operations by minimizing the touch time required to maintain the network.

This section covers the installation and basic network configuration needed on the Cisco DNA Center for accessing its GUI in CCI deployment.

For step-by-step instructions for installing and configuring Cisco DNA Center, refer to the *Cisco DNA Center Installation Guide, Release 2.2.3* at the following URLs:

Cisco DNA Center First Generation Appliance Installation Guide

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/install_guide/1stgen/b_cisco_dna_center_install_guide_2_2_3_1stGen.html

Cisco DNA Center Second Generation Appliance Installation Guide

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_3_2ndGen.html

Preparing Cisco Identity Service Engine for SD-Access

Cisco Identity Services Engine (ISE) is a policy-based access control system that enables the enterprises, Smart Cities, and the like to enforce compliance and infrastructure security. ISE is an integral part of Cisco SD-Access acting as the authentication, authorization, and accounting (AAA) server for devices identity management, access control, and enforcement of access policies on fabric devices.

In the CCI solution, ISE is coupled with the Cisco DNA Center for dynamic mapping of users and devices to scalable groups, which simplifies end-to-end security policy management and enforcement at a greater scale than traditional network policy implementations relying on IP access lists.

ISE Installation and Initial Configuration

A centralized standalone deployment of ISE is configured with the Cisco DNA Center in the shared services network as shown in the network topology that is depicted in Figure 3. ISE can be installed in various ways; OVA deployment of ISE as a virtual machine is used in this implementation. Refer to the URL below for step-by-step instructions on installing ISE:

For ISE v2.4:

- https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/install_guide/b_ise_InstallationGuide24/b_ise_InstallationGuide24_chapter_011.html

If you prefer to deploy the latest compatible version of ISE, refer the following URL for ISE v3.0 Installation:

- https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install_guide/b_ise_InstallationGuide30/b_ise_InstallationGuide30_chapter_3.html

Once the ISE installation is complete, update the Patch 13 on ISE v2.4, which is compatible with Cisco DNA Center SD-Access, by completing the following steps:

1. Download the ISE patch bundle ise-patchbundle-2.4.0.357-Patch13-20080314.SPA.x86_64.tar.gz.

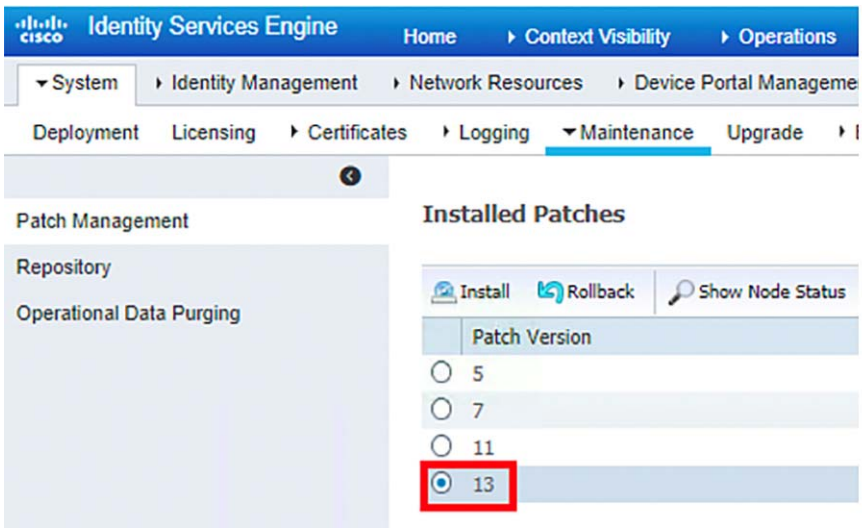
   Note: Software downloads from Cisco website requires a registered Cisco Account and Cisco software download access.

2. Log in to the ISE GUI and navigate to **Administration-> Maintenance-> Patch Management**.

3. Click **Install**, upload the patch file, and then click **Install** again. The installation will take about 1 hour and during the time ISE will not be available.

4. To verify the patch is installed successfully, check **Patch Management** in to see whether the Patch 13 is listed, as shown in Figure 19.

Figure 19 Cisco ISE Patch Installation View



This completes the installation and relevant patch upgrade of ISE compatible with Cisco DNA Center Release 2.3.2.

Note: Refer to the *Cisco SD-Access 2.3.2.x Hardware and Software Compatibility Matrix* at the following URL for more details: https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/sda_compatibility_matrix/index.html

Integrating ISE with Cisco DNA Center

Once ISE installation and basic configuration is complete, it has to be integrated with the Cisco DNA Center. Refer to the section Integrate Cisco ISE with Cisco DNA Center in the *Cisco DNA Center Installation Guide Release 2.2.3* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_3_2ndGen/m_complete_first_time_setup_2_2_3_2ndgen.html#task_ikj_pg3_sfb

Note: Before integrating ISE with the Cisco DNA Center, ensure that PxGrid services are online on ISE and that the cluster node is up in Cisco DNA Center.

Once integrated with Cisco DNA Center using PxGrid, information sharing between the two platforms is enabled, including device information and group information. This allows the Cisco DNA Center to define policies that are pushed to ISE and then rendered into the network infrastructure by the ISE Policy Service Nodes (PSNs). When integrating the two platforms, a trust is established through mutual certificate authentication. This authentication is completed seamlessly in the background during integration and requires both platforms to have accurate NTP time synchronization.

Configuring DHCP and DNS Services

DHCP Server

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol (DHCP) to respond to broadcast queries by clients.

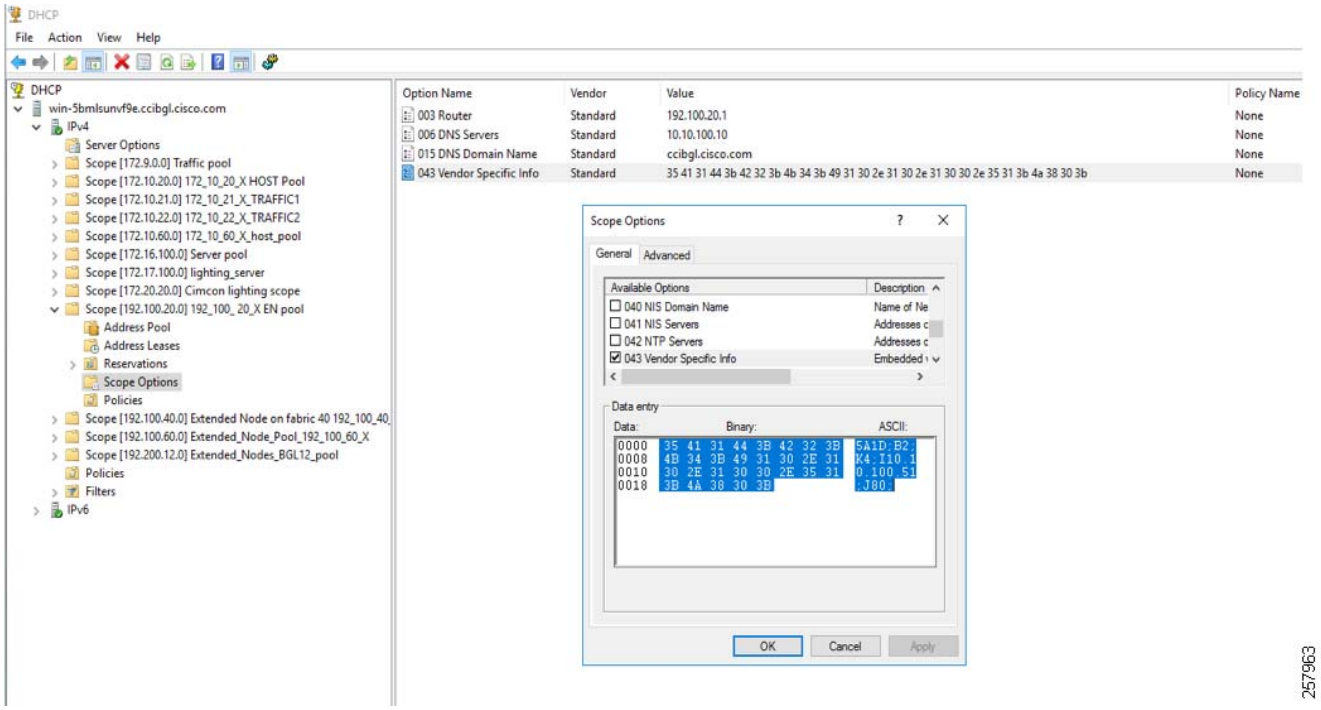
DHCP services can be configured in the network in many ways. In this implementation, a centralized DHCP services in the CCI network shared services, running on a Windows 2016 server is used. This section covers the example DHCP scope and IP pools definition and discusses other scope options that are required for implementing SD-Access in the CCI network.

Refer to the step-by-step instructions on *Microsoft Windows Server 2016: DHCP Server Installation & Configuration* at the following URL:

- https://social.technet.microsoft.com/wiki/contents/articles/51170.microsoft-windows-server-2016-dhcp-server-installation-configuration.aspx

After the DHCP server is successfully configured on a Windows 2016 server, create Scopes for all the IP pools configured on the Cisco DNA Center with options 43 (example pools are for extended node and host node pools) in the DHCP server, as shown in Figure 20:

Figure 20 Example IP Scope and Scope Options in CCI Network



For more information on DHCP option 43, refer to the section DHCP Controller Discovery in the *Cisco Digital Network Architecture Center User Guide, Release 2.2.3* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01101.html?bookSearch=true#id_90877

Domain Name Server

In this implementation, Domain Name Servers (DNS) in the CCI network shared services, running on a Windows 2016 server (co-located on the DHCP server), are used.

Refer to the following URL for step-by-step instructions and configuration of the DNS on the Windows 2016 server for the CCI network:

- https://www.microsoftpressstore.com/articles/article.aspx?p=2756482

Implementing Field Network Director for CCI

Cisco Field Network Director (FND) is an essential component for IoT solution deployments. FND in CCI provides easier deployment and management of devices such as Field Area Routers (CGR), Connected Grid End Points (CGEs) and IC3000 Industrial Compute Gateway. FND is the critical component of the FAN solution. FND is the one component that interacts with most of the components in the FAN solution.

For information about installing/configuring FND, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/install/oracle/iot_fnd_oracle/installation_rpm_new_oracle.html

Note: FND with the Oracle database, which is used in this implementation, is needed for CGR mesh support.

Prerequisites for FND Installation

- In the CCI network, FND OVA (this OVA includes Oracle for mesh management (CGR, IR5x)), can be downloaded from the following link:
  - https://software.cisco.com/download/home/286287993/type/286320249/release/4.5.1

  Note: -v containing image should be used for mesh deployment.

  Note: After download, use the **iot-fnd-oracle-4.4.0-79.ova** file to install the FND Application.
- FND is installed in the shared services network in CCI so that it can be accessible by FAR and other headend components. The installation steps can be found at the following link (refer to section "Prerequisites, Installing the OVA").
  - https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/install/ova/installation-ova-fnd-4-3-1.html#pgfId-1544292
- RHEL needs an active account with access to subscription management, needed for performing yum updates, yum install, and so on. Addressing these prerequisites is beyond the scope of this document. Please refer to Red Hat documentation.
- IP address configuration on a couple of interfaces:
  - a) One interface configured with the IP Address of the FND:
    - The interface must be configured with an IPv4 address and an IPv6 address.
  - b) Another temporary interface providing Internet connectivity.

Implementation of FND

- The section "Implementing Field Network Director" in the FND implementation guide has detailed implementation information (you can skip the sections "Integrating FND with TPS Proxy" and "Integrating FND with FND-DB") at the following URL:
  - https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872
- After successful implementation, you should check the status of FND in the CLI:

```
[root@iot-fnd-oracle conf]# service cgms status
IoT-FND Version 4.5.1-11
04-09-2020 18:45:46 PDT: INFO: IoT-FND database server: localhost
04-09-2020 18:45:46 PDT: INFO: IoT-FND database connection verified.
04-09-2020 18:45:47 PDT: INFO: IoT-FND application server is up and running.
04-09-2020 18:45:48 PDT: INFO: IoT-FND is up and running.
```

Implementation of Cisco IC3000 Industrial Compute Gateway

In CCI, the IC3000 Industrial Compute Gateway connected to the edge switch via the management port learns about the FND via the DHCP server through option 43 and connects to the FND. Registration succeeds assuming the CSV file is uploaded to the FND and connectivity exists between the FND and the IC3000 Industrial Compute Gateway. As part of registration, FND enables the data ports for data traffic if enabled from the IC3000 Industrial Compute Gateway template under the FND.

For information about managing/deploying IC3000 Industrial Compute Gateway, refer to the *Cisco IC3000 Industrial Compute Gateway Deployment Guide* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/DeploymentGuide.html

Implementing Centralized Wireless LAN Controller for Cisco Unified Wireless Network

In CCI, Cisco Catalyst 9800 Series Wireless Controller (C9800-40) is configured as a Centralized Wireless LAN Controller (WLC) with High Availability (HA) for managing Cisco Unified Wireless Network (CUWN) with Wi-Fi mesh deployments in PoPs. Refer to the "Cisco Unified Wireless Network (CUWN) with Mesh" section in the Connected Communities Infrastructure Design Guide at the following URL for more details on the design:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

This section covers the initial installation and HA configuration of C9800-40 WLC in CCI Shared Services network. This section applies to you if you are doing CUWN wireless and deploying WLC centrally in Shared Services.

Cisco WLC (C9800-40) Installation and Initial Configuration

The Cisco Catalyst 9800-40 Wireless Controller is a 40-G wireless controller that offers a compact form factor that consumes less rack space and power while offering 40 Gbps forwarding throughput. This section covers the installation and Day-0 Configuration required to setup the C9800 WLC.

Refer to the following URL for rack mounting and installing the C9800-40 hardware:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/installing-the-controller.html

Once the WLC is rack mounted, verify the following:

1. The network interface cable or the optional Management port cable is connected.
2. The chassis is securely mounted and grounded.
3. The power and interface cables are connected
4. Terminal server is connected to the console port.

There are two modes in which a IOS XE software image on a Catalyst 9800 WLC can run: Install mode and Bundle mode.

Install Mode

The install mode uses pre-extracted files from the binary file into the flash in order to boot the controller. The controller uses the 'packages.conf' file that was created during the extraction as boot variable.

Bundle Mode

The system works in bundle mode if the controller boots with the binary image (.bin) as boot variable. In this mode the controller extracts the .bin file into the RAM and runs from there. This mode uses more memory than install mode since the packages extracted during boot up are copied to the RAM.

Note: Install mode is the recommended mode to run the wireless controller.

Boot the Controller in Install Mode:

Step 1: Make sure to boot from flash:packages.conf (and we do not have other boot files specified in our configuration).

```
WLC(config)#no boot system
WLC(conf)#boot system flash:packages.conf
```

Step 2: Install software image to flash. The install add file bootflash:<image.bin> activate commit command moves the switch from bundle-mode to install-mode where image.bin is our base image.

```
WLC#install add file <image.bin location> activate commit
```

Step 3: Type **yes** to all the prompts. Once the installation is completed the controller proceeds to reload.

Step 4: After the controller bootup, you can verify the current installation mode of the controller. Run the **show version** command to confirm the mode.

```
WLC#show version | include System image
System image file is "bootflash:packages.conf"

WLC#show version | include Installation mode
Installation mode is INSTALL
```

For more details on WLC power up and initial configuration, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/power-up-and-initial-configuration.html

Day-0 Manual Configuration Using the Cisco IOS-XE CLI:

C9800-40 WLC is connected to shared services network with 10G link. The steps to access WLC CLI to perform the initial configuration on the controller are provided below.

Step 1: Terminate the configuration wizard (this wizard is not specific for wireless controller):

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

Step 2: Press **Return** and continue with the manual configuration.

Step 3: Press **Return** to bring up the WLC> prompt and Type enable to enter privileged EXEC mode.

```
WLC> enable
WLC#
```

Step 4: Enter the config mode and set the hostname:

```
WLC(config)#hostname WLC_C9800-40_1
```

Step 5: Configure login credentials:

```
WLC_C9800-40_1(config)#username <name> privilege 15 password 0 <pwd>
WLC_C9800-40_1(config)#enable secret <secret>
```

Step 6: Configure the VLAN for wireless management interface and shared services VLAN in CCI network.

```
WLC_C9800-40_1(config)#vlan 1000
WLC_C9800-40_1(config-vlan)#name WirelessVLAN
```

Step 7: Configure the SVI for wireless management interface.

```
WLC_C9800-40_1(config)#interface Vlan1000
WLC_C9800-40_1(config-if)#ip address x.x.x.x 255.255.255.0
WLC_C9800-40_1(config-if)#no shutdown
WLC_C9800-40_1(config-if)#exit
```

Step 8: Configure the interface TenGigabitEthernet0/0/1 as trunk:

```
WLC_C9800-40_1(config)#interface TenGigabitEthernet0/0/1
WLC_C9800-40_1(config-if)#switchport mode trunk
WLC_C9800-40_1(config-if)#switchport trunk allowed vlan 1000
WLC_C9800-40_1(config-if)#exit
```

Step 9: Configure a default route (or a more specific route) to reach the box:

```
WLC_C9800-40_1(config)#ip route 0.0.0.0 0.0.0.0 x.x.x.x
```

Step 10: Disable the wireless network to configure the country code:

```
WLC_C9800-40_1(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
WLC_C9800-40_1(config)#ap dot11 24ghz shutdown
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
```

Step 11: Configure the AP country domain. This configuration is what will trigger the GUI to skip the DAY 0 flow as the C9800 needs a country code to be operational:

```
WLC_C9800-40_1(config)#ap country IN
```

Step 12: Specify the interface to be the wireless management interface:

```
WLC_C9800-40_1(config)# wireless management interface vlan 1000
```

Step 13: For the Controller to be discovered by the Cisco DNA Center or Prime Infrastructure, CLI, SSH and SNMP credentials should be configured on the devices along with NETCONF:

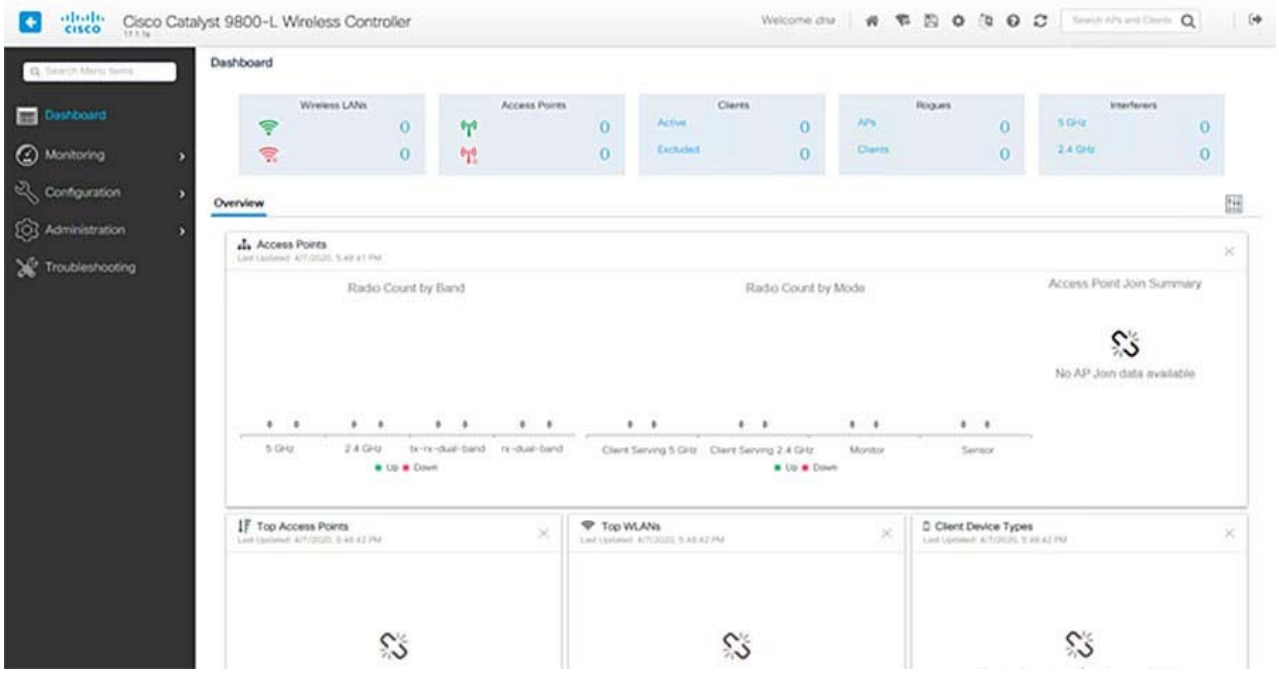
```
WLC_C9800-40_1(config)# crypto key generate rsa modulus 2048
WLC_C9800-40_1(config)# ip ssh version 2
WLC_C9800-40_1(config)# line vty 0 15
WLC_C9800-40_1(config-line)# login local
WLC_C9800-40_1(config-line)# transport input all
WLC_C9800-40_1(config-line)# transport preferred ssh

WLC_C9800-40_1(config)# snmp-server group default v3 priv
WLC_C9800-40_1(config)# snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
WLC_C9800-40_1(config)# snmp-server view SNMPv3All iso included
WLC_C9800-40_1(config)# snmp-server view SNMPv3None iso excluded
WLC_C9800-40_1(config)# snmp-server community <CommunityString> RW
WLC_C9800-40_1(config)# snmp-server user <username> default v3 auth md5 <password> priv aes 128
<password>

WLC_C9800-40_1(config)#ntp server x.x.x.x
WLC_C9800-L_1(config)#ip http server

WLC_C9800-40_1(config)#netconf-yang
```

Verify that you can ping the wireless management interface and then just https://<IP of the device wireless management interface>. Use the credentials you have entered earlier. Since the box has a country code configured, the GUI will skip DAY 0 page and you will get access to the main Dashboard for DAY 1 configuration.

Accessing C9800-40 WebUI:

Access the C9800 Web UI using https://<IP_addr_of_C9800-40-WLC>. The username and password configured during the Day-0 configuration of WLC must be used to log on to WLC Web UI. Figure 21 shows C9800-40 WLC Web UI dashboard view after successful login.

Figure 21 Cisco 9800-L WLC Web UI Dashboard View



Cisco WLC (C9800-40) High Availability Configuration

High availability (HA) has been a requirement on wireless controllers to minimize downtime in live networks. This section provides information on the theory of operation and configuration for the Catalyst 9800 Wireless Controller as it pertains to supporting stateful switchover of access points and clients (AP and Client SSO).

The redundancy explained on this document is 1:1, which means that one of the boxes will be in Active State while the other one will be in Hot Standby. If the active box is detected to be unreachable, the Hot Standby unit will become Active and all the APs and clients will keep its service through the new active box.

Once both boxes are synchronized with each other, the standby 9800 WLC will mimic its configuration with the primary box. Any configuration change is done on the active unit will be replicated to the standby unit via the Redundancy Port (RP). Configuration changes are no longer allowed to be performed on the standby 9800 WLC.

Besides the synchronization of the configuration between boxes, they also synchronize the APs in UP state (not APs in downloading state or APs in DTLS handshaking), clients in RUN state (this means that if there is a client in Web Authentication required state and a switchover occurs, that client will have to restart its association process), RRM configuration along other settings.

For more details on deployment and configuration, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_vewlc_high_availability.html

High Availability Prerequisites:

- HA Pair can only be form between two wireless controllers of the same form factor
- Both controllers must be running the same software version in order to form the HA Pair
- Maximum RP link latency = 80ms RTT, minimum bandwidth = 60 Mbps and minimum MTU = 1500

Configure HA on 9800 WLC Hardware:

C9800-40-K9 Wireless controller has two RP Ports as shown in Figure 22.

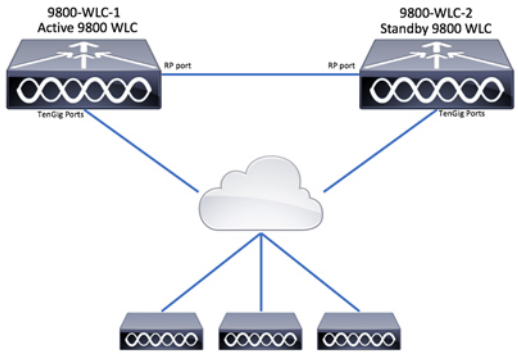
Figure 22 C9800-40 WLC Front View

In Figure 22:

1. RJ-45 Ethernet Redundancy port
2. SFP Gigabit Redundancy port

The HA Pair always has one active controller and one standby controller. If the active controller becomes unavailable, the standby assumes the role of the active. The Active wireless controller creates and updates all the wireless information and constantly synchronizes that information with the standby controller. If the active wireless controller fails, the standby wireless controller assumes the role of the active wireless controller and continues to the keep the HA Pair operational. Access Points and clients continue to remain connected during an active-to-standby switchover.

Figure 23 C9800-40 WLC High Availability Network Topology



Redundancy SSO is enabled by default, but you still need to configure the communication between the boxes. Follow the step-by-step instructions below for deploying WLC in HA.

Step 1: Make sure both the C9800 WLCs are reachable to each other. Wireless management interface from both boxes must belong to the same VLAN and subnet (in our case connected to Nexus 5000).

Step 2: Connect both 9800 WLC to each other through its RP port.

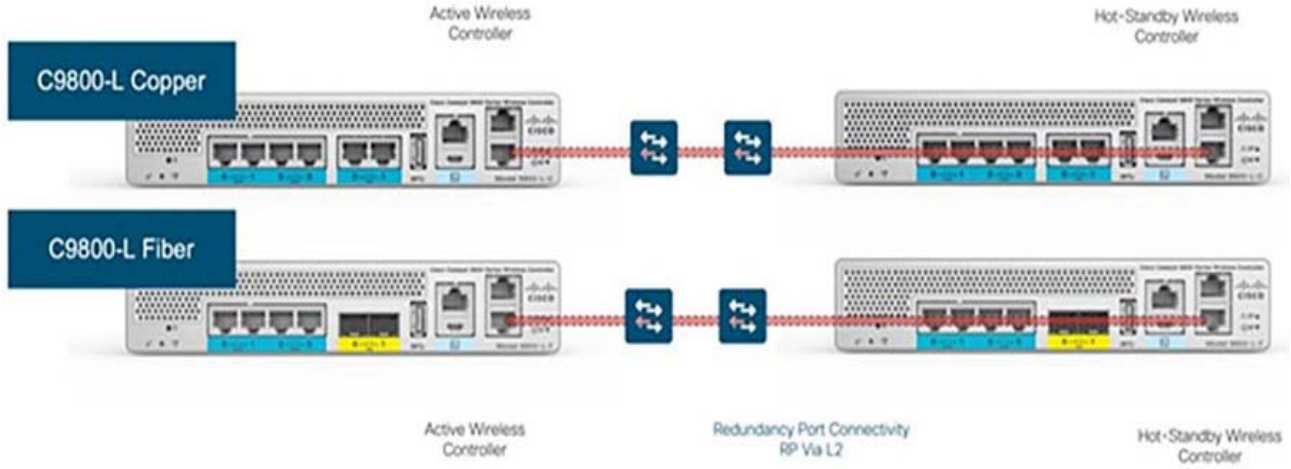
There are two options to connect both 9800 WLCs to each other, choose the one that fits you more. In this example implementation, RJ45 Ethernet ports are connected.

1. Redundancy Port–RJ45 10/100/1000 redundancy Ethernet port, as shown in Figure 24.

Figure 24 C9800-40 WLC RJ45 Redundancy Ports Connection

2. Redundancy Port–10-GE SFP ports, as shown in Figure 25:

Figure 25 C9800-L WLC Redundancy Ports Connection



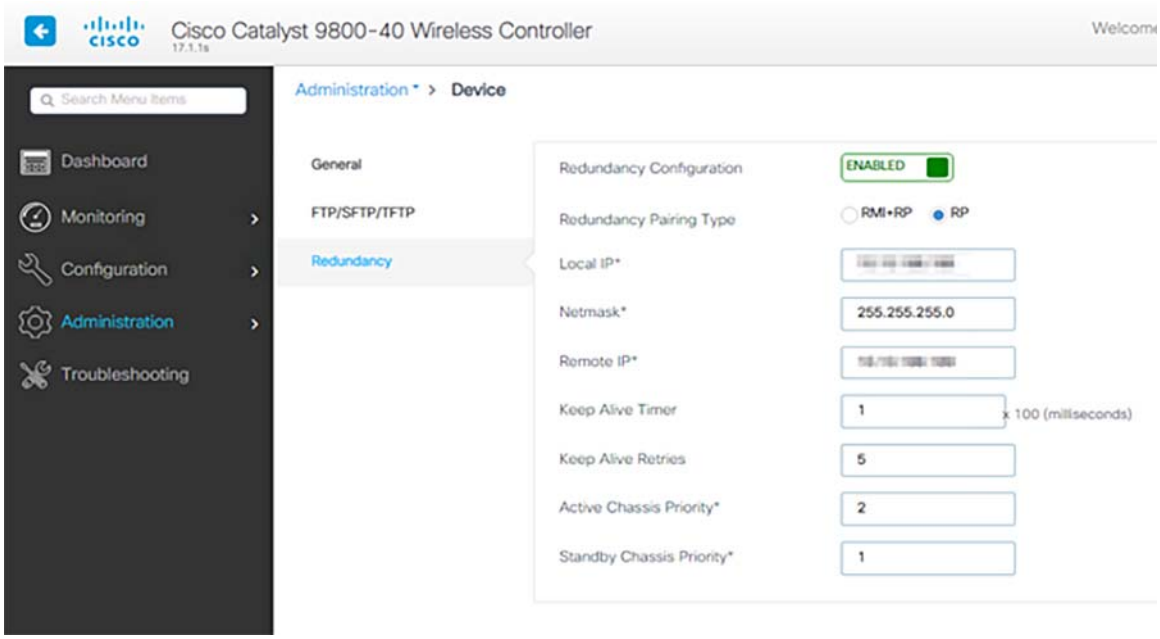
Step 3: Provide the required redundancy configurations to both 9800 WLCs.

Step 4: On WLC Web UI, navigate to **Administration-> Device-> Redundancy.** Enable **"Redundancy Configuration",** check '**RP**' for **"Redundancy Pairing Type"** and enter the desired IP address along with the Active and Standby Chassis Priorities. Each box should have its own IP address and they should both belong to the same subnet.

On the Active controller, the priority is set to a higher value than the standby controller. The wireless controller with the higher priority value is selected as the active during the active-standby election process. If we do not choose a specific box to be active, the boxes themselves will elect Active based on lowest MAC address. The Remote IP is the IP address of the standby controller's redundancy port IP.

C9800-40 WLC1 and C9800-40 WLC2:

Figure 26 Redundancy Pairing on both C9800-40 WLCs



Step 4: Switch to C9800 WLC CLI and configure Chassis HA interface.

```
C9800-40-WLC# chassis redundancy ha-interface local-ip x.x.x.x /24 remote-ip x.x.x.x
```

Step 5: Configure the priority of the specified device.

```
C9800-40-WLC# chassis 2 priority 2
```

Step 6: Configure the peer keepalive timeout value.

```
C9800-40-WLC# chassis redundancy keep-alive timer 1
```

Step 7: Configure the peer keepalive retry value before claiming peer is down.

```
C9800-40-WLC# chassis redundancy keep-alive retries 5
```

Step 8: Save configurations on both 9800 WLCs and reboot both boxes at the same time.

Step 9: On WLC Web UI, Navigate to **Administration-> Reload**, select **Save Configuration and Reload,** and click **Apply**.

Step 10: Switch to WLC CLI and type reload on CLI prompt.

```
C9800-40-WLC#reload
```

Step 11: Verify the HA configuration on both WLCs. Once both 9800 WLC have rebooted and are synchronized to each other, we can console into them and verify their current state with CLI commands as shown below.

```
WLC_C9800-40_1#show chassis
Chassis/Stack Mac Address : 4c71.0d17.b880 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
```

```
-------------------------------------------------------------------------------------
 1       Standby  10b3.d5ee.a520     1      V02     Ready               x.x.x.x
*2       Active   4c71.0d17.b880     2      V02     Ready               x.x.x.x
WLC_C9800-40_1#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 5 weeks, 35 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 2
        Current Software state = ACTIVE
       Uptime in current state = 5 weeks, 35 minutes
                 Image Version = Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9),
Version 17.1.1s, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 15-Feb-20 20:00 by mcpre
                         BOOT = bootflash:packages.conf,1;tftp:packages.conf 255.255.255.255,12;
                  CONFIG_FILE =
        Configuration register = 0x2102
               Recovery mode   = Not Applicable

Peer Processor Information :
----------------------------
              Standby Location = slot 1
        Current Software state = STANDBY HOT
       Uptime in current state = 5 weeks, 32 minutes
                 Image Version = Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9),
Version 17.1.1s, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 15-Feb-20 20:00 by mcpre
                         BOOT = bootflash:packages.conf,1;tftp:packages.conf 255.255.255.255,12;
                  CONFIG_FILE =
        Configuration register = 0x2102
```

Enable Console Access to Standby 9800 WLC

Once we enable HA and one of the boxes is assigned as active and the other one as standby hot, by default we are not allowed to reach exec mode (enable) on the standby box. To enable it, login by SSH/console to the active 9800 WLC and enter these commands:

```
# config t
# redundancy
# main-cpu
# standby console enable
# end
```

Force Switchover (Optional)

If we want to force a switchover between boxes you can either manually reboot the active 9800 WLC or run this command:

```
# redundancy force-switchover
```

Cisco Prime Infrastructure Installation and Configuration

Cisco Prime Infrastructure (PI) will act as a dedicated Network Management Server (NMS) providing network device and client monitoring and reporting services. The solution will integrate WLCs and APs with the existing virtual PI deployment. All configuration for WLCs and APs can be deployed using PI with the aid of configuration templates.

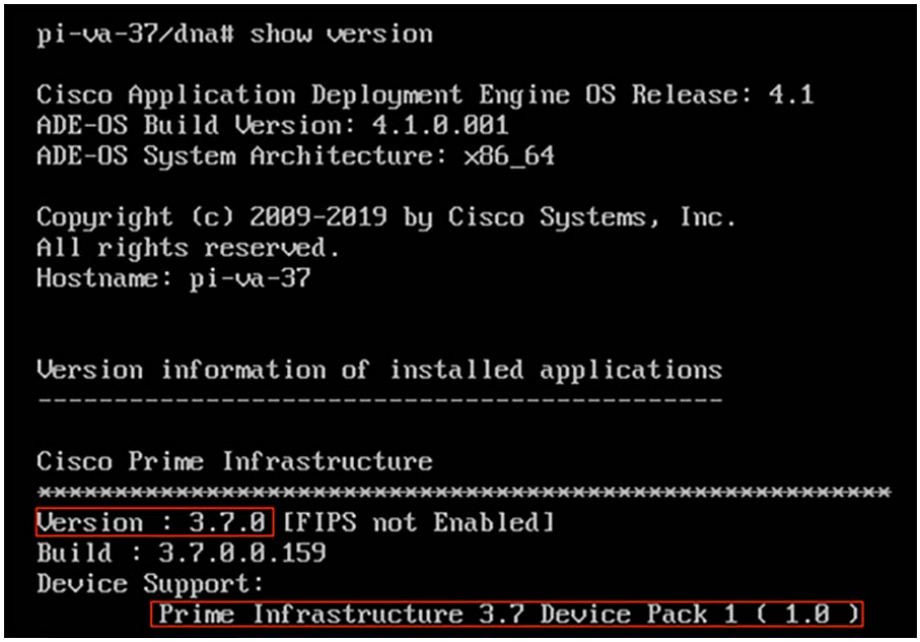
This section describes how to configure and integrate Catalyst 9800 Series Wireless Controllers with Prime Infrastructure (3.7) which uses CLI, Simple Network Management Protocol (SNMP) and NETCONF. Configuration details for SNMPv2 and SNMPv3 are included.

PI 3.7 Installation

PI 3.7 Virtual Appliance (VA) is installed in Shared Services network. Refer to the installation guide at the following URL which describes how to install Cisco Prime Infrastructure 3.7 as an OVA on VMware. Download the OVA file PI-VA-3.7.0.0.159.ova from Cisco.com. Verify the integrity of the OVA file using its checksum listed on Cisco.com.

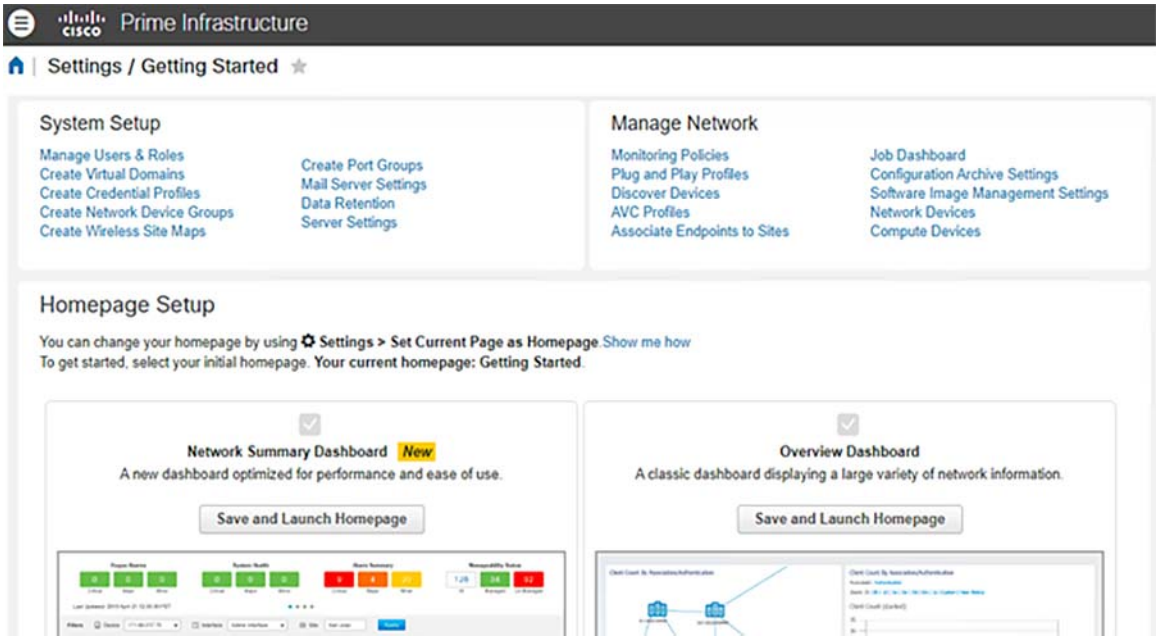
- https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/quickstart/guide/bk_Cisco_Prime_Infrastructure_3_7_0_Quick_Start_Guide.html

Figure 27 Prime Infrastructure 3.7 Verification



Access the PI WebUI with the IP address configure:

Figure 28 Cisco Prime Infrastructure Web UI–Dashboard View



Managing Catalyst 9800 WLC with Prime Infrastructure Using SNMP v3 and NETCONF

In order for Prime Infrastructure to configure, manage, and monitor Catalyst 9800 Series Wireless LAN Controllers, it needs to be able to access Catalyst 9800 via CLI, SNMP, and NETCONF. When adding Catalyst 9800 to Prime Infrastructure, telnet/SSH credentials as well as SNMP community string, version, etc. will need to be specified. PI uses this information to verify reachability and to inventory Catalyst 9800 WLC. It will also use SNMP to push configuration templates as well as support traps for AP and client events. However, in order for PI to gather Access Point (AP) and client statistics, NETCONF is leveraged. NETCONF is not enabled by default on Catalyst 9800 WLC and needs to be manually configured.

For more details, refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214286-managing-catalyst-9800-wireless-controll.html

Configuration on Catalyst 9800 WLC

SNMPv2 Configuration on Catalyst 9800 WLC

GUI:

Step 1. Navigate to **Administration -> Management -> SNMP -> Slide to Enable SNMP**.

Step 2. Click on **Community Strings** and create a Read-Only and a Read-Write community name.

CLI:

```
(config)#snmp-server community <snmpv2-community-name>
(optional)(config)# snmp-server location <site-location>
(optional)(config)# snmp-server contact <contact-number>
```

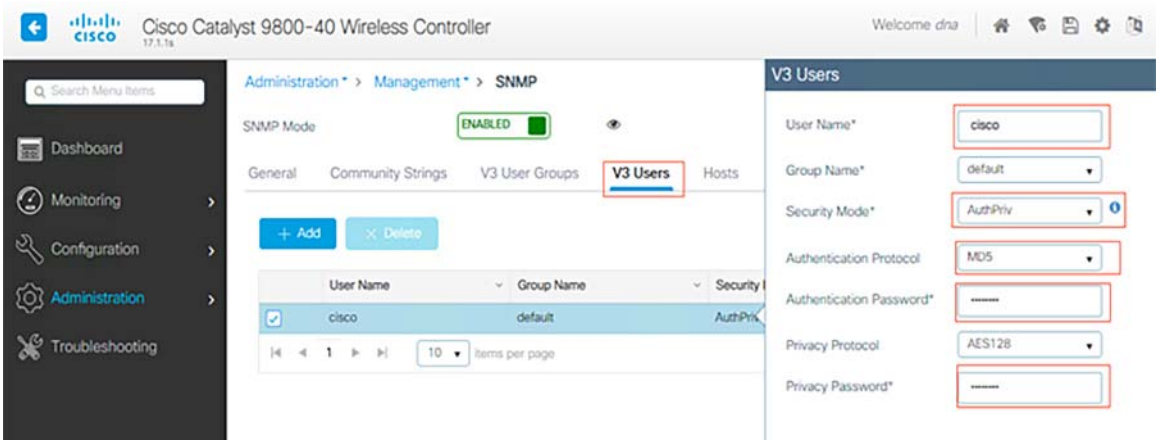
SNMPv3 Configuration on Catalyst 9800 WLC

GUI:

Note: As of 17.1 IOS-XE, the web UI will only allow to create read-only v3 users. Follow the CLI procedure to create a read-write v3 user.

Click on **V3 Users**. Create a user, choose **AuthPriv**, **SHA**, and **AES** protocols and chose long passwords as show in Figure 29.

Figure 29 Cisco 9800-40 WLC SNMP Configuration



CLI:

```
(config)#snmp-server view primeview iso included
(config)#snmp-server group <v3-group-name> v3 auth write primeview
(config)#snmp-server user <v3username> <v3-group-name> v3 auth {md5 | sha} <AUTHPASSWORD> priv
{3des | aes | des} {optional for aes 128 | 192| 256} <PRIVACYPASSWORD>
```

Note: SNMPv3 User Config is not reflected on running-configuration. Only SNMPv3 group configuration is seen

```
WLC_C9800-40_1#sh snmp user

User name: cisco
Engine ID: 8000000903004C710D17B88C
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: AES128
Group-name: default
```

NETCONF Configuration on the Catalyst 9800 WLC:

GUI:

Navigate to **Administration -> Management -> HTTP/HTTPS/NetConf**.

CLI:

```
(config)#netconf-yang
```

Note: If aaa new-model is enabled on Cat9800, then we will also need to configure

```
(config)#aaa authorization exec default local
(config)#aaa authentication login default local
```

NETCONF on 9800 uses the default method (and we cannot change this) for both aaa authentication login as well as aaa authorization exec. In case we want to define a different method for SSH connections, we can do so under the " line vty" command line. NETCONF will keep using the default methods.

Cisco Prime Infrastructure 3.7 Configuration

GUI:

Navigate to **Configuration -> Interface -> Wireless**.

Step 1. Capture the Wireless Management IP address configured on the Catalyst 9800 WLC.

CLI:

```
# show wireless interface summary
```

Navigate to **Administration -> User Administration**.

Step 2. Capture the privilege 15 user credentials as well as enable password.

CLI:

```
# show run | inc username
# show run | inc enable
```

Step 3. Get the SNMPv2 community strings and/or SNMPv3 user as applicable.

GUI:

For SNMPv2, Navigate to **Administration-> Management-> SNMP-> Community Strings**.

For SNMPv3, Navigate to **Administration-> Management-> SNMP-> V3 Users**.

CLI:

```
For SNMPv2 community strings
# show run | sec snmp
For SNMPv3 user
# show snmp user
```

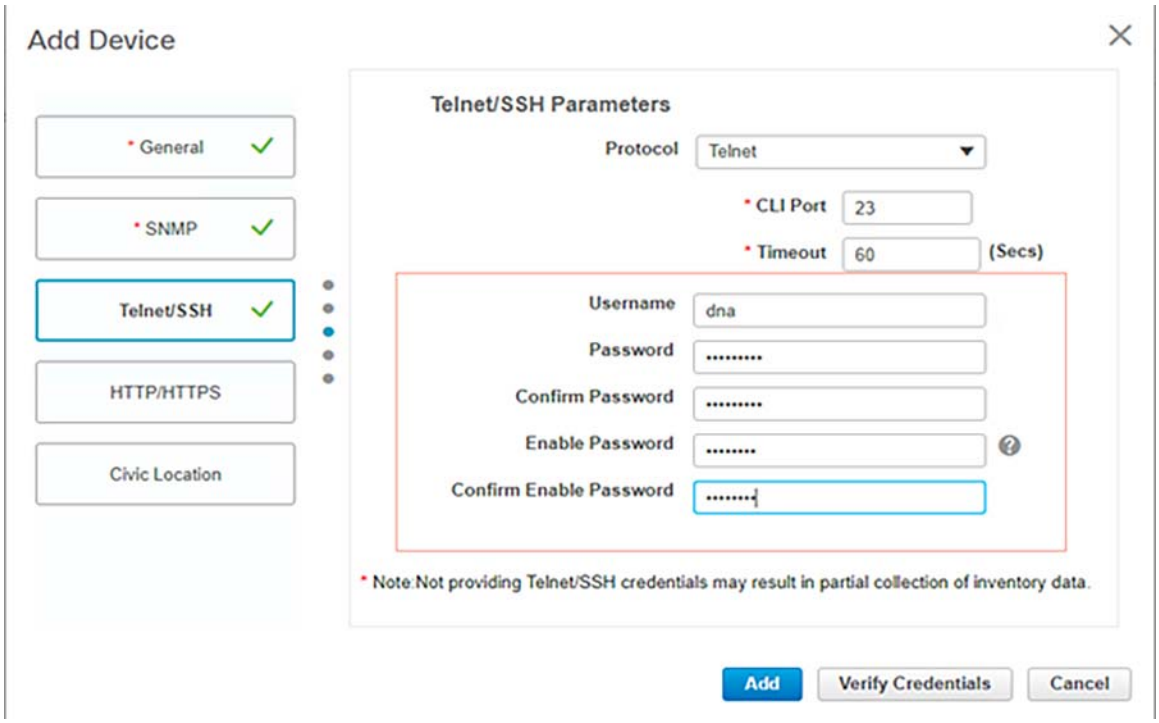
Step 4. On Prime Infrastructure GUI, navigate to click on **Configuration-> Network : Network Devices->** Click on Drop-Down beside **+-> Select Add Device.**

Step 5. On the **Add Device** pop-up, enter the interface IP address on 9800 that will be used to establish communication with Prime Infrastructure.

Step 6. Navigate to **SNMP** tab and provide **SNMPv3** details configured on Cat9800 WLC. From **Auth-Type** Drop-down match the previously configured authentication type and from **Privacy Type** Drop-Down select the encryption method configured on Cat9800 WLC.

Step 7. Navigate to **Telnet/SSH tab of Add Device**, provide the Privilege 15 Username and Password along with Enable Password. Click on **Verify Credentials** to ensure CLI, SNMP credentials work fine. Then click on **Add**, as shown in Figure 30.

Figure 30 Adding C9800 WLC to the PI



Verification:

Step 1. Verify that NETCONF is enabled on Cat9800:

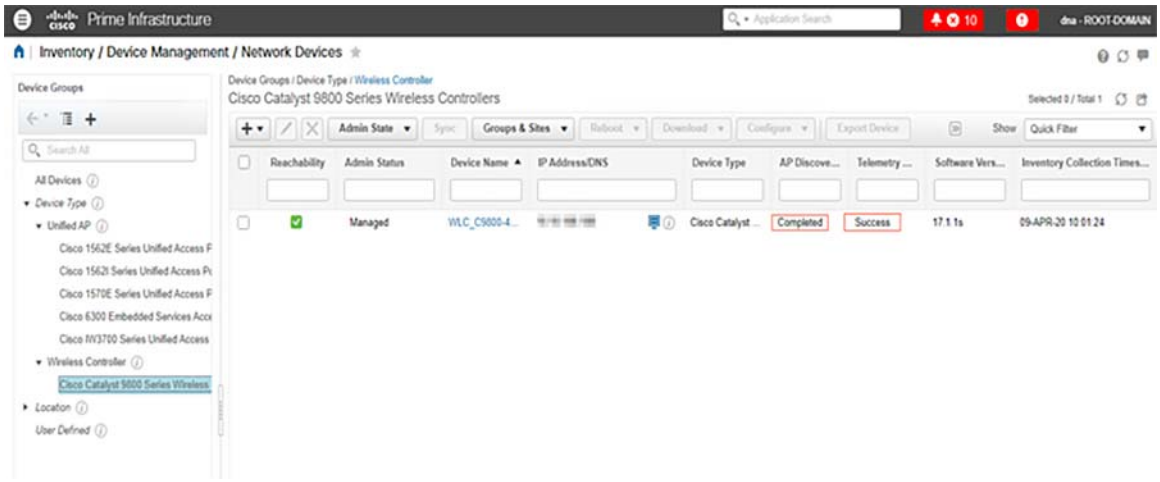
```
WLC_C9800-40_1#show run | inc netconf
netconf-yang
```

Step 2. Verify the telemetry connection to Prime from the Cat9800

```
WLC_C9800-40_1#show telemetry internal connection
Telemetry connection

Peer Address    Port  VRF Source Address  Transport  State         Profile
--------------- ----- --- --------------- ---------- ------------- -------------
< Prime IP >    20830   0 <   WLC IP  >   cntp-tcp   Active
```

Step 3. On Prime Infrastructure, navigate to **Inventory-> Network Devices-> Device Type** and verify the status as shown in Figure 31.

Figure 31 C9800 WLC on the PI as a Managed Device



Cisco Secure Network Analytics Installation and Configuration

The Cisco Secure Network Analytics (Stealthwatch) system collects and analyses flow telemetry generated by the network infrastructure for the purposes of network and security visibility. The Flow Collector leverages enterprise telemetry such as NetFlow, IPFIX (Internet Protocol Flow Information Export), and other types of flow data from existing infrastructure such as routers, switches, firewalls, endpoints, and other network infrastructure devices, Using flow telemetry, host behavior is monitored using continuous automated behavioral analysis techniques. The intelligence generated by Stealthwatch can be reported both to security and network operations staff in order to provide quick access and detailed analysis of security and network events.

The main components of Cisco Stealthwatch system are:

- Stealthwatch Management Console (SMC)
- Stealthwatch Flow Collector (SFC)

For more information, see the Cisco Secure Network Analytics web page:
https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

Stealthwatch Management Console

The Stealthwatch Management Console (SMC) is an enterprise-level security management system that allows network administrators to define, configure, and monitor multiple distributed Stealthwatch Flow Collectors from a single location. This system provides flow-based security, network, and application performance monitoring across physical and virtual environments. With Stealthwatch, network operations and security teams can see who is using the network, what applications and services are in use, and how well they are performing. The SMC client software allows you to access the SMC's user-friendly graphical user interface (GUI) from any local computer with access to a web browser.

Through the client GUI, you can easily access real-time security and network information about critical segments throughout your network.

Stealthwatch Flow Collector for NetFlow

The Stealthwatch Flow Collector (SFC) is responsible for collecting all NetFlow telemetry generated by a network's flow-capable devices. This is the heart of the Stealthwatch system and where data normalization and analysis occurs.

SMC and SFC are deployed as an Virtual Appliances in CCI Shared services VLAN in underlay network on ESXI host. This section describes and explains how to initialize SMC and add Flow Collector to SMC.

SMC and SFC Installation

For installing a SMC and FC Virtual Appliance using VMware, refer to “Installing a Virtual Appliance using VMware” in:

- https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf

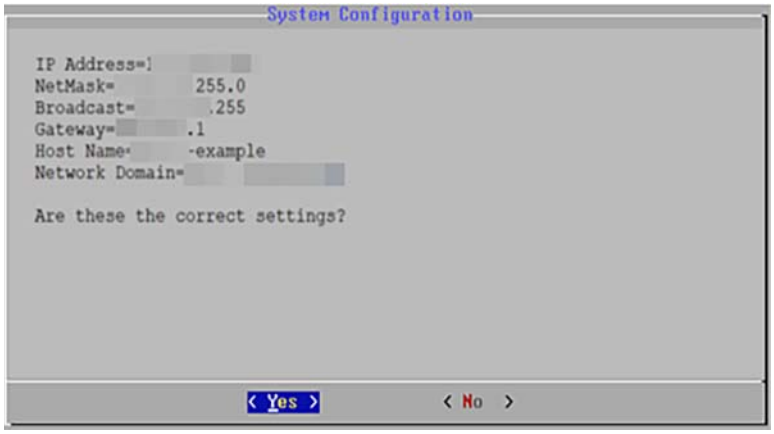
Step 1: Configuring IP addresses.

After you install the Stealthwatch VE appliances (both SMC and SFC) using VMware, you are ready to configure the basic virtual environment for them. In CCI network, we deployed the OVA file and powered up the VM. After the initial boot, it will ask you to enter the IP address, subnet, broadcast address, and gateway you would like to use. After you configure this, it will restart again.

For IP address configuration refer to “Configuring the IP Addresses” in:

- https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf

Figure 32 Stealthwatch System Configuration



After the VM restarts, you are shown a log in prompt. The default username/password is sysadmin/lan1cope. You can enter this and change the default password if you want.

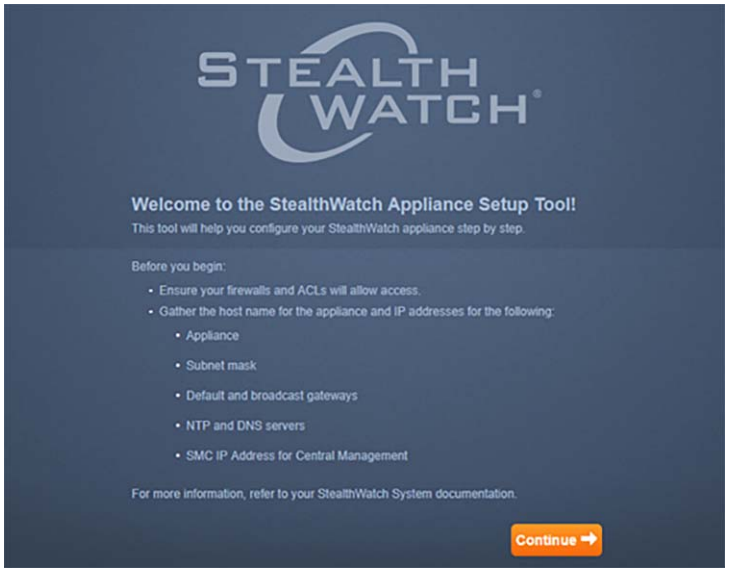
Note: You'll have to do the following setup for both the SMC and the SFC.

Step 2: Configuring the appliances.

Open up a browser and navigate to https://<ip-addr-of-SMC>.

You will be able to login to this page with the default username/password of admin/lan411cope. After initially signing in, you are shown the welcome screen shown in Figure 33.

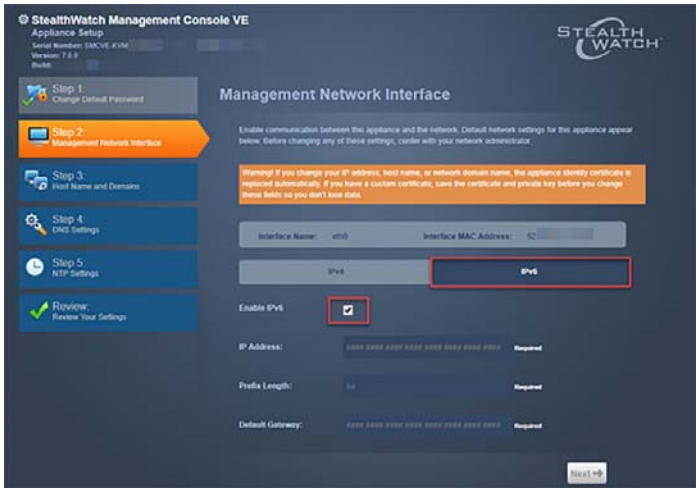
Figure 33 Stealthwatch Appliance Setup Tool



To configure the appliance, refer to “Configuring Your Appliances” in:

- https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf

Figure 34 Stealthwatch Management Console Appliance Configuration



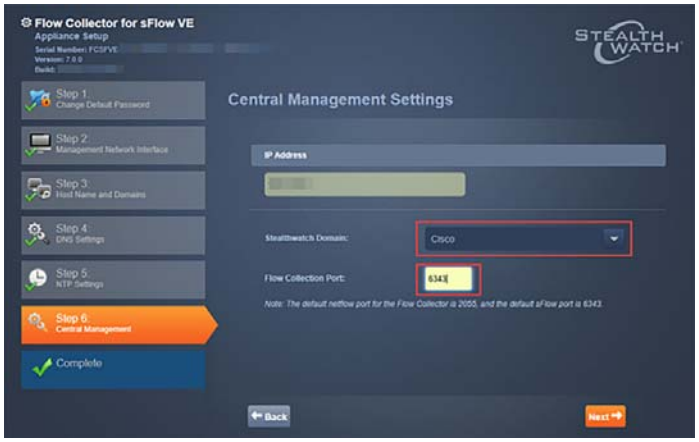
Note: You will have to do the appliance configurations for both the SMC and the SFC.

Step 3: Configure your Flow Collectors for Central Management.

To configure your Flow Collector so it communicates with your primary SMC/Central Manager, refer to “Configure your Flow Collectors for Central Management” in:

- https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf

Figure 35 Stealthwatch Flow Collector Appliance Configuration

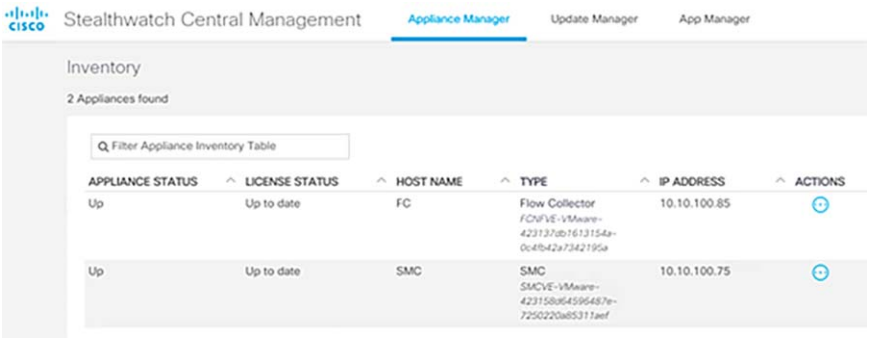


Verification:

After you configure an appliance in the Appliance Setup Tool and configure SFC for Central Management, confirm the appliance status in Central Management by navigating to log in to your primary SMC. Click the **Global Settings** icon and select **Central Management**.

Confirm the appliance is shown in the inventory and the status for the appliance is shown as **Up**.

Figure 36 Appliances on SMC



Netflow Configuration on Network Devices

In CCI network, NetFlow is enabled on Cisco IE switches (IE4000, IE5000, IE3400, and IE3300) in the ring to monitor the network flows. Using the DNA Center templates, Netflow can be enabled on the CCI devices.

Refer the following URL for details about the Cisco DNA Center Template Editor:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01000.html

Template:

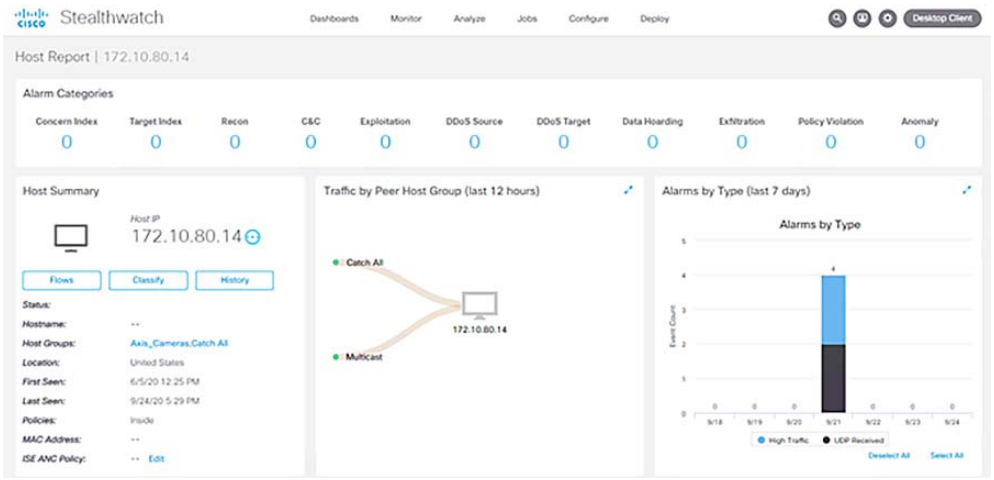
```
ip flow-export destination $fc $fc_port

##Configure the Flow Record##
flow record fnf-rec
match ipv4 tos
match ipv4 protocol
match ipv4 source address
```

```
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
##collect timestamp absolute first
##collect timestamp absolute last
exit

##Configure the Exporter##
flow exporter fnf-exp
destination $fc
transport udp $fc_port
template data timeout 30
option interface-table
option application-table timeout 10
exit

##Configure the Flow Monitor##
flow monitor fnf-mon
exporter fnf-exp
cache timeout active 60
record fnf-rec
exit

##Apply to an interface##
interface $wired_interface
ip flow monitor fnf-mon input
```

Verification:

You can verify the traffic flow monitoring on the SMC dashboard.

Figure 37 Stealthwatch Management Console Dashboard



Stealthwatch and ISE Integration

This section describes the steps to configure Cisco Stealthwatch Management Centre (SMC) and Cisco Identity Services Engine (ISE) using pxGrid. Once integrated with ISE, the SMC will learn the user session information (IP address/username bindings), Static TrustSec mappings, and Adaptive Network Control (ANC) mitigation actions for quarantining endpoints.

Step 1: Generating certificates.

To connect Stealthwatch and Cisco ISE, certificates must be deployed correctly for trusted communication between the two systems. Deploying certificates requires that you use several different product or application interfaces: the SMC Web App, the Central Management interface, and the Cisco ISE Server management portal. Starting with v7.0, Stealthwatch only imports client certificates created with a Certificate Signing Request (CSR) generated from Stealthwatch Central Management to connect to ISE pxGrid node.

The recommended method of deploying certificates is to use the ISE internal Certificate Authority (CA). This option is only available with ISE 2.2 and above.

To deploy certificates using the ISE internal CA, refer to “Using ISE Internal CA” in:

- https://community.cisco.com/t5/security-documents/deploying-cisco-stealthwatch-7-0-with-cisco-ise-2-4-using-pxgrid/ta-p/3793357?attachment-id=165804

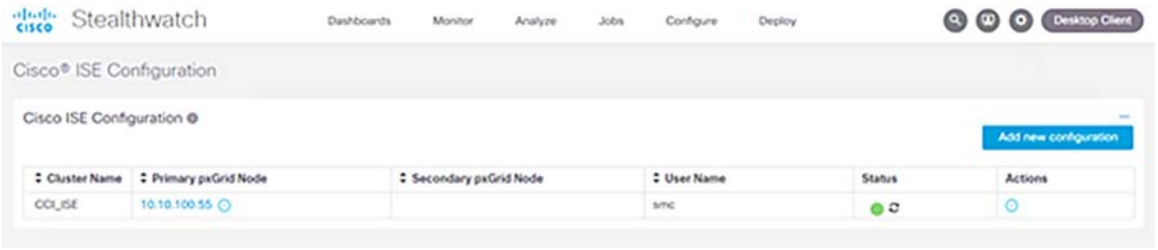
Figure 38 Client Identity in SMC

Step 2: Configuring ISE pxGrid integration.

To configure Stealthwatch to successfully connect, register, and subscribe to the ISE pxGrid node, refer to “Configuring ISE pxGrid Integration” in:

- https://community.cisco.com/t5/security-documents/deploying-cisco-stealthwatch-7-0-with-cisco-ise-2-4-using-pxgrid/ta-p/3793357?attachment-id=165804

Figure 39 Stealthwatch Integration with ISE



Step 3: Applying ISE Adaptive Network Control (ANC) policies.

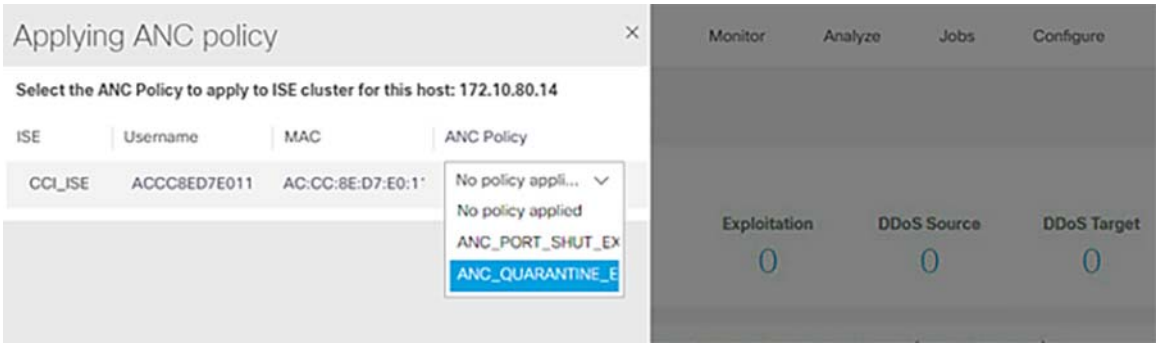
ISE ANC policies align with organizations security policies. For example, when malware or breaches are detected, the organization may investigate further by providing segmented network access or, if the threat is more severe and capable of propagating through the network, the IT administrator may want to shut down the port.

Possible ANC actions are: quarantine (Change or Authorization), port-shut, and port bounce. These ANC policies will then be used as condition rules in ISE authorization policies to enforce the organizations security policy.

To create ISE ANC policies and associate to Stealthwatch, refer to “SE Adaptive Network Control (ANC) Policies” in:

- https://community.cisco.com/t5/security-documents/deploying-cisco-stealthwatch-7-0-with-cisco-ise-2-4-using-pxgrid/ta-p/3793357?attachment-id=165804

Figure 40 ISE ANC Policy on Stealthwatch



Stealthwatch Use Cases

Cisco Stealthwatch provides comprehensive network visibility and threat detection for accelerated incident response. For more information, see:

- https://community.cisco.com/t5/security-documents/stealthwatch-use-cases/ta-p/3611837

Licensing

Use the Stealthwatch Downloading and Licensing Guide to activate licenses on your appliances:

- https://www.cisco.com/c/en/us/support/security/stealthwatch/products-licensing-information-listing.html

Cisco Cyber Vision Center Installation and Configuration

This section describes the deployment of Cisco Cyber Vision Center (CVC) in Shared Services.

The Cyber Vision Center can be deployed as a virtual machine (VM) or as a hardware appliance. In this deployment, the standalone Cyber Vision Center is deployed as a VM on a Cisco Unified Computing System (UCS) in the CCI Shared Services network.

For step-by-step instructions on installation and resource recommendations of CVD, refer to the Cisco Cyber Vision Center VM Installation Guide at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_4_0_0.pdf

It is recommended to install the Cyber Vision Center application in the CCI Shared Services network with dual interfaces; one for management and the other for sensor communication, respectively.? An example of the IP addressing schema used in CVC installation is shown below.

■Admin Interface (eth0): 10.104.206.225 (Routable IP address for CVC UI access)

■Collection interface (eth1): 10.10.100.33 (shared services network IP)

■Collection network gateway: 10.10.100.1 (shared services gateway)

■NTP: 10.10.100.1

Refer to the section “Cisco Cyber Vision Operational Technology (OT) Flow and Device Visibility Design” in the CCI General Solution Design Guide for the detailed design and deployment considerations for CVC, Network Sensors on IE3400 and IE3300-X series switches, and the IR1101 for RPoP in a CCI deployment.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html

Implementation of Point-of-Presence (PoP) Sites

This section covers the implementation of a CCI PoP site aka Fabric site with the Cisco DNA Center SD-Access. A fabric overlay network is provisioned on the underlay network implemented on each fabric/PoP site for SD-Access network implementation in a PoP or a fabric site construct, as defined in the CCI Solution design.

This section includes the following major topics:

Note: The implementation steps for the SD-Access Network deployment that are covered in this section provide a summary of steps to be followed along with example configurations used for implementing fabric sites for CCI network topologies discussed in the section Deployment Topology Diagrams, page 7. For detailed step-by-step instruction for SD-Access deployment, refer to the following URL:

- https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/sda-fabric-deploy-2019oct.pdf

Preparing Cisco DNA Center for PoP Site Provisioning

In the Cisco DNA Center, the “Design” area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Create a network hierarchy of areas, buildings, and floors that reflect the physical deployment. In later steps, discovered devices are assigned to respective PoP sites in Cisco DNA Center GUI, so that they are displayed hierarchically in the topology maps.

To prepare to design your Cisco DNA Center for CCI network fabric implementation, refer to the chapter “Design Network Hierarchy & Settings” in the *Cisco Digital Network Architecture Center User Guide, Release 2.2.3* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html

1. Creating network hierarchy.

   In this implementation, three fabric sites are created as shown in Figure 3 and Figure 4 for various deployment models of the network topologies with IP Transit and SD-Access Transit fabric interconnection. Example fabric sites with the names MGRoad, Hebbal, Elex City are configured for the fabric sites PoP1 Site, PoP2 Site, PoP3 Site respectively. In Figure 41, the sites with names Cessna and Koramangala are configured as HQ/DC site and SDA transit site respectively.

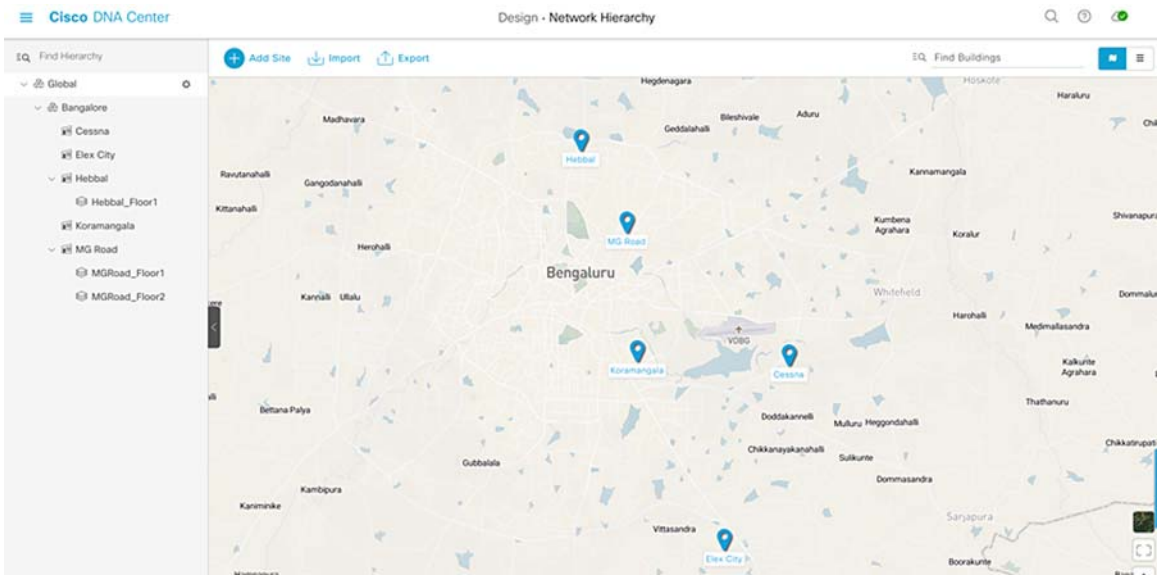
   Note: In CCI deployment, a PoP site can be mapped to an area with a building under that area in Cisco DNA Center network hierarchy. By creating buildings, you can apply settings to a specific area or a PoP site.

   For more details about Network Hierarchy and steps to configure the hierarchy of PoP sites and HQ/DC Site, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.htm

  Figure 41 shows an example Network Hierarchy under the **Design** tab in the Cisco DNA Center user interface for the CCI network implementation:

Figure 41 Example CCI Network Hierarchy View in Cisco DNA Center



2. Configuring network settings.

   Set up network properties such as AAA, DHCP, DNS, and NTP for the CCI network. Cisco DNA Center will configure the network settings on the devices while provisioning the discovered devices in the fabric.

   Refer to the following sections to configure network settings:

   – Manage Global Network Settings:

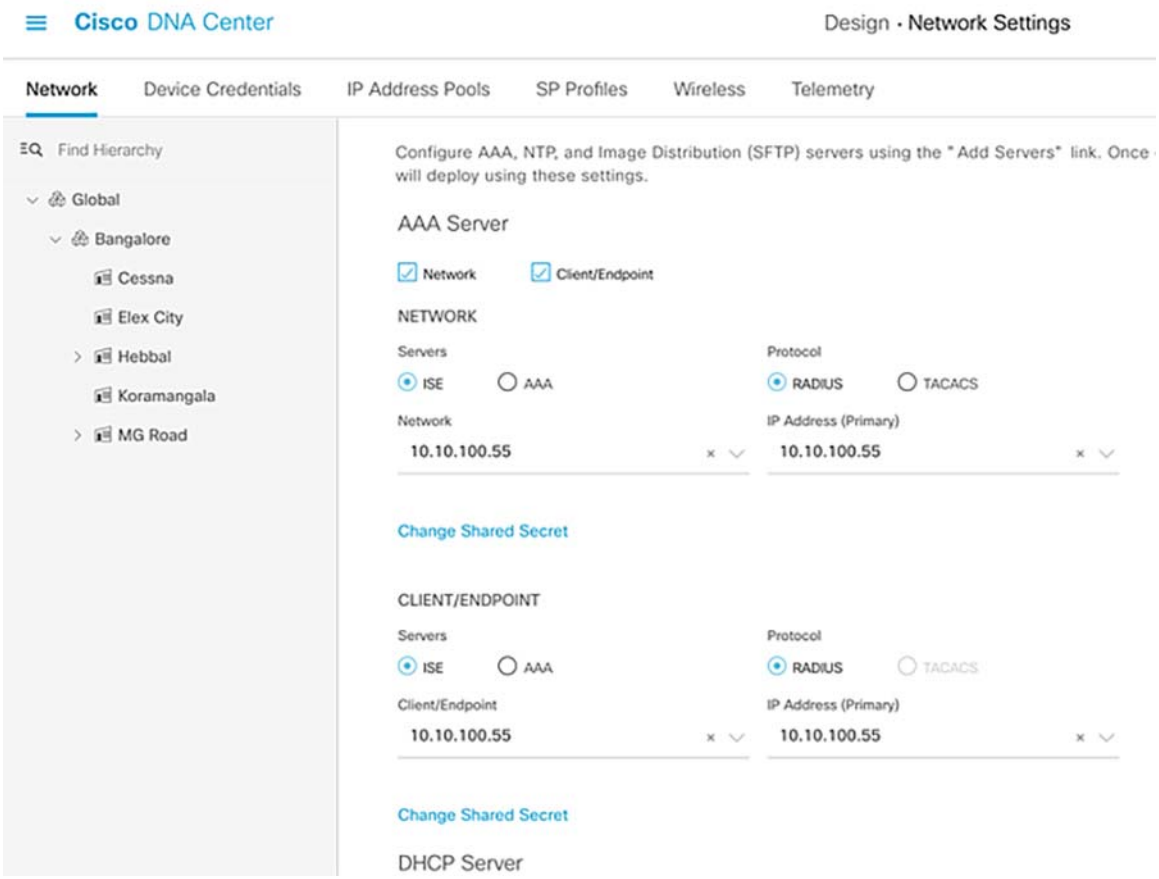
     ▪ https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#concept_gvs_1rd_wy

   – Configure Global Network Servers:

     ▪ https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#task_bw1_vyb_yz

Figure 23 shows an example Network Settings configured in the Cisco DNA Center for the CCI network topology:

Figure 42 Example Global Network Settings View in Cisco DNA Center



3. Setting device credentials for device discovery.

   – Device credentials refer to the CLI, SNMP, and HTTPS credentials that are configured on network devices. Cisco DNA Center uses these credentials to discover and collect information about the devices in your network. Configure global/site level device credentials to discover all the network devices in the CCI network for fabric/PoP site provisioning.

Refer to the following sections for configuring device credentials in the Cisco DNA Center:

– About Global Device Credentials:

  ▪ https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#concept_zww_qtd_wy

– Configure Global CLI Credentials:

  ▪ https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#task_a5t_5xg_2z

– Configure SNMPv3 Credentials:

  ▪ https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#task_fgz_lyg_2z

4. Configuring IP address pools.

   IP address pools that will used for fabric infrastructure provisioning, extended nodes in the CCI network, and data network are manually defined and configured on the Cisco DNA Center. It reserves pools as a visual reference for use in fabric sites (PoPs). In this implementation, a windows DHCP server is used.

   Alternatively, you can integrate third party IP Address Manager (IPAM) servers to Cisco DNA Center in order reduce IP address management tasks. IPAM integration with Cisco DNA Center provides:

   – Access to existing IP address scopes, referred to as IP address pools in Cisco DNA Center.

   – When configuring new IP address pools in Cisco DNA Center, the pools populate to the IPAM server automatically.

   To integrate IPAM server to Cisco DNA Center, refer to the “Configure an IP Address Manager” section at the following URL:

   - https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#task_umt_4kt_pcb

   Refer to the following sections for adding and reserving IP address pools as needed in CCI network deployment:

   – Configure IP Address Pool:

   - https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#task_znt_jdc_yz

   – Reserve an IP Pool:

   - https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_0110.html#id_105306

   Figure 43 and Figure 44 show example IPv4 address pools with global network prefixes and reserved IP pools in a site for fabric border network handoff, extended node, and data networks on fabric overlay VNs.

Figure 43 Example Global IPv4 Address Pools View in Cisco DNA Center

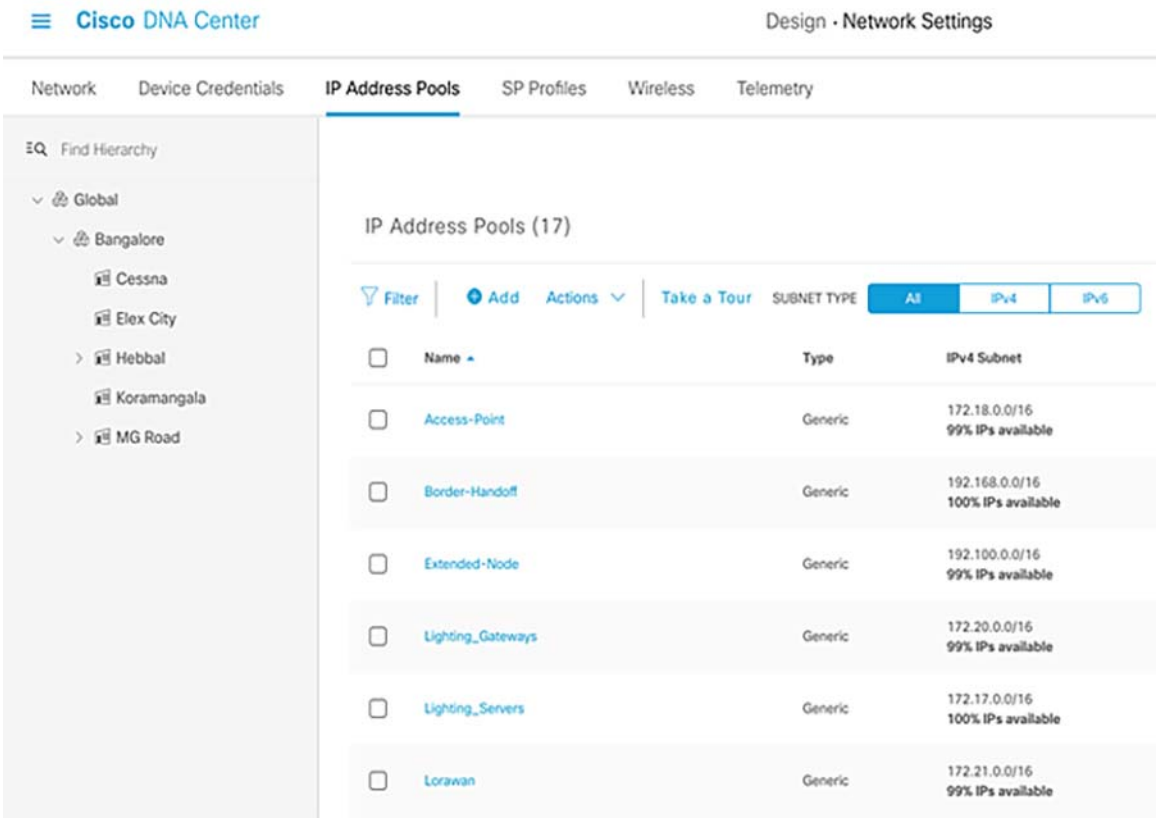
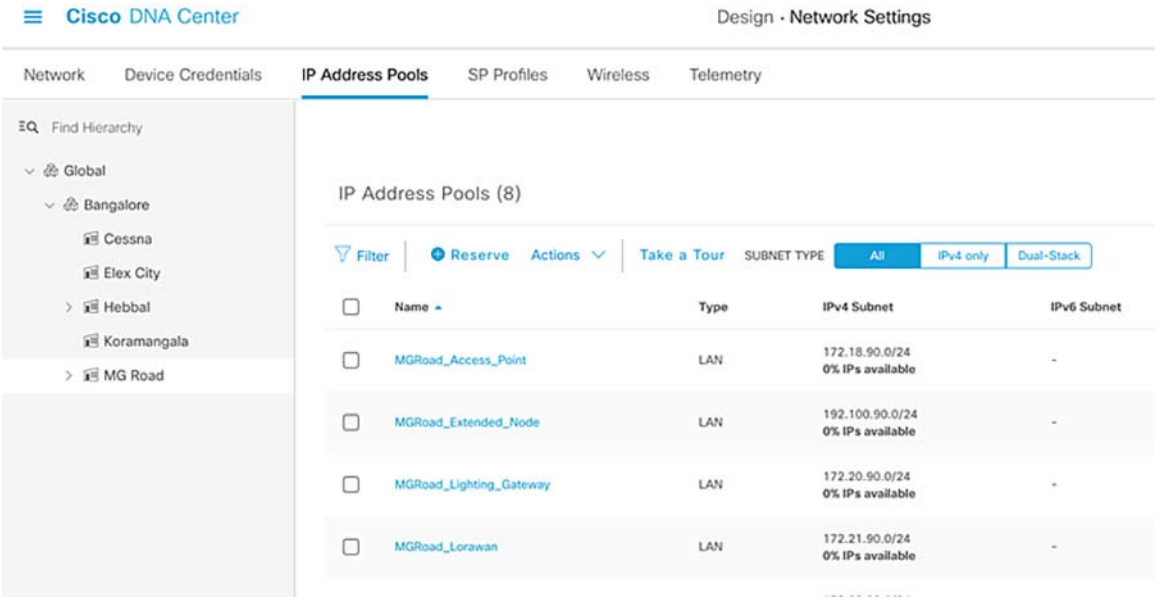


Figure 44 Example IPv4 Address Pools Reserved in a Fabric/PoP Site



This completes the initial preparation of Cisco DNA Center for devices discovery and fabric site provisioning.

Discovering Devices in the Network

Cisco DNA Center is used to discover and manage the SD-Access underlay network devices that are compatible with the Cisco DNA Center. For the list of the devices supported by Cisco DNA Center, refer to the following URL:

- https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

To discover equipment in the network, the appliance must have IP reachability to these devices, and CLI and SNMP management credentials must be configured on the devices. Once discovered, the devices are added to Cisco DNA Center's inventory, allowing the controller to make configuration changes through provisioning.

1. For the Network devices to be discovered by the Cisco DNA Center, CLI and SNMP credentials should be configured on the devices as configured at the Cisco DNA Center in the previous section.

   The example configuration used network devices in this implementation:

   a. Configure CLI SSH user credentials on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

   ```
   username <username> privilege 15 password 7 <password>
   enable secret <password>
   ```

   b. Configure SNNMPv3 credentials on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

```
snmp-server group default v3 priv snmp-server group ciscogrp v3 priv read SNMPv3All write
SNMPv3None snmp-server view SNMPv3All iso included snmp-server view SNMPv3None iso excluded

snmp-server community <CommunityString> RW
snmp-server user <username> default v3 auth md5 <password> priv aes 128 <password>
```

   c. Enable SSH Version 2 access on the network device. Example configuration on Cisco Catalyst 9300 Switch Stack:

   ```
   ip ssh source-interface Loopback0
   crypto key generate rsa modulus 2048
   ip ssh version 2
   !
   line vty 0 4
    login local
    transport preferred ssh
    transport input all
   line vty 5 15
    login local
    transport preferred ssh
    transport input all
   !
   ```

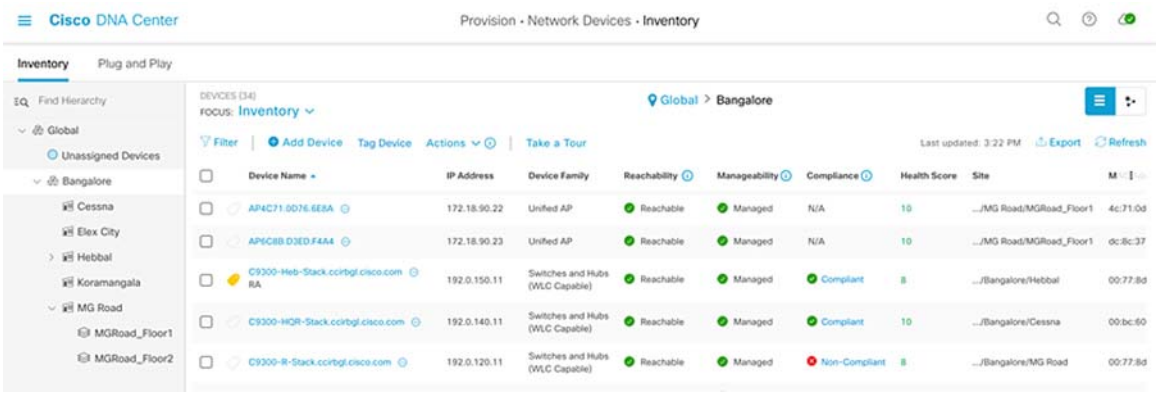
   Repeat the above configurations on all the network devices in the network to be discovered by the Cisco DNA Center.

2. For detailed step-by-step instructions on discovering all the device in the CCI network on Cisco DNA Center, refer to the chapter “Discover your Network” in the *Cisco Digital Network Architecture Center User Guide, Release 2.2.3* at the following URL:

   – https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_010.html

   Once device discovery is successful, all the devices are added to Cisco DNA Center Inventory, as shown in the example in Figure 45:

Figure 45 Example List of Discovered Devices in Cisco DNA Center Inventory



Provisioning Devices in SD-Access

Once the devices are discovered and managed in the Cisco DNA Center inventory, devices have to be provisioned to the sites for SD-Access Deployment.

For more details and step-by-step instruction for provisioning devices in SD-Access site, refer to the following section in the *Software-Defined Access for Distributed Campus Deployment Guide* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487388

For how to assign the device to sites and provisioning devices, click “Process 5: Deploying SD-Access with the Provision Application” and follow Procedures 1 and 2 at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487382

Once the devices are provisioned to the sites, all the details added in the network settings like AAA, NTP, DHCP, and DNS are configured on the devices by Cisco DNA Center.

Provisioning Fabric Overlay Network

Once devices are provisioned to a site, the fabric overlay workflows can begin. This starts through the creation of transits, the formation of a fabric domain, and the assignment of sites, buildings, and/or floors to this fabric domain.

Fabric domain is configured in the Cisco DNA Center for a fabric overlay network. After adding the sites to the Network Hierarchy, the network sites have to be part of a fabric domain. Once the fabric domain is added, add the transit networks (either IP transit or SDA transit or both) for interconnecting multiple fabric sites (PoPs). In this implementation, both the transit network types (IP Transit and SD-Access Transit) are validated for the network topologies, as shown in Figure 3 and Figure 4.

Configuring Fabric Domain and Transit Network(s)

Depending on your network deployment and backhaul network for interconnecting fabric sites, you can choose to deploy either IP Transit or SD-Access Transit as applicable:

1. For provisioning the fabric domain and creating a IP-based transit network in the Cisco DNA Center, click " Process 6: Provisioning the Fabric overlay" and follow Procedures 1, 3, and 4 in the *Software-Defined Access for Distributed Campus Deployment Guide* at the following URL:

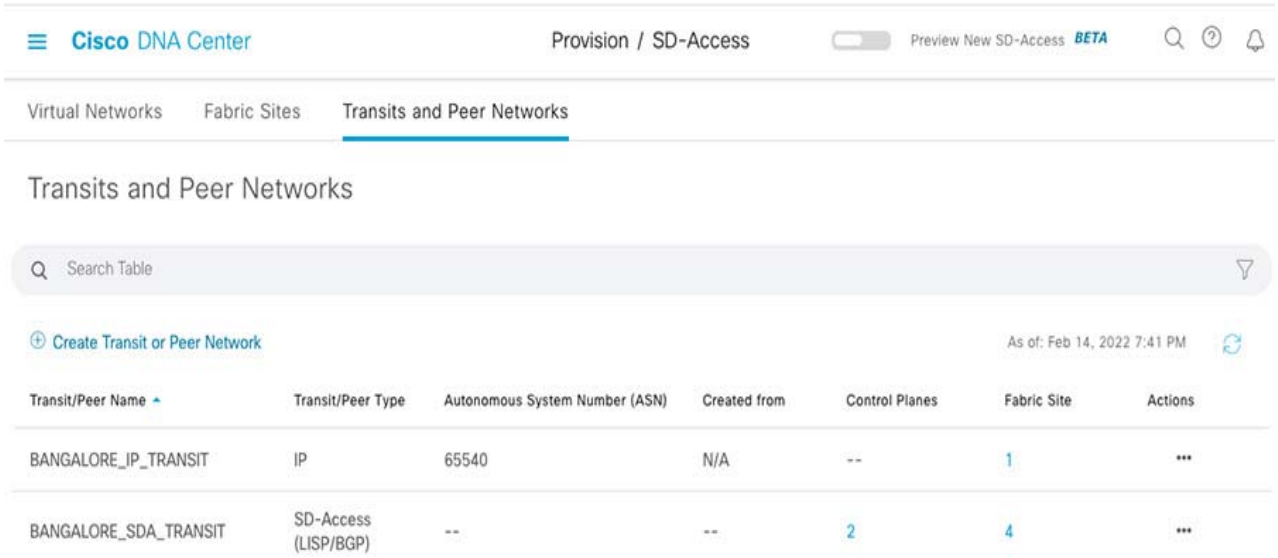
- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487387

2. Optionally, follow Procedure 2 to create an SD-Access transit network for an example network topology, as shown in Figure 3.

   Note: For the SD-Access transit network, it is required to assign the transit control plane nodes (example: Cisco Catalyst 9500 switches) to a site that will be provisioned as a SD-Access transit site, by completing the steps mentioned in Provisioning Devices in SD-Access, page 73.

Figure 46 shows an example fabric domain: IP-based Transit and SD-Access Transit networks created for the network topology in Figure 3 and Figure 4.

Figure 46 Example Fabric Domain, IP-based, and SD-Access Transit Networks



Assigning Fabric Role (Fabric-in-a-Box)

Once the sites are added to the fabric domain in the Cisco DNA Center, a Cisco Catalyst 9300 Stack that is added in a site is provisioned with fabric roles. A fabric overlay consists of three different fabric nodes: control plane node, border node, and edge node. To function, a fabric must have an edge node and control plane node. This allows endpoints to traverse their packets across the overlay to communicate with each other (policy dependent). The border node allows communication from endpoints inside the fabric to destinations outside of the fabric along with the reverse flow from outside to inside.

In the CCI network fabric site (PoP), a switch stack (Cisco Catalyst 9300) is configured with all the fabric roles (i.e., border, control plane, and edge called FiaB). Fabric is provisioned with an overlay VN; i.e., macro-segmentation for the overlay network is defined. (Note that the overlay network will only be fully created until the host onboarding stage). This process virtualizes the overlay network into multiple self-contained VNs.

1. Creating Overlay VN

   In the CCI network, VNs and SGTs are created for each vertical use case overlaid on the CCI network. An example list of VNs created in this implementation are available in Table 2.

   To create VNs in the fabric as needed, refer to Procedure 1 under section " Process 4: Creating Segmentation with the Cisco DNA Center Policy Application" in the Software-Defined Access for Distributed Campus Deployment Guide

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487379

2. Associate VN to Fabric Site

   IP address pools enable host devices to communicate within the fabric site. Associate IP addresses pools for end-points data traffic in the overlay VN.

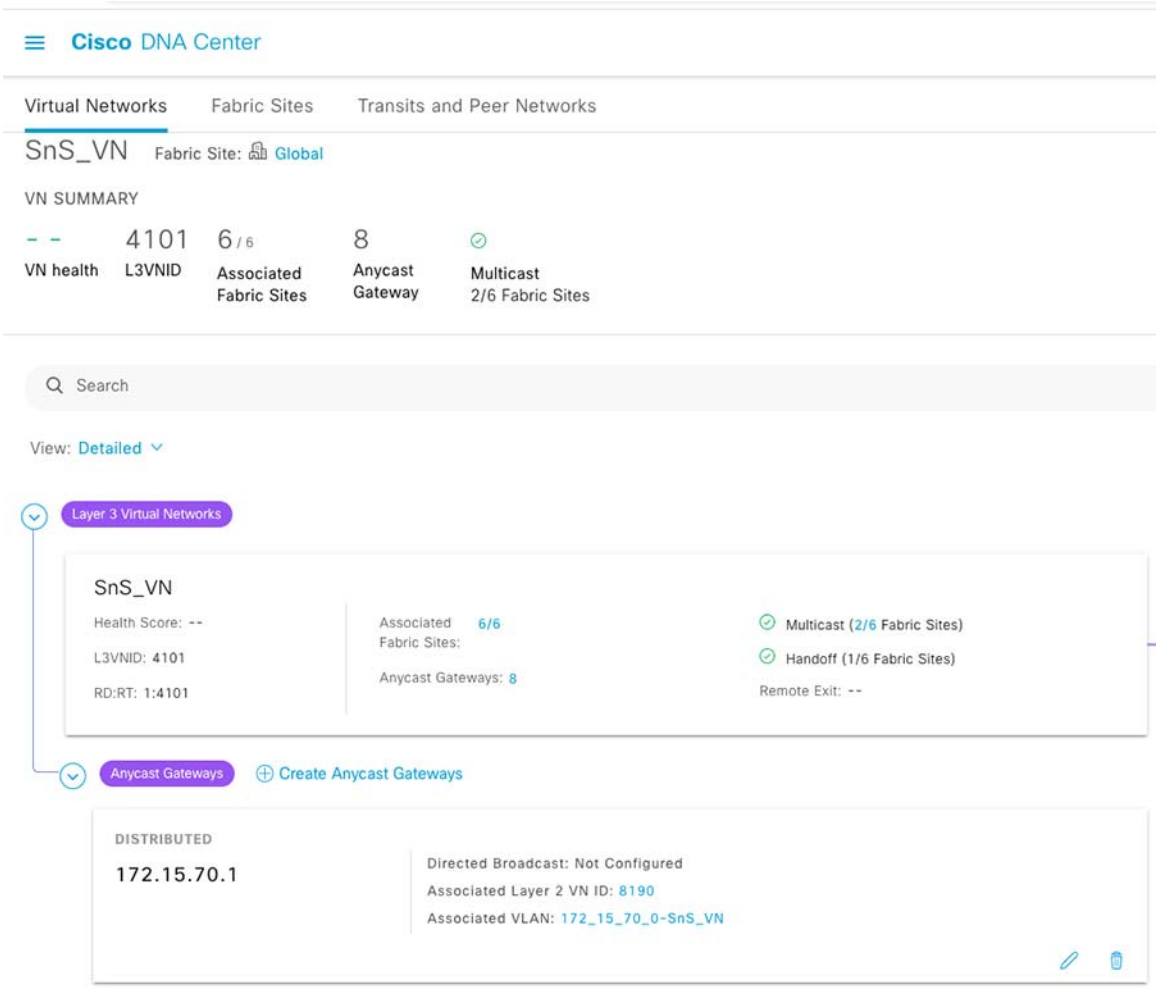
   Follow the steps in Virtual Network section under the chapter “Provision Fabric Networks” to create VNs and associate IP address pools to a VN:

   https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01110.html#id_50854

   Note: Select **No Authentication** for the default Authentication Template for a fabric site. The No Authentication template is selected as default template.

Figure 47 shows an example VN and overlay IP pools associated with a VN (SnS_VN) in the CCI network:

Figure 47 Example Virtual Network and IP Pools Association in CCI Network



– Similarly, associate an IP pool in the fabric default INFRA_VN for Extended Nodes IP addressing.

3. Provisioning Fabric-in-a-Box (FiaB)

   Once the VNs are associated with the fabric sites, provision a Cisco Catalyst 9300 Switch stack as FiaB in the CCI fabric (PoP) site. A Layer 3 handoff that extends the fabric VNs to the next hop (i.e., fusion router, in the case of IP-based Transit or SDA Transit CP or intermediate network device, in the case of SDA Transit). This will allow the end-points in the fabric to access shared services once the fusion router configuration is completed.

   Complete the following steps to provision a Cisco Catalyst 9300 Switch stack in a fabric/PoP site as FiaB for IP-based transit network topology, as shown in Figure 3:

   a. In **Cisco DNA Center**, navigate to **Provision-> Fabric**.

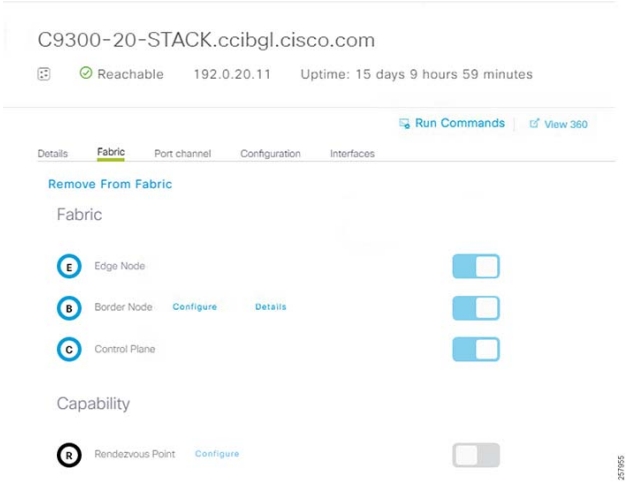
   b. Select the **Fabric Enabled Site** (Bangalore) that was created.

   c. Select the PoP site (MGRoad) from the fabric-enabled sites in the left pane.

   d. Select the device to be provisioned as a FiaB. A slide pane appears.

   e. On the slide pane, select the roles **Edge node**, **control plane**, and **border node**, as shown in Figure 48.

Figure 48 Example FiaB Provisioning View for IP Transit



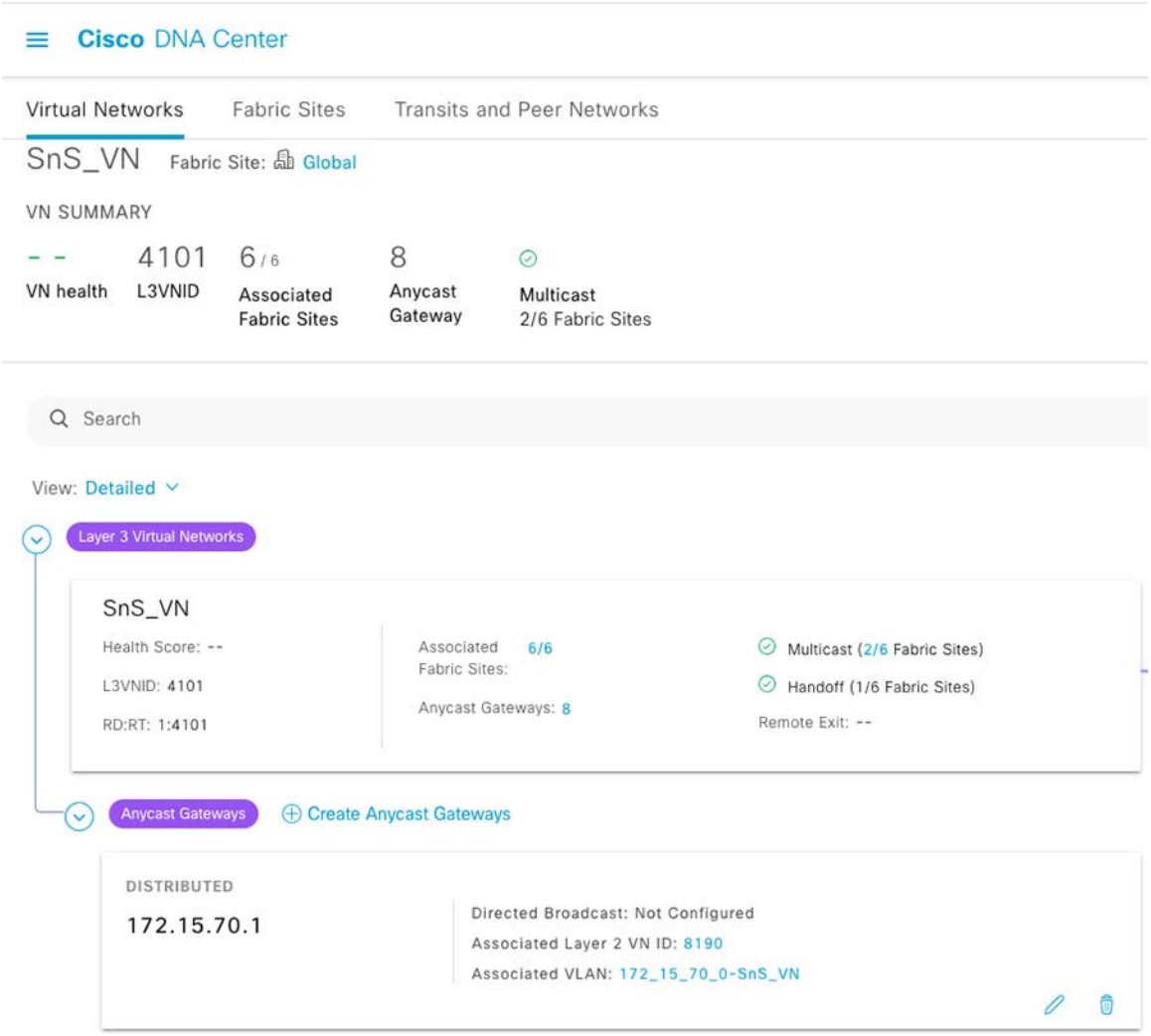
   f. Click **Configure** next to **Border Role**, configure the local Autonomous number for the site, and select the Layer 3 handoff network pool associated with the site.

   g. Under the **Transit/Peer networks**, enable the option **Default to all Virtual networks** and then select the transit site. In this case, we used **SD Access Transit**.

   h. Select the Transit Control Plane devices and then click **Add**.

   Example provisioning for IP transit external interfaces is shown in Figure 49.

Figure 49 Example FiaB Border Configuration for SD-Access Transit in CCI Network



i. Once done, click **Add** and **Save** to provision the FiaB and for the successful provisioning of the Fabric message in the Cisco DNA Center UI.

j. Verify the FiaB provisioning in Cisco DNA Center UI for the network site. No errors should be reported in the **Fabric Infrastructure** map view of the FiaB.

Alternatively, if you are deploying an IP Transit based network topology, as shown in Figure 4, you need to configure the FiaB Border to connect to an SD-Access Transit Network created in Step 2 of the Configuring Fabric Domain and Transit Network(s), page 73.

Refer to the following URL for steps to create the IP Transit network in Cisco DNA Center:

– https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01110.html#id_75992

This completes the FiaB provisioning or fabric role assignment in the fabric overlay network for a PoP site connected to either the SD-Access Transit or IP-based Transit network.

Implementing Wireless LAN Controller in a PoP

In CCI, Cisco Catalyst 9800 Series Wireless Controller (C9800-L) or Cisco Catalyst 9300 Series Switch Stack with embedded Wireless Controller can be configured. C9800-L WLC manages Cisco Unified Wireless Network (CUWN) Wi-Fi access mesh and non-mesh deployments. Alternatively, an embedded WLC on C9300 switch stack can be deployed for managing SD Access Wireless (Wi-Fi) networks. Refer to the "CCI Wi-Fi Access Network Solution" section in the Connected Communities Infrastructure Design Guide at the following URL for more details on the CCI Wi-Fi design.

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

Implementing Cisco Unified Wireless Network WLC (C9800-L)

Cisco Catalyst 9800-L Wireless Controller can be configured as a per PoP Wireless LAN Controller (WLC) with High Availability (HA) for managing CUWN Wi-Fi networks within a PoP. Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features from Cisco 3504 Wireless Controller. This section covers the initial installation and HA configuration of C9800-L WLC in a CCI PoP.

For more details on C9800-L controller, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/overview.html

For rack mounting and installing the C9800-L hardware, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Installing-the-Cisco-Catalyst-9800-L-Wireless-Controller.html

Once the WLC is rack mounted make sure the following:

1. The network interface cable or the optional Management port cable is connected.
2. The chassis is securely mounted and grounded.
3. The power and interface cables are connected
4. Terminal server is connected to the console port

Note: Install mode is the recommended mode to run the wireless controller.

Boot the controller in INSTALL mode:

Step1: Make sure to boot from flash:packages.conf (and you do not have other boot files specified in your config).

```
WLC(config)#no boot system
WLC(conf)#boot system flash:packages.conf
```

Step2: Software install image to flash. The install add file bootflash:<image.bin> activate commit command moves the switch from bundle-mode to install-mode where image.bin is our base image.

```
WLC#install add file <image.bin location> activate commit
```

Step3: Type **yes** to all prompts. When the install is complete, the controller reloads.

Verify:

After the controller reboot we can verify the current installation mode of the controller. Run **show version** to confirm.

```
WLC#show version | include System image
System image file is "bootflash:packages.conf"

WLC#show version | include Installation mode
Installation mode is INSTALL
```

For more details on WLC power up and initial configuration, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Power-Up-and-Initial-Configuration.html

Day-0 Manual Configuration Using the Cisco IOS-XE CLI:

C9800-L WLC is connected to one of our CCI PoP sites MGRoad C9300 FiaB Switch with 10G link.

This section shows you how to access the CLI to perform the initial configuration on the controller.

Step 1: Terminate the configuration wizard (this wizard is not specific for wireless controller):

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

Step 2: Press **Return** and continue with the manual configuration.

Step 3: Press **Return** to bring up the WLC> prompt and Type **enable to enter privileged EXEC mode**.:

```
WLC> enable
WLC#
```

Step 4: Enter the config mode and set the hostname:

```
WLC(config)#hostname WLC_C9800-L_1
```

Step 5: Configure login credentials:

```
WLC_C9800-L_1(config)#username <name> privilege 15 password 0 <pwd>
WLC_C9800-L_1(config)#enable secret <secret>
```

Step 6: Configure the underlay VLAN for wireless management interface. For example, vlan 199, IP: 10.10.199.199 with gateway 10.10.199.1 in underlay EIGRP 2000 AS.:

```
WLC_C9800-L_1(config)#vlan 199
WLC_C9800-L_1(config-vlan) #name WirelessVLAN
```

Step 7: Configure the SVI for wireless management interface:

```
WLC_C9800-L_1(config)#interface Vlan199
WLC_C9800-L_1(config-if)#ip address x.x.x.x 255.255.255.0
WLC_C9800-L_1(config-if)#no shutdown
WLC_C9800-L_1(config-if)#exit
```

Step 8: Configure the interface TenGigabitEthernet0/0/0 as trunk:

```
WLC_C9800-L_1(config)#interface TenGigabitEthernet0/0/0
WLC_C9800-L_1(config-if)#switchport mode trunk
WLC_C9800-L_1(config-if)#switchport trunk allowed vlan 199
WLC_C9800-L_1(config-if)#exit
```

Step 9: Configure a default route (or a more specific route) to reach the box:

```
WLC_C9800-L_1(config)#ip route 0.0.0.0 0.0.0.0 x.x.x.x
```

Step 10: Disable the wireless network to configure the country code:

```
WLC_C9800-L_1(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
WLC_C9800-L_1(config)#ap dot11 24ghz shutdown
```

```
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
```

Step 11: Configure the AP country domain. This configuration is what will trigger the GUI to skip the DAY 0 flow as the C9800 needs a country code to be operational:

```
WLC_C9800-L_1(config)#ap country IN
```

Step 12: Specify the interface to be the wireless management interface:

```
WLC_C9800-L_1(config)# wireless management interface vlan 199
```

Step 13: For the Controller to be discovered by the Cisco DNA Center or Prime Infrastructure, CLI,SSH, and SNMP credentials should be configured on the devices along with NETCONF.:

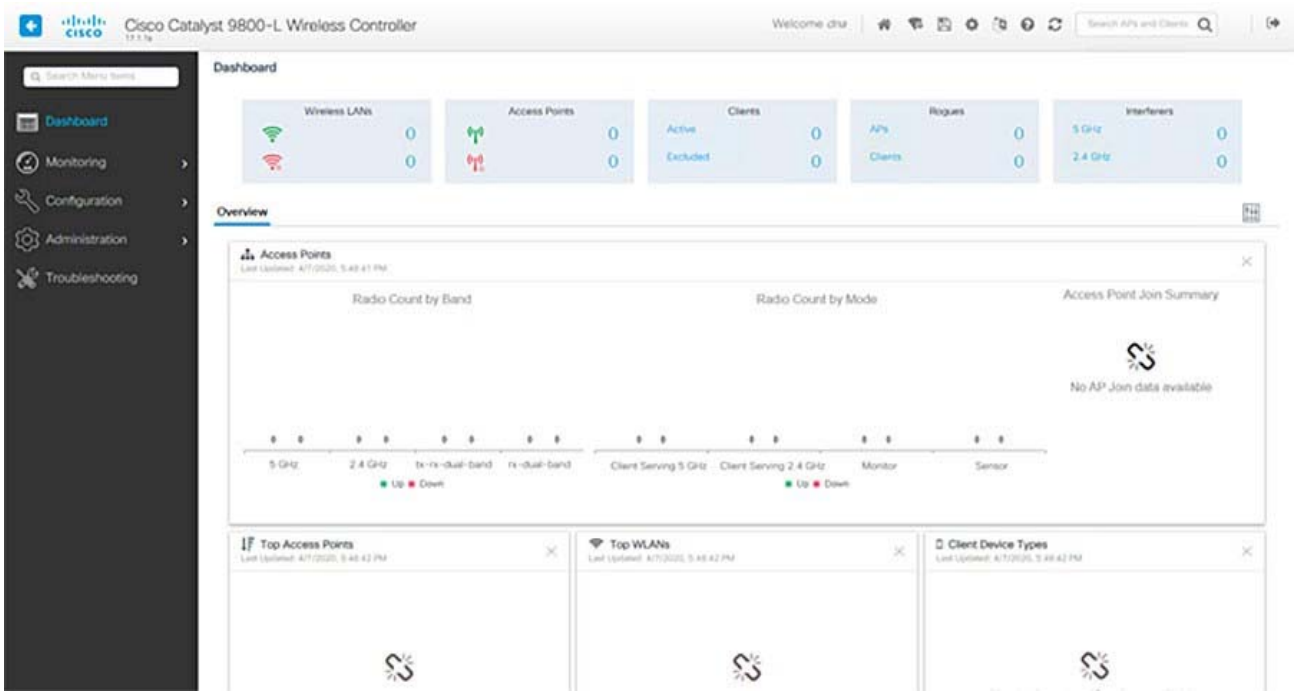
```
WLC_C9800-L_1(config)# crypto key generate rsa modulus 2048
WLC_C9800-L_1(config)# ip ssh version 2
WLC_C9800-L_1(config)# line vty 0 15
WLC_C9800-L_1(config-line)# login local
WLC_C9800-L_1(config-line)# transport input all
WLC_C9800-L_1(config-line)# transport preferred ssh

WLC_C9800-L_1(config)# snmp-server group default v3 priv
WLC_C9800-L_1(config)# snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
WLC_C9800-L_1(config)# snmp-server view SNMPv3All iso included
WLC_C9800-L_1(config)# snmp-server view SNMPv3None iso excluded
WLC_C9800-L_1(config)# snmp-server community <CommunityString> RW
WLC_C9800-L_1(config)# snmp-server user <username> default v3 auth md5 <password> priv aes 128
<password>

WLC_C9800-L_1(config)#ntp server x.x.x.x
WLC_C9800-L_1(config)#ip http server

WLC_C9800-L_1(config)#netconf-yang
```

Verify that we can ping the wireless management interface and then just https://<IP of the device wireless management interface>. Use the credentials you have entered earlier. Since the box has a country code configured, the GUI will skip DAY 0 page and you will get access to the main Dashboard for DAY 1 configuration.

Accessing C9800-L Web UI

Access the C9800 Web UI using https://<C9800-L-WLC-IP>. The username and password configured during the Day-0 configuration is used to log on to WLC Web UI.

Figure 50 Cisco 9800-L WLC Web UI Dashboard View



Cisco WLC (C9800-L) High Availability (HA) Configuration

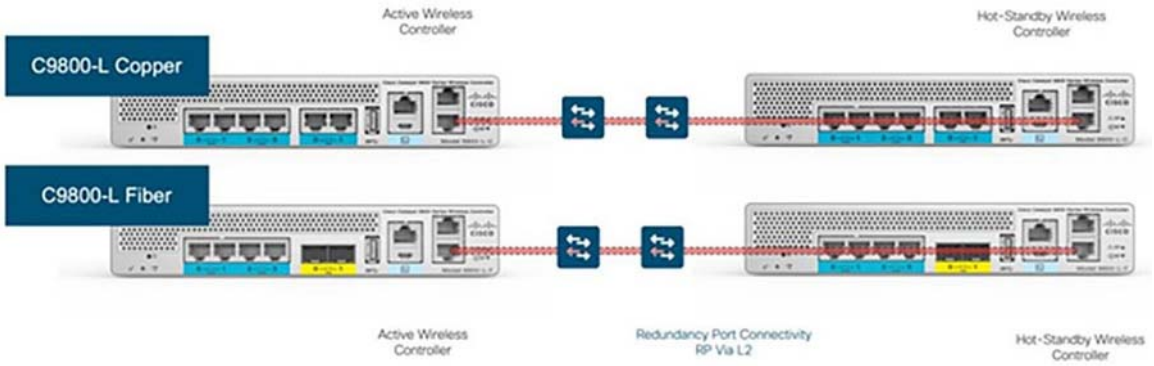
The HA Pair always has one active controller and one standby controller. If the active controller becomes unavailable, the standby assumes the role of the active. The Active wireless controller creates and updates all the wireless information and constantly synchronizes that information with the standby controller. If the active wireless controller fails, the standby wireless controller assumes the role of the active wireless controller and continues to the keep the HA Pair operational. Access Points and clients continue to remain connected during an active-to-standby switchover. Follow the steps below for configuring C9800-L WLC with HA in a PoP.

Note: Redundancy SSO is enabled by default but you still need to configure the communication between the boxes.

Step 1: Make sure both the C9800 WLCs are reachable to each other. Wireless management interface from both boxes must belong to the same VLAN and subnet. Connected to C9300 FiaB, one of our PoP sites in our case.

Step 2: Connect both 9800 WLC to each other through its RP port. Connecting C9800-L Wireless Controllers using RJ-45 RP Port for SSO:

Figure 51 C-9800-L WLC Redundancy Port Connections



Step 3: Provide the required redundancy configurations to both 9800 WLCs.

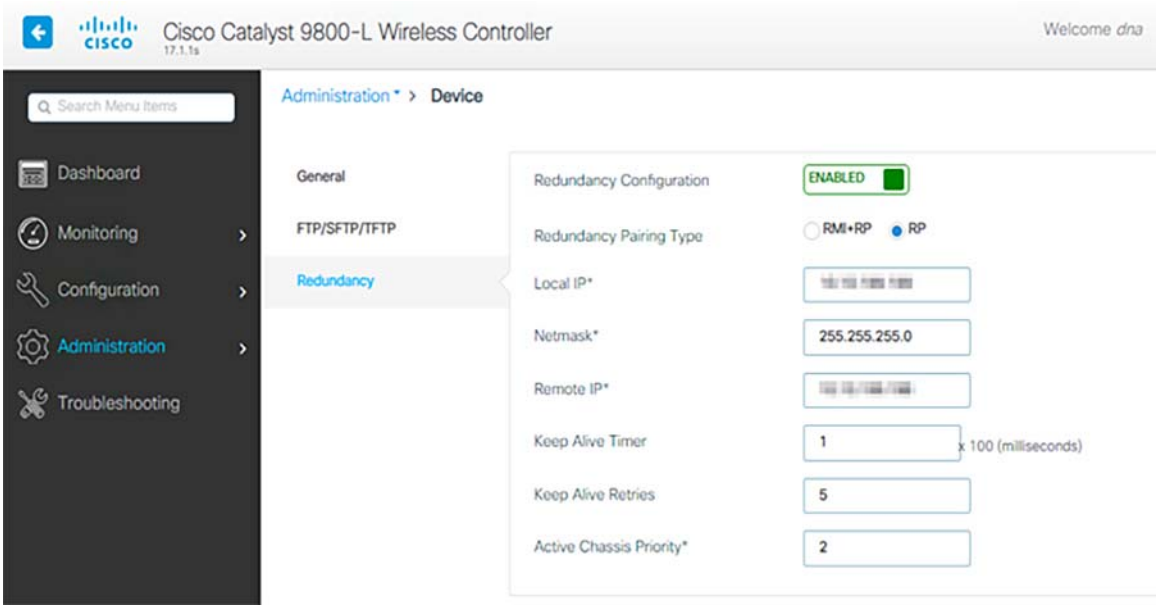
On WLC Web UI:

Navigate to **Administration-> Device-> Redundancy. Enable "Redundancy Configuration"**, check '**RP**' for "**Redundancy Pairing Type**" and enter the desired IP address along with the Active and Standby Chassis Priorities. Both boxes should have its own IP address, and both should belong to the same subnet.

On the Active controller, the priority is set to a higher value than the standby controller. The wireless controller with the higher priority value is selected as the active during the active-standby election process. If we do not choose a specific box to be active, the boxes themselves will elect Active based on lowest MAC address. The Remote IP is the IP address of the standby controller's redundancy port IP.

C9800-L WLC1 & C9800-L WLC2:

Figure 52 Redundancy Pairing on both C9800-L WLCs



CLI:

Configuring Chassis HA interface:

```
C9800-L-WLC# chassis redundancy ha-interface local-ip x.x.x.x /24 remote-ip x.x.x.x
```

Configure the priority of the specified device:

```
C9800-L-WLC# chassis 2 priority 2
```

Configure the peer keepalive timeout value:

```
C9800-L-WLC# chassis redundancy keep-alive timer 1
```

Configure the peer keepalive retry value before claiming peer is down.:

```
C9800-L-WLC# chassis redundancy keep-alive retries 5
```

Step 4: Save configurations on both 9800 WLCs and Reboot both boxes at the same time.

GUI:

Navigate to **Administration-> Reload**.

CLI:

```
C9800-40-WLC#reload
```

Verification:

Once both 9800 WLC rebooted and are synced to each other we can console into them and verify their current state with these commands:

```
WLC_C9800-L_1#show chassis
Chassis/Stack Mac Address : xxx.xxxx.xxxx  - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair
H/W Current
Chassis# Role Mac Address Priority Version State IP
---------------------------------------------------------------------------------------
*1     Active  xxx.xxxx.xxxx  2     V02   Ready  x.x.x.x
2      Standby xxx.xxxx.xxxx  1     V02   Ready  x.x.x.x
```

Enable Console Access to Standby 9800 WLC:

Once we enable HA and one of the boxes is assigned as active and the other one as standby hot, by default we are not allowed to reach exec mode (enable) on the standby box. To enable it, login by SSH/console to the active 9800 WLC and enter these commands:

```
# config t
# redundancy
# main-cpu
# standby console enable
# end
```

Force Switchover (Optional):

If we want to force a switchover between WLCs, you can either manually reboot the active 9800-L WLC or run this command:

```
# redundancy force-switchover
```

Configuring SD Access Wireless Embedded WLC on C9300 Stack

Integrating the Wireless with the SD Access brings the best of both the architectures like Simplifying the Control & Management Plane, optimizing the data plane and Integrating Policy & Segmentation end to end. This section covers the installation of Cisco Catalyst Embedded 9800 Wireless Controller (eWLC) on Catalyst 9K series Switches and bring up with Cisco DNA Center.

In CCI, Cisco Catalyst Embedded 9800 Wireless Controller (eWLC) is installed in PoP sites which require SD Access Wireless (Wi-Fi) on C9300 FiaB switch stack. Follow the steps below to configured eWLC on C9300 switch stack.

We will categorize this section into two parts:

- Installation of eWLC (c9800-sw) on C9300 FiaB PoP Site
- Enable Embedded SDA-Wireless through DNA Center Provisioning & AP Onboarding:

Installation of eWLC (c9800-sw) on C9300 FiaB PoP Site:

The steps to install eWLC on the C9300 FiaB switch are the following:

1. Check that license is dna-advantage.
2. Boot the switch in install mode.
3. Install the eWLC package.
4. Enable netconf-yang.

Step1: Check that license is dna-advantage.

For eWLC package to install properly you need to have the dna-advantage active on the switch. You can check this through show version command.

```
C9300-R-Stack#show version | b Technology
Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                 Technology-package
Current                       Type                    Next reboot
------------------------------------------------------------------------------
network-advantage       Smart License                 network-advantage
dna-advantage           Subscription Smart License    dna-advantage
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage
```

Step2: Boot the switch in install mode.

When we boot the switch passing directly the .bin image, this is called " bundle mode" . Packaging only works, when the switch is booted in " install mode" . To verify the mode, run " show version" :.

Make sure to boot from flash:packages.conf (there are no other boot files specified in our configuration):

```
C9300-R-Stack (config)#no boot system
C9300-R-Stack (conf)#boot system flash:packages.conf
```

a. Software install image to flash. The install add file bootflash:<image.bin> activate commit command moves the switch from bundle-mode to install-mode where image.bin is our base image.

```
C9300-R-Stack #install add file <image.bin location> activate commit
```

b. Type **yes** to all the prompt. Once the install is completed the switch proceeds to reload.

After the controller reboot, we can verify the current installation mode of the controller. Run the show version command in order to confirm.

```
C9300-R-Stack#show version | include System image
System image file is "flash:packages.conf"

C9300-R-Stack#show version | inc INSTALL
     1 41    C9300-24UX         17.1.1s           CAT9K_IOSXE           INSTALL
*    2 41    C9300-24UX         17.1.1s           CAT9K_IOSXE           INSTALL
```

Step3: Install the eWLC package.

After downloading the eWLC image to the switch you can install the wireless package using one single command line.

In our CCI, eWLC version installed is C9800-SW-iosxe-wlc.17.01.01s.SPA.bin

```
C9300-R-Stack#install add file flash:ewlc_pkg.bin activate commit
```

Where " flash:ewlc_pkg.bin" is our ewlc package. Alternatively, we can also install it from tftp directly.

Say " yes" to all questions. The switch should then reload and come up with ewlc package installed.

Verification:

After reloading we can confirm the install with the install summary command.:

```
C9300-R-Stack#sh install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
PKG   C    flash:C9800-SW-iosxe-wlc.17.01.01s.SPA.bin
IMG   C    17.1.1s.0.351

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Step4: Enable netconf-yang.

To enable NETCONF on the switch these three commands needs to be on the switch.

```
C9300-R-Stack# netconf-yang ------> Enable NETCONF/YANG globally. It may take up to 90 seconds to
initialize

C9300-R-Stack# aaa new-model

C9300-R-Stack# aaa authorization exec default local -----> Required for NETCONF-SSH connectivity
and edit-config operations
```

Verification:

We can check NETCONF is running with the following command.

```
C9300-R-Stack#show platform software yang-management process
confd : Running
nesd : Running
syncfd : Running
ncsshd : Running
dmiauthd : Running
```

```
nginx : Running
ndbmand : Running
pubd : Running
gnmib : Not Running
```

Enable Embedded SDA-Wireless through DNA Center Provisioning and AP Onboarding

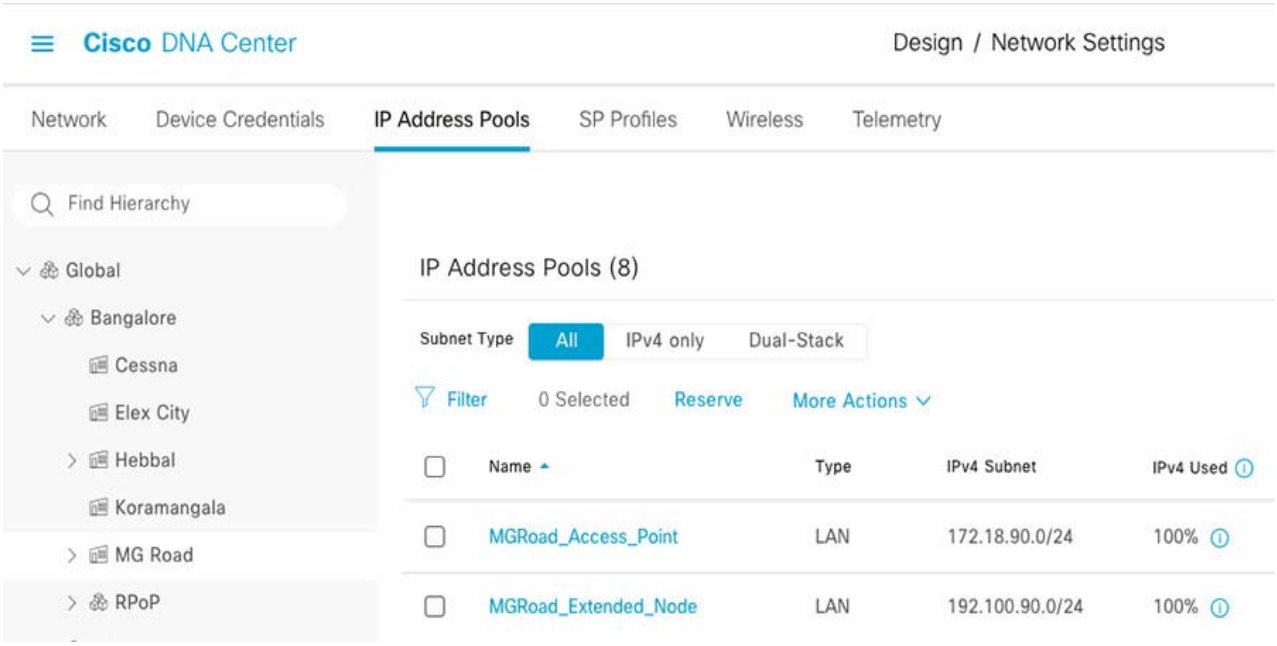
Prerequisites:

- Make sure we don't have a WLC in the site where you plan to enable Embedded SDA-Wireless.
- It is important that we do the discovery after we have installed the -wlc pkg otherwise DNACenter will not display the "embedded wireless" option in fabric view.
- Configure our AP IP pool and attach it to INFRA_VN. In that DHCP scope, point DHCP option 43 DNA Center with this PnP will discover the AP

Reserving IP Pool for Access Points:

Navigate to **Design-> Network Settings-> IP Address Pools**, for MG Road PoP Site reserve IP Pool for SDA Wireless Access Points, as shown in Figure 53.

Figure 53 AP IP Pool Reservation on Cisco DNA Center

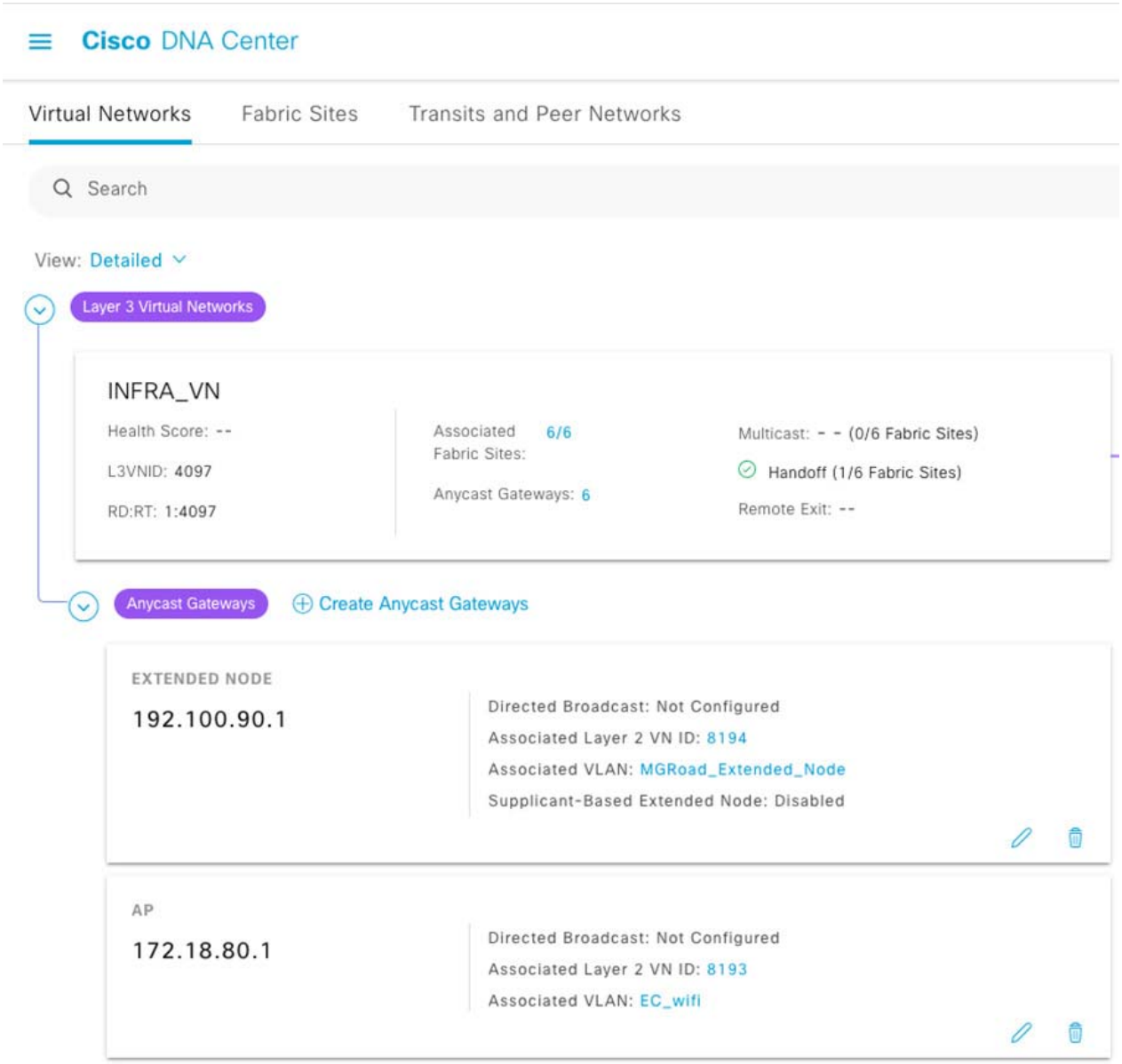


Attaching AP IP Pool to INFRA_VN:

Attach an AP IP pool to MGRoad Fabric Site by following the steps under "Add a Gateway to a Layer 3 Virtual Network" section in the following URL.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01110.html#task_zm2_sfl_1qb

Figure 54 Attaching AP Pool to INFRA_VN on Cisco DNA Center



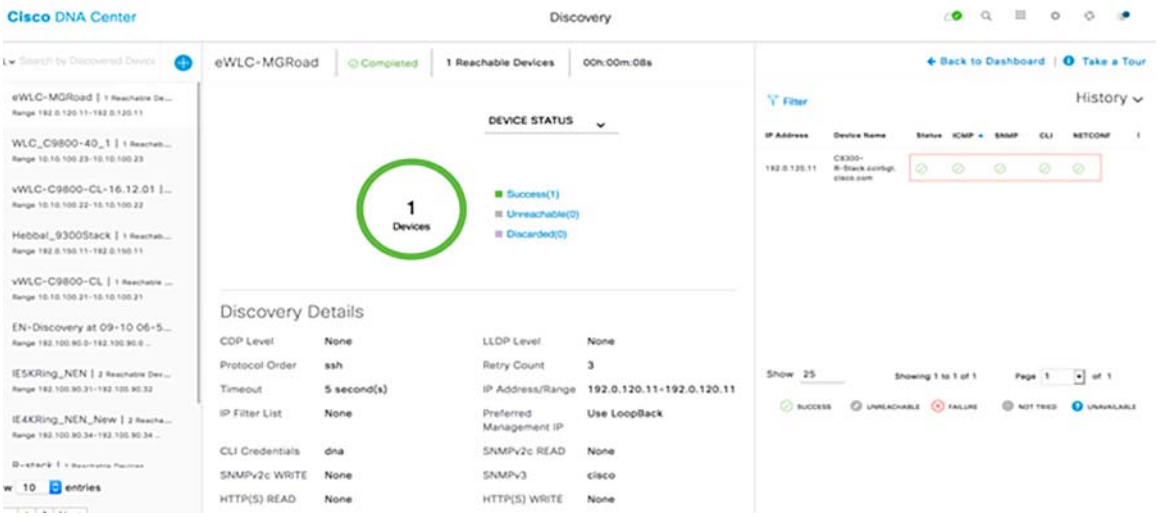
The workflow is as follows:

1. Discover device.
2. Assign to site.
3. Provision switch.
4. Add device as FiaB.
5. Enable Embedded wireless.
6. Provision AP (Will be added to DNAC automatically by joining the Catalyst 9800 WLC).

7. Configure onboarding SSID (refer to Implementing Wi-Fi Access Network, page 156).

   a. When configuring the discovery properties, click the add credentials and configure the NETCONF port to 830.

Figure 55 eWLC Discovery on Cisco DNA Center

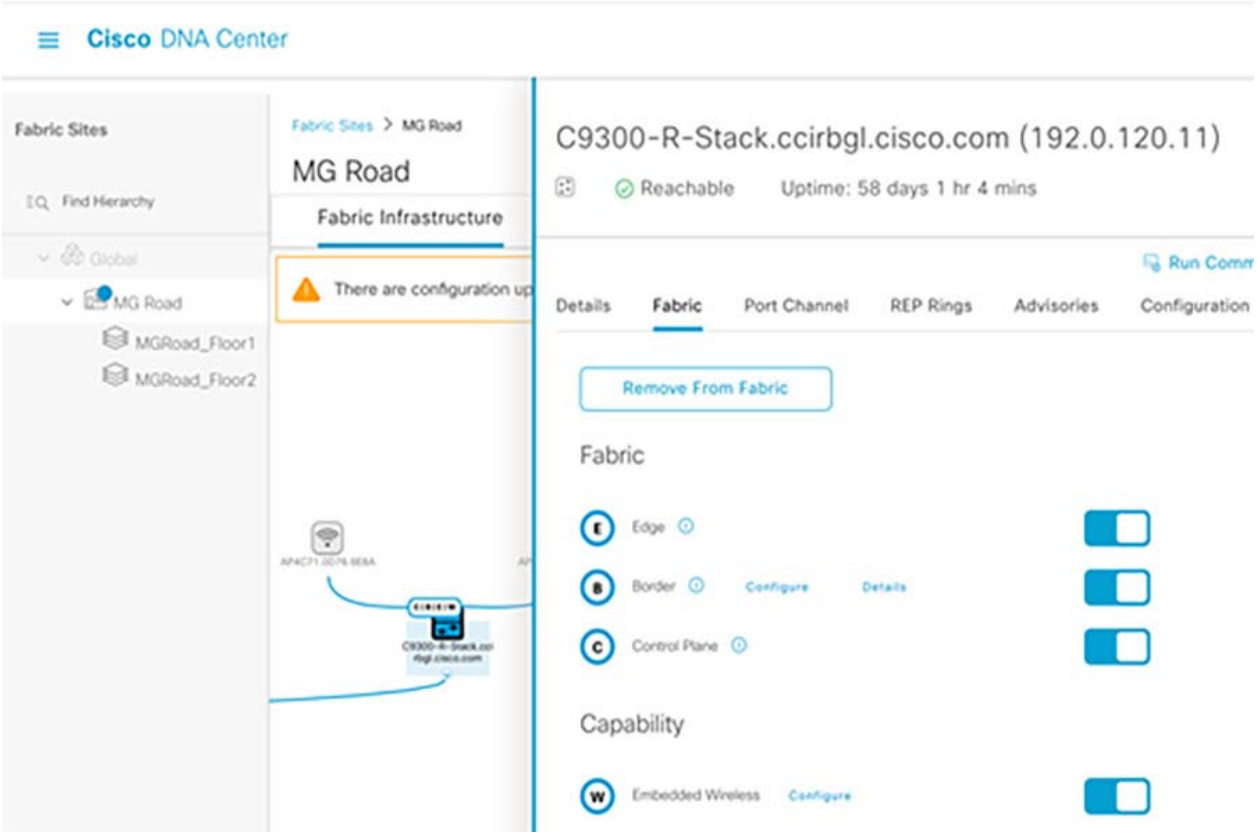


   b. Assign the switch to MGRoad PoP Site.

   c. Provision the device. Refer to Provisioning Devices in SD-Access, page 73 for the device provisioning steps.

   d. Add the device as Fabric in a Box (configure as Border, Control, and Edge Node) and Enable Embedded Wireless.

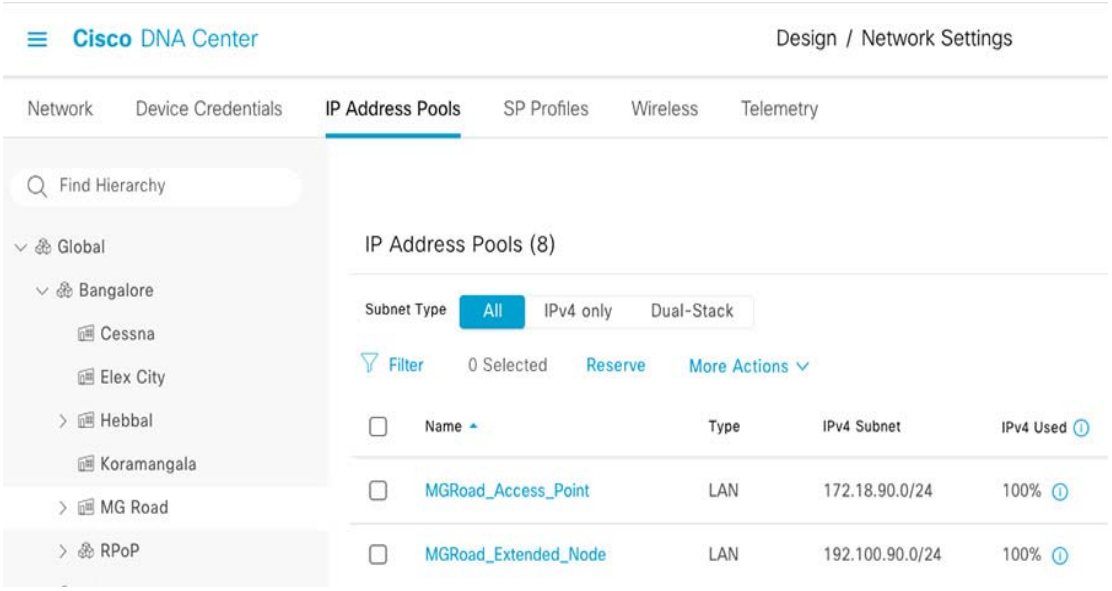
Figure 56 Enabling Embedded Wireless on FiaB Switch



e. Connect the SDA Wireless APs connect to either Fabric Edge (FE) ports, or Extended Node (EN) ports. It is recommended to resync of the switch for it to add the AP. Go to **Provision-> Inventory**, select the switch from the site, and resync the switch. The APs will be shown in the Devices tab for us to assign to our eWLC site and provision.

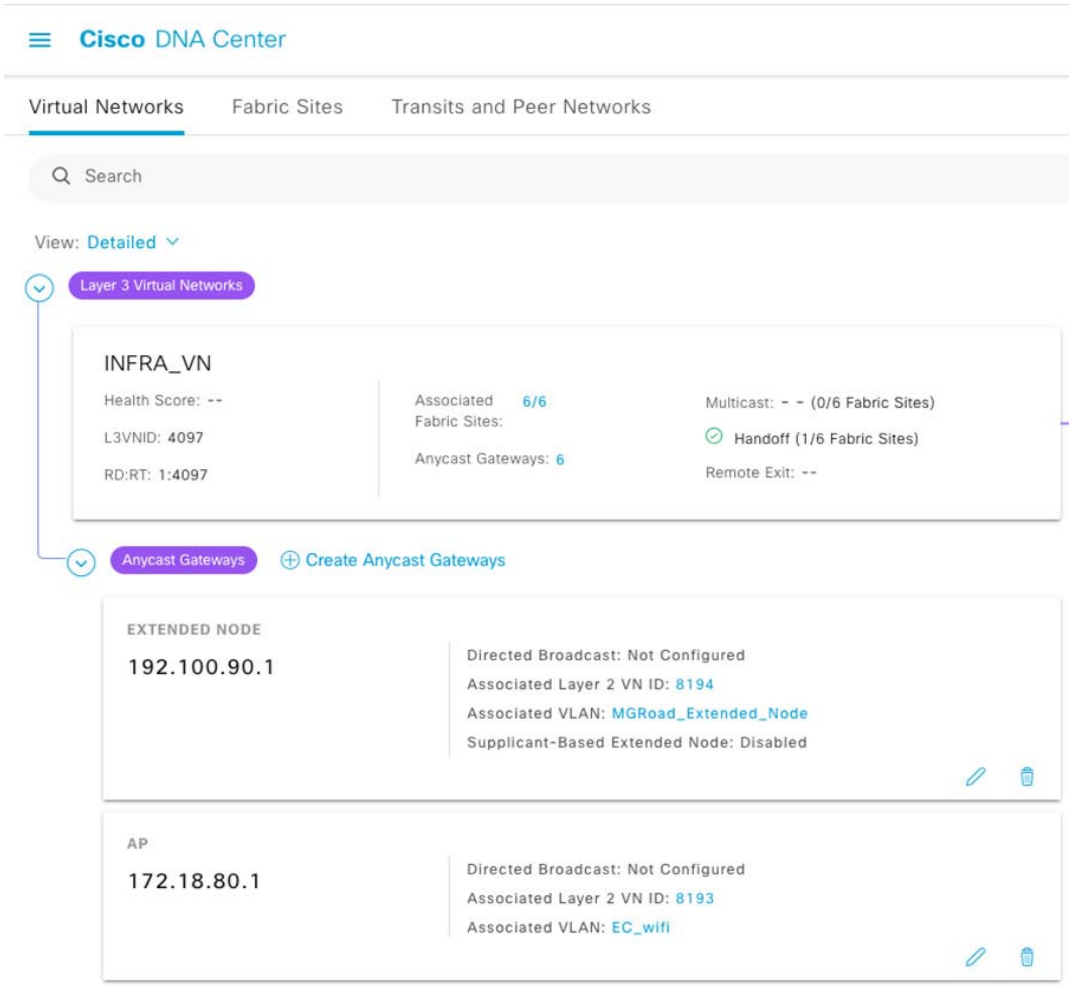
Note: Latency between AP and WLC needs to be < 20 ms.

Figure 57 AP IP Pool Reservation on Cisco DNA Center



Note: To assign the APs to the Site, Floors should be created under the Building under Network Hierarchy.

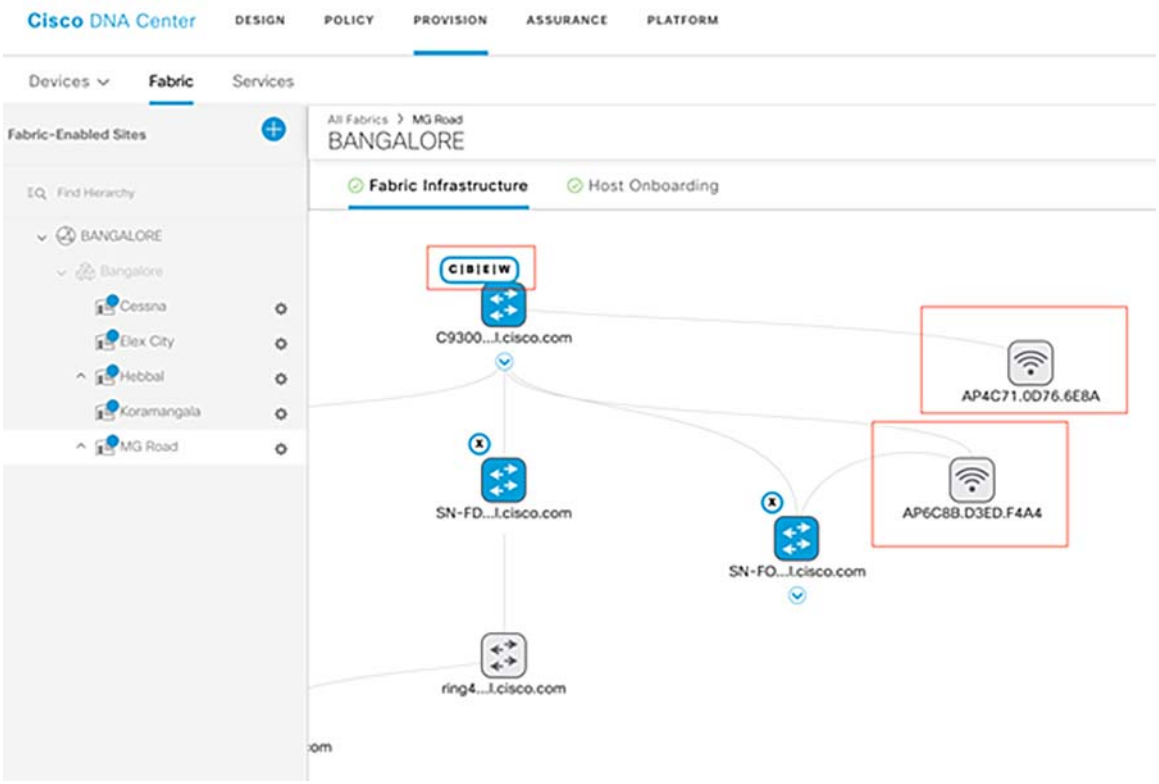
Figure 58 Attaching AP Pool to INFRA_VN on Cisco DNA Center



Note: By default, the RF profile that you is marked as default under Design > Network Settings > Wireless > Wireless Radio Frequency Profile is selected in the RF Profile drop-down list. You can change the default RF Profile value for an AP by selecting a value from the RF Profile drop-down list. The options are: High, Typical, and Low. The AP group is created based on the RF profile selected.

For verifying successful provisioning of SD Access Wireless on C9300 Stack in a PoP site, navigate to Provision -> SD Access-> Fabric Infrastructure view as shown in Figure 59.

Figure 59 SD Access Wireless AP View on Fabric Infrastructure



Implementation of PoP (Fabric) Sites Interconnection

This section covers the implementation of the backhaul network for interconnecting fabric sites (PoPs). It is mandatory to configure the underlay network connectivity between the Fabric Border (FiaB) and the backhaul network (Enterprise Ethernet or MPLS) as mentioned in Underlay Network Implementation, page 20. Fabric sites can be interconnected either using SD-Access Transit or IP-based Transit, which is implemented depending on the CCI backhaul network.

Note: This section provides example configurations for Private Ethernet and MPLS-based network backhauls implemented in this solution validation, as shown in Figure 3 and Figure 4.

This section includes the following major topics:

PoP Interconnection over Ethernet Network Backhaul

This section covers the example configuration of fabric interconnection for the SD-Access Transit-based network topology shown in Figure 3.

When configuring the interfaces on a fabric border to communicate with SD-Access transit, Cisco DNA will configure a VRF for each VN in the fabric site Border (i.e., FiaB and Transit Control Plane (T-CP) nodes). BGP peering is configured between the T-CP node and FiaB to enable overlay routing. In this implementation, two Cisco Catalyst 9500 switches as Ethernet network backhaul are provisioned as " SD-Access Transit" T-CP nodes, as shown in Figure 19. When connecting fabric sites to a SD-Access Transit network, each VN with subnets configured for data traffic is created as a VRF in FiaB and VN subnet(s) network prefixes for data traffic are registered with T-CP nodes in the SD-Access Transit site.

Example FiaB VRF Configuration:

```
vrf definition SnS_VN
  rd 1:4099
  !
  address-family ipv4
    route-target export 1:4099
    route-target import 1:4099
  exit-address-family
```

Cisco DNA Center automatically configured the BGP peering between the FiaB Border and SD-Access Transit Control Plane nodes (i.e., Cisco Catalyst 9500 switches in this implementation) using lookback interfaces configured (routing enabled in the underlay network) on these devices. It leverages the existing underlay physical interfaces/network connectivity to backhaul network. Therefore, no separate physical interface selection is required.

Note: P subnet pools configured for extended nodes are added in the Global Routing Table (GRT) address family in the BGP routing configuration outside of the VRF address family.

Example FiaB Border BGP Routing Automatically Configured by Cisco DNA Center

```
router bgp 90
  bgp router-id interface Loopback0
  bgp log-neighbor-changes
  bgp graceful-restart
  neighbor 192.0.130.11 remote-as 65540
  neighbor 192.0.130.11 ebgp-multihop 255
  neighbor 192.0.130.11 update-source Loopback0
  neighbor 192.0.130.12 remote-as 65540
  neighbor 192.0.130.12 ebgp-multihop 255
  neighbor 192.0.130.12 update-source Loopback0
  !
```

```
  address-family ipv4
    bgp aggregate-timer 0
    network 192.0.120.11 mask 255.255.255.255
    network 192.100.90.0
    aggregate-address 192.100.90.0 255.255.255.0 summary-only
    redistribute lisp metric 10
    neighbor 192.0.130.11 activate
    neighbor 192.0.130.11 send-community both
    neighbor 192.0.130.12 activate
    neighbor 192.0.130.12 send-community both
  exit-address-family
  !
  address-family vpnv4
    bgp aggregate-timer 0
    neighbor 192.0.130.11 activate
    neighbor 192.0.130.11 send-community both
    neighbor 192.0.130.12 activate
    neighbor 192.0.130.12 send-community both
  exit-address-family
  !
  address-family ipv4 vrf SnS_VN
    bgp aggregate-timer 0
    network 172.10.90.0 mask 255.255.255.0
    aggregate-address 172.10.90.0 255.255.255.0 summary-only
    redistribute lisp metric 10
  exit-address-family
```

Example SD-Access Transit Control Plane Node BGP Routing Automatically Configured by Cisco DNA Center

```
router bgp 65540
  bgp router-id interface Loopback0
  bgp log-neighbor-changes
  bgp graceful-restart
  neighbor 192.0.120.11 remote-as 90
  neighbor 192.0.120.11 ebgp-multihop 255
  neighbor 192.0.120.11 update-source Loopback0
  !
  address-family ipv4
    redistribute lisp metric 10
    neighbor 192.0.120.11 activate
    neighbor 192.0.120.11 send-community both
    neighbor 192.0.120.11 route-map deny-all in
    neighbor 192.0.120.11 route-map tag_transit_eids out
  exit-address-family
  !
  address-family vpnv4
    neighbor 192.0.120.11 activate
    neighbor 192.0.120.11 send-community both
    neighbor 192.0.120.11 route-map deny-all in
    neighbor 192.0.120.11 route-map tag_transit_eids out
  exit-address-family
  !
  address-family ipv4 vrf SnS_VN
    redistribute lisp metric 10
  exit-address-family
```

PoP Interconnection via IP Transit over MPLS Network Backhaul

When configuring the interfaces on a fabric border to communicate with an IP transit, the Cisco DNA Center will configure a VRF for each VN in the fabric site. This is known as VRF-lite because the VRFs are only locally significant. When connecting to an MPLS backhaul, the provider will use its own VRFs to keep different customers' traffic separated. Using a VRF-aware routing protocol within the service provider gives them the ability to keep the VRF configuration at the

service provider edge instead of every single device in the core. These VRFs, however, are not related to the VRFs configured on the fabric border. To maintain the macro-segmentation provided by a VN's use of VRFs between fabric sites over an IP transit, the service provider must also provide a VRF for each VN configured at a fabric site.

Example Provider Edge VRF Configuration

```
vrf definition cci-roadways-iteris
 rd 23:23
 !
 address-family ipv4
  route-target export 23:23
  route-target import 23:23
 exit-address-family
```

When configuring the border services, Cisco DNA will automatically configure a VLAN interface on the border node. When configuring the provider edge node, there must be a matching VLAN configuration to enable connectivity. The border configuration is shown in Figure 60.

Figure 60 Border Node External Interface

On the provider edge interface facing the edge fabric border, the services are separated using a different service instance. Each service instance is then associated with a bridge domain interface. For ease of administration, the VLAN encapsulation and bridge-domain should match. If the IP transit is owned by a different operator, they will have to ensure the encapsulation matches the VLAN configured on the fabric border.

```
interface GigabitEthernet0/0/4
 service instance 3008 ethernet
  encapsulation dot1q 3008
  rewrite ingress tag pop 1 symmetric
  bridge-domain 3008

interface BDI3008
 vrf forwarding cci-roadways-iteris
 ip address 172.16.1.14 255.255.255.252
```

The VRF is also added to the service provider's BGP configuration:

```
address-family ipv4 vrf cci-roadways-iteris
  redistribute connected
  neighbor 172.16.1.13 remote-as 65003
  neighbor 172.16.1.13 activate
```

A service provider interface will be connected to the data center (fusion router, in this implementation) and this must have all the VRFs configured to maintain segmentation end to end. Because these devices are not part of the fabric, the configuration must be done manually.

Provider Edge VRF facing the fusion router:

```
vrf definition cci-roadways-iteris
 rd 23:23
 !
 address-family ipv4
  route-target export 23:23
  route-target import 23:23
```

Since the VLAN encapsulation is not automatically generated by Cisco DNA for this connection, there are no mandates on the VLAN other than what the service provider may require:

```
interface GigabitEthernet0/3/4
 service instance 23 ethernet
  encapsulation dot1q 23
  rewrite ingress tag pop 1 symmetric
  bridge-domain 23

interface BDI23
 vrf forwarding cci-roadways-iteris
 ip address 10.2.1.30 255.255.255.252
```

The VRF is then added to the service provider's BGP configuration:

```
 address-family ipv4 vrf cci-roadways-iteris
  neighbor 10.2.1.29 remote-as 65001
  neighbor 10.2.1.29 activate
```

A complementary configuration also exists on the customer edge device (fusion router, in this implementation):

```
interface GigabitEthernet0/0/0.23
 encapsulation dot1Q 23
 vrf forwarding Iteris
 ip address 10.2.1.29 255.255.255.252
```

Because the VRF separation is maintained within the IP transit network, the VN will maintain its macro-segmentation from one fabric site to another.

Configuring Fusion Router

When fabric traffic needs to cross over between user-defined VRFs or services that are shared by fabric and non-fabric devices, it must be manually routed by a non-fabric device. These shared services include, but aren't limited to, Cisco DNA, ISE, DHCP, WLC, and NTP. The shared services can be in the GRT or a separate VRF. This routing device is known as a fusion router because it fuses together traffic from different VRFs or a VRF and the GRT. This process involves leaking the appropriate routes between VRFs or the GRT. VRF import/export statements and route maps can limit the routes leaked between services.

This section covers the following two example implementations of the fusion router for the network topologies, as shown in Figure 4 and Figure 19. Depending on the deployment topology/backhaul network, you can choose to implement either of the configurations:

- Configuring a Fusion Router in IP-Based Transit Network, page 97
- Configuring a Fusion Router in SD-Access Transit Network, page 99

For more details about fusion routers, route leaking, and step-by-step instructions for configuring a fusion router, refer to the section " About Fusion Routers" in the *Software-Defined Access for Distributed Campus Deployment Guide* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487404

Configuring a Fusion Router in IP-Based Transit Network

For the IP Transit scenario, a Cisco ASR 1000 Series Router was used as the fusion router, but the only requirement is that the router must support route leaking between VRFs. In this implementation, the shared services were part of the global routing table, but they could also be part of a separate shared services VRF.

1. The fusion router configuration is outside the scope of Cisco DNA and must therefore be done manually. The first step is to configure a VRF for every VN configured in Cisco DNA.

```
vrf definition Iteris
 rd 1:9
 !
 address-family ipv4
  route-target export 1:9
  route-target import 1:9
 exit-address-family
```

2. The fusion router must then have interfaces configured in the VRF, which can connect to a fabric border node or other non-fabric router. In the case of a fabric border node, Cisco DNA will configure the interface and BGP configuration as part of the border configuration. The fusion router side must be done manually. The following is an example of the automatically generated border node interface configuration:

```
interface Vlan3001
 description vrf interface to External router
 vrf forwarding Iteris
 ip address 172.16.0.1 255.255.255.252
 no ip redirects
 ip route-cache same-interface
end
```

3. The following is the complementary interface configuration manually entered on the fusion router:

```
interface TenGigabitEthernet0/2/0.3001
 encapsulation dot1Q 3001
 vrf forwarding Iteris
```

```
 ip address 172.16.0.2 255.255.255.252
end
```

4. Cisco DNA also automatically generates the BGP config for the VRF on the border node:

```
router bgp 65000
 address-family ipv4 vrf Iteris
  bgp aggregate-timer 0
  network 172.16.5.1 mask 255.255.255.255
  aggregate-address 172.16.5.0 255.255.255.192 summary-only
  redistribute lisp metric 10
  neighbor 172.16.0.2 remote-as 65001
  neighbor 172.16.0.2 update-source Vlan3001
  neighbor 172.16.0.2 activate
  neighbor 172.16.0.2 weight 65535
 exit-address-family
```

5. The fusion router must be manually configured to successfully neighbor with the border node:

```
router bgp 65001
 address-family ipv4 vrf Iteris
  redistribute connected
  neighbor 172.16.0.1 remote-as 65000
  neighbor 172.16.0.1 activate
 exit-address-family
```

6. Because the VRF creates a routing table separate from the GRT, routes must be shared between them for the VRF to have access to the shared services, and vice versa. One way to achieve this is with prefix lists and route maps.

   Example from fusion router:

```
! Permit subnet for shared services (DNA, ISE, DHCP, etc)
ip prefix-list shared-services-to-vrf seq 5 permit 10.0.1.0/24
! Permit loopback IP of fusion router
ip prefix-list shared-services-to-vrf seq 10 permit 100.0.0.100/32
!
! Route map matches on prefix-list
route-map shared_map permit 10
 match ip address prefix-list shared-services-to-vrf
```

7. The route-map must then be imported into the target VRF:

```
vrf definition Iteris
 !
 address-family ipv4
  import ipv4 unicast map shared_map
```

8. Verifying the routes on a fabric site:

```
Routing Table: Iteris
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
B        10.0.1.0/24 [20/0] via 172.16.0.2, 2w1d
      100.0.0.0/32 is subnetted, 1 subnets
B        100.0.0.100 [20/0] via 172.16.0.2, 2w1d
```

9. Additionally, routes from the VRF must be exported to the GRT so the shared services can reach interfaces in the VRF:

```
! Border subnet between fusion router and fabric border
ip prefix-list iteris-to-global seq 25 permit 172.16.0.0/30
! Subnet for IP pool configured in Cisco DNA
ip prefix-list iteris-to-global seq 54 permit 172.16.5.64/26
!
! Route map matches on prefix-list
route-map iteris_map permit 10
```

```
 match ip address prefix-list iteris-to-global
```

10. The route map must then be exported from the target VRF:

```
vrf definition Iteris
 !
 address-family ipv4
  export ipv4 unicast map iteris_map
```

11. Verifying the routes on the fusion router:

```
sh ip route | inc Iteris

B        172.16.5.64/26 [20/0] via 10.2.1.34 (Iteris), 02:06:17
```

Configuring a Fusion Router in SD-Access Transit Network

Implementation of fusion routers in SD-Access Transit-based network topology (Figure 3) is similar to IP-based Transit since both network topologies connect to fusion routers via the IP Transit network. In this implementation, an IP Transit network interconnects a HQ/DC site with an external network outside of fabric overlay in order to provide access to shared services. Therefore, steps to configure the fusion router is similar to what was described in the previous section.

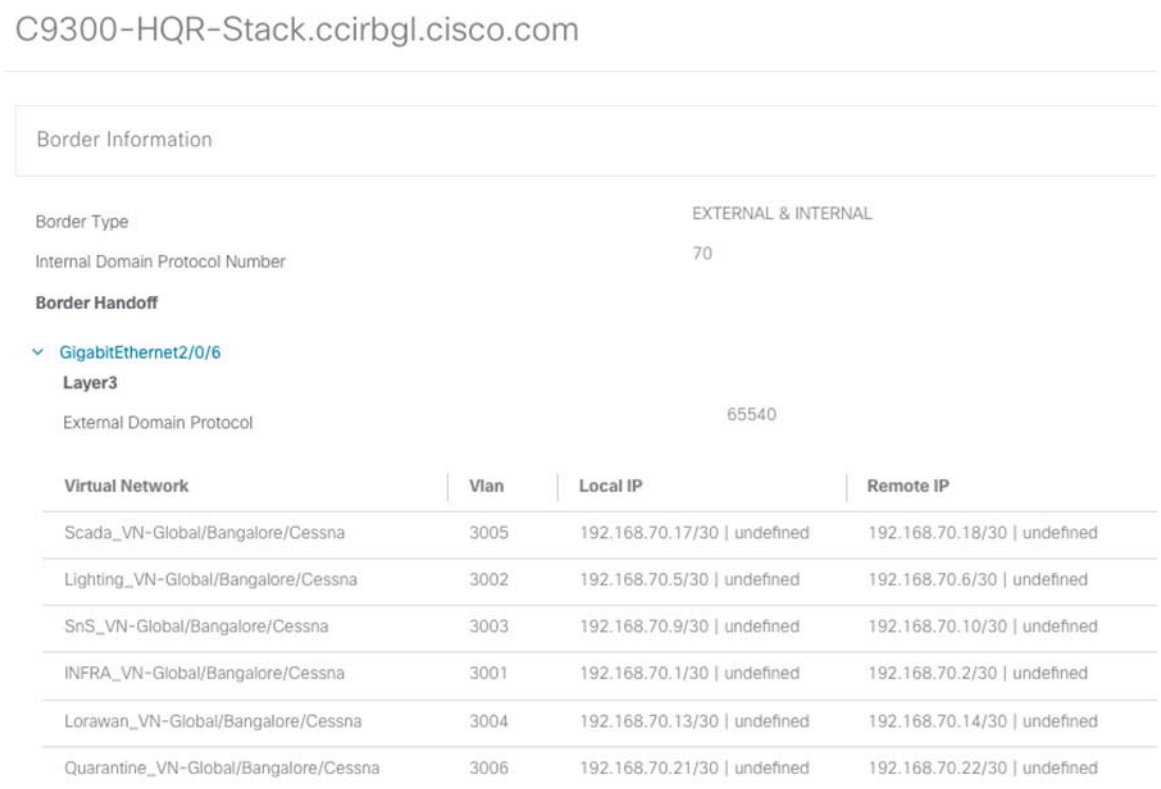
This section discusses an example implementation of redundant fusion routers in HQ/DC site, as shown in Figure 19, for a CCI implementation (with an SD-Access Transit-based network topology). A couple of Cisco Cloud Services Routers 1000V are used as redundant fusion routers in this implementation.

1. Configure VRF for every VN configured in Cisco DNA Center on the fusion router. Example VRF configuration:

```
vrf definition SnS_VN
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

Figure 61 shows an example VLAN automatically created by the Cisco DNA Center Border while FiaB role provisioning.

Figure 61 Example Border Configuration for Connecting to IP Transit



2. In Figure 61, GigabitEthernet2/0/6 is a physical link connecting to a fusion router (CSR1000V-1 used as fusion router) and GigabitEthernet1/0/6 is a physical link to redundant (secondary) fusion router (CSR1000V-2). Example VLAN configurations automatically configured by the Cisco DNA Center on HQ/DC Site FiaB border:

```
interface Vlan3001                  # Vlan for INFRA_VN in Gloabal Routing Table
 description vrf interface to External router
 ip address 192.168.70.1 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3002 # Vlan for SnS_VN in VRF Routing Table
 description vrf interface to External router
 vrf forwarding SnS_VN
 ip address 192.168.70.5 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
```

3. Configure complementary interface configurations matching this VLAN interfaces on the fusion router:

```
interface GigabitEthernet5
 description connected to 9300-HQ-Stack on port Gi 2/0/6
 no ip address
 negotiation auto
 cdp enable
 no mop enabled
 no mop sysid
!
interface GigabitEthernet5.3001
 encapsulation dot1Q 3001
```

```
 ip address 192.168.70.2 255.255.255.252
!
interface GigabitEthernet5.3003
 encapsulation dot1Q 3003
 vrf forwarding SnS_VN
 ip address 192.168.70.10 255.255.255.252
!
```

4. Cisco DNA Center automatically generates the BGP config for the VRF (SnS_VN) and INFRA_VN on the border node:

```
router bgp 70

bgp router-id interface Loopback0 bgp log-neighbor-changes
bgp graceful-restart

neighbor 192.168.70.2 remote-as 65540
neighbor 192.168.70.2 update-source Vlan3001
!

address-family ipv4
network 192.0.140.11
mask 255.255.255.255

redistribute lisp metric 10
neighbor 192.0.130.11
 activate
neighbor 192.0.130.11
 send-community both
neighbor 192.0.130.12
 activate
neighbor 192.0.130.12
 send-community both
neighbor 192.168.70.2
 activate
neighbor 192.168.70.2
 weight 65535
neighbor 192.168.70.2
 advertisement-interval 0
exit-address-family
!

address-family ipv4 vrf SnS_VN
 bgp aggregate-timer 0
 network 172.15.70.0mask 255.255.255.0
 network 172.16.70.0mask 255.255.255.0
 network 192.168.70.8mask 255.255.255.252
 aggregate-address 172.16.70.0255.255.255.0 summary-only
 aggregate-address 172.15.70.0255.255.255.0 summary-only
 redistribute lisp metric 10
 neighbor 192.168.70.10 remote-as 65540
 neighbor 192.168.70.10 update-source Vlan3003
 neighbor 192.168.70.10 activate
 neighbor 192.168.70.10 weight 65535
exit-address-family
```

5. The fusion router must be manually configured to successfully neighbor with the border node:

```
router bgp 65540

bgp log-neighbor-changes

neighbor 192.168.70.1 remote-as 70
```

```
!

address-family ipv4
bgp redistribute-internal
network 192.168.70.0 mask 255.255.255.252 redistribute connected
redistribute static
neighbor 192.168.70.1 activate
neighbor 192.168.70.1 allowas-in
neighbor 192.168.70.1 soft-reconfiguration inbound
distribute-list 1 out
exit-address-family

!
address-family ipv4 vrf SnS_VN
network 192.0.50.11 mask 255.255.255.255
network 192.168.70.8 mask 255.255.255.252

redistribute connected
redistribute static
neighbor 192.168.70.9 remote-as 70
neighbor 192.168.70.9 update-source GigabitEthernet5.3003
neighbor 192.168.70.9 activate
neighbor 192.168.70.9 allowas-in
neighbor 192.168.70.9 soft-reconfiguration inbound
exit-address-family
```

6. Configure prefix-lists and to match shared services network routes:

```
ip prefix-list SHARED_SERVICES_NETS seq 1 permit 10.10.100.0/24
```

7. Configure route-map to import shared services network into the target VRF:

```
route-map SS-NETWORK-TO-VRF permit 10
 match ip address prefix-list SHARED_SERVICES_NETS
```

8. The route-map must then be imported into the target VRF. Example configuration for a VN (SnS_VN):

```
vrf definition SnS_VN
 rd 1:4099
 !
 address-family ipv4
  import ipv4 unicast map SS-NETWORK-TO-VRF
```

9. Verifying the routes on a fabric site (for example, on the HQ/DC site):

```
C9300-HQR-Stack#sh ip route vrf SnS_VN
Routing Table: SnS_VN
<Snip>
Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 2 subnets
B        10.10.100.0 [20/0] via 192.168.70.8, 03:59:24
```

10. Additionally, routes from the VRF must be exported to the GRT so that the shared services can reach interfaces in the VRF:

```
! IP Transit Border Handoff subnet pool, VRF subnet(s) prefixes (SnS_VN)
ip prefix-list CESSNA_SnS_VN_ROUTES seq 25 permit 192.168.70.0/30
ip prefix-list CESSNA_SnS_VN_ROUTES seq 26 permit 192.168.70.8/30
ip prefix-list CESSNA_SnS_VN_ROUTES seq 27 permit 192.100.90.0/24
ip prefix-list CESSNA_SnS_VN_ROUTES seq 29 permit 172.16.70.0/24
!
! Route-map matching the prefixes-list
route-map SnS-VN-TO-GLOBAL permit 10
```

```
 match ip address prefix-list CESSNA_SnS_VN_ROUTES
```

11. The route map must then be exported from the target VRF:

```
vrf definition SnS_VN
 rd 1:4099
 !
 address-family ipv4
    export ipv4 unicast map SnS-VN-TO-GLOBAL
```

12. Verify the routes on the fusion router:

```
FR-CSR1KV-1#sh ip route | inc SnS_VN
B        172.16.70.0 [20/0] via 192.168.70.5 (SnS_VN), 04:09:56
```

13. This completes the fusion routing configuration on CSR1000v-1. Repeat the same steps for the secondary fusion router (CSR1000v-2) in the network.

Note: Shared services network prefixes are advertised to other fabric sites (PoP) via Control Plane nodes (SD-Access Transit) BGP neighborship between all PoP sites border and Transit Site control plane nodes.

Configuring Internet Connectivity

Regardless of how the rest of the network itself is designed or deployed outside of the fabric, a few things are going to be in common in deployments due to the configuration provisioned by the Cisco DNA Center. Providing Internet access to PoP (fabric) site devices is one of such common use cases to be provisioned in the deployments. In the CCI network, Internet access to PoP sites are configured on the fusion router that connects to DMZ network as **Internet Edge**.

Refer to the following URL for mode details on different types for fabric border.

- https://community.cisco.com/t5/networking-documents/guide-to-choosing-sd-access-sda-border-roles-in-cisco-dnac-1-3/ta-p/3889472

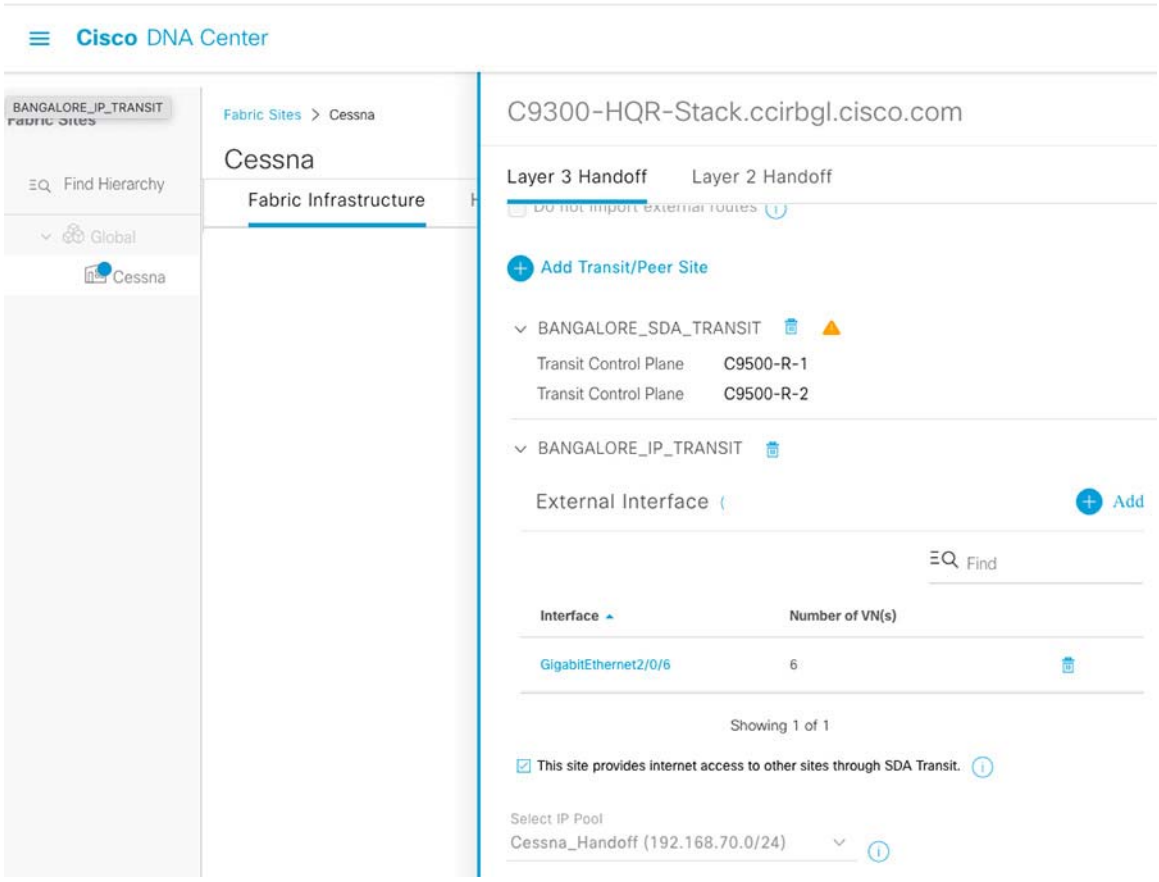
In the SD-Access Transit based network topology as shown in Figure 3, the fusion routers (CSR1000V) are acting as Internet edges to HQ/DC site FiaB. Alternatively, on IP based Transit network topology, as shown in Figure 4, a couple of Catalyst 9500 switches as fusion routers are the Internet Edges.

This section covers an example implementation of configuring Internet access to PoP sites via HQ/DC site which is connected to Internet edge as shown in Figure 3. The FiaB border in HQ/DC site will have the SD-Access network prefixes in its VRF routing tables. As a prerequisite for being “connected-to-Internet,” it will also have a default route to its next hop (fusion router as Internet edge) in its Global Routing Table.

Note: Make sure that in order to provide Internet access to other SD-Access Transit-connected PoP (Fabric) sites, the Fabric Border which connects to your network Internet edge is configured with the **Connected to the Internet** checkbox enabled.

In this implementation, the HQ/DC site border (FiaB) connects to the Internet edge and provides Internet access to other PoP sites via SD-Access network. Therefore, the border is configured with the **Connected to the Internet** checkbox enabled.

Figure 62 Example Border Configuration for Internet Connectivity



The fusion router as Internet edge has the default route in its GRT to the next-hop of the Internet (i.e., FirePower2140 in DMZ network in this implementation).

Default static route in underlay network on fusion router:

```
ip route 0.0.0.0 0.0.0.0 10.10.204.1   #Next hop interface on Firepower in DMZ
```

This default route must be advertised from the GRT to the VRFs. This allows packets to egress the fabric domain towards the Internet. In addition, the SD-Access prefixes in the VRF tables on the border nodes must be advertised to the external domain (outside of the fabric domain) to draw (attract) packets back in.

These SD-Access network prefixes are already configured in fusion routers; however, they must be added in the Firepower configuration. For detailed Firepower implementation in DMZ network in this implementation, refer to the 3.Configure Static and Dynamic Routing:, page 372. It includes, the configuration required to enable Internet access for endpoints/devices in the PoP sites.

VRF and BGP configurations have already been provisioned by Cisco DNA Center, along with the Layer 3 handoff. All fabric domain prefixes will be learned in the GRT of the Internet edge routers. Configure the default route on the fusion router (Internet edge) to advertise the default route. The default route is injected into the BGP RIB of VRFs needing Internet access, resulting in a general advertisement to all BGP neighbors via SD-Access Transit for the VRF.

Advertising a default route in BGP has different methods, each with its own caveats. In this implementation, the " network 0.0.0.0" method is used as an example.

```
network 0.0.0.0
```

- This will inject the default route into BGP if there is a default route present in the GRT.

- The route is then advertised to all configured neighbors.

Example BGP Configuration on Fusion Router (Internet Edge)

```
router bgp 65540

  <Config snipped>

address-family ipv4
 network 0.0.0.0
  <Config snipped>
address-family ipv4 vrf SnS_VN
 network 0.0.0.0
 <Config snipped>
address-family ipv4 vrf Lighting_VN
 network 0.0.0.0
```

1. Verify the default route is injected on the border (FiaB) VRF:

```
C9300-HQR-Stack#show ip route vrf Lighting_VN
<config snipped>
Gateway of last resort is 192.168.70.22 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 192.168.70.22, 5d23h
      10.0.0.0/24 is subnetted, 2 subnets
B        10.10.100.0 [20/0] via 192.168.70.22, 6d20h
B        10.40.100.0 [20/0] via 192.168.70.22, 5d23h
```

2. Once the Firepower in DMZ is configured for Internet access, verify the Internet access from border (FiaB) via VRF as shown belowL

```
C9300-R-Stack#ping vrf Lighting_VN 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/11/12 ms
```

This completes the Internet access configuration for the PoP sites in overlay VNs. For more details on Internet access for fabric sites, refer to the section " Configuring Internet Connectivity" in the *Software-Defined Access for Distributed Campus Deployment Guide*.

Implementation of CCI Access Networks

This section covers the implementation of various last mile access networks like Ethernet Access, CR-Mesh, DSRC, and LoRaWAN in each PoP site, as per the solution design validated in this CVD.

This section includes the following major topics:

Implementation of Ethernet Access Network

The Ethernet network access in a PoP site is provided by connecting Cisco Industrial Ethernet (IE) switches in a ring topology. This section covers the implementation of Ethernet access ring(s) in a PoP site to provide network access to wired endpoints or gateways (examples: IP Camera, Cohda RSU, ICS300, and CGR) connected to the CCI network. Follow the steps covered in this section to complete the implementation of Ethernet access rings in PoP sites.

Linear Daisy chaining of Extended Nodes & Policy Extended Nodes

This section details the steps required for onboarding Extended Nodes or Policy Extended Node into a linear daisy chain topology, as discussed, in the CCI design guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html#pgfId-457899.

Prerequisites for Daisy Chaining Linear Topology

To create a linear daisy chain topology of IE switches in a CCI PoP site the pre-requisites for EN & PEN onboarding (described in previous section) must be met. Additionally, following points must be ensured:

- Ensure that there is only one upstream switch via switch being onboarded can reach Cisco DNA Center for PnP.
- The physical topology connecting the devices that are to be onboarded as ENs & PENs must be completed.

Begin the following steps once the setup meets all the above pre-requisites:

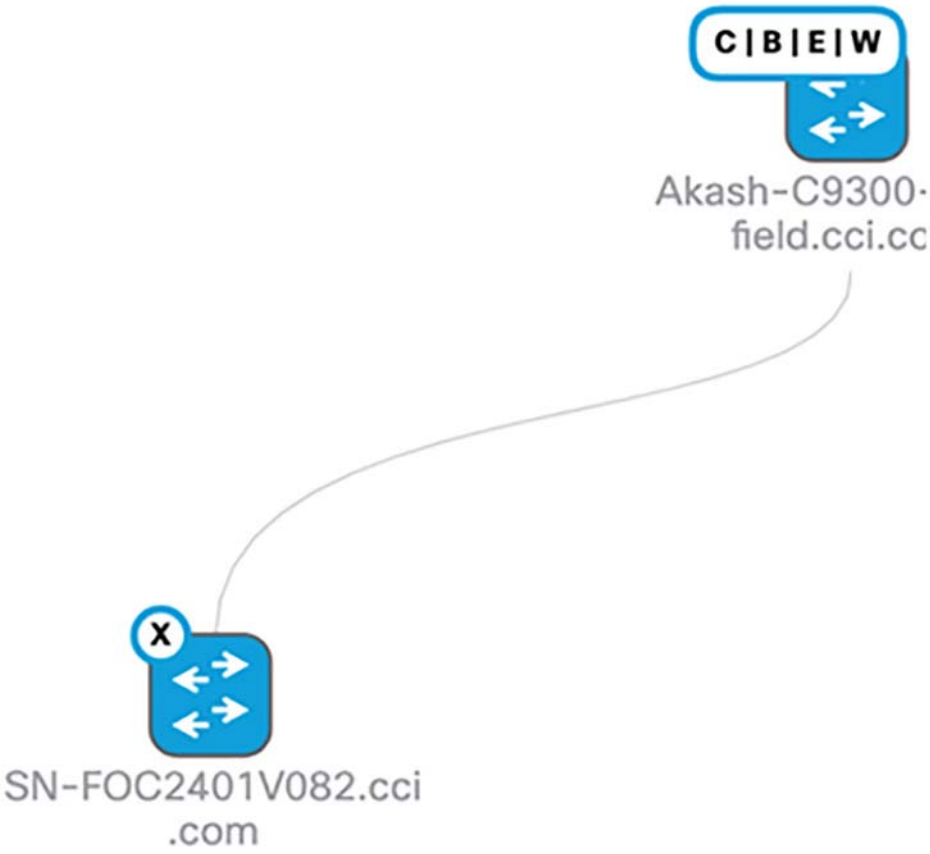
1. Connect the EN/PEN devices to the fabric edge device (FiaB in this case) in the form of a daisy chain topology. You can have multiple links from the extended node device to the fabric edge for redundancy. If there are multiple links between the node and the FiaB , Cisco DNA Center bundles them into a port-channel as part of onboarding process.
2. Power-up the first extended node in the daisy chain and execute the following CLI commands:

```
delete /force sdflash:vlan.dat
delete /force sdflash:*.cer
delete /force sdflash:pnp*
delete /force /recursive sdflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pnp-tech-time
delete /f flash:pnp-tech-discovery-summary
#Delete all the certificates in NVRAM
delete /f nvram:*.cer
conf t
crypto key zeroize
Yes
```

```
!
no crypto pki certificate pool
Yes
vtp mode transparent
End
write erase
Reload
no
```

After the switch reboots, PnP gets triggered, and the device appears under Provision->Plug and Play with state “Unclaimed” which then changes to **Planned->Onboarding** and finally to **Provisioned**. After successful onboarding, device will appear in the fabric topology under **Provision->Fabric sites->Fabric Sites->Site_Name** as shown in Figure 63.

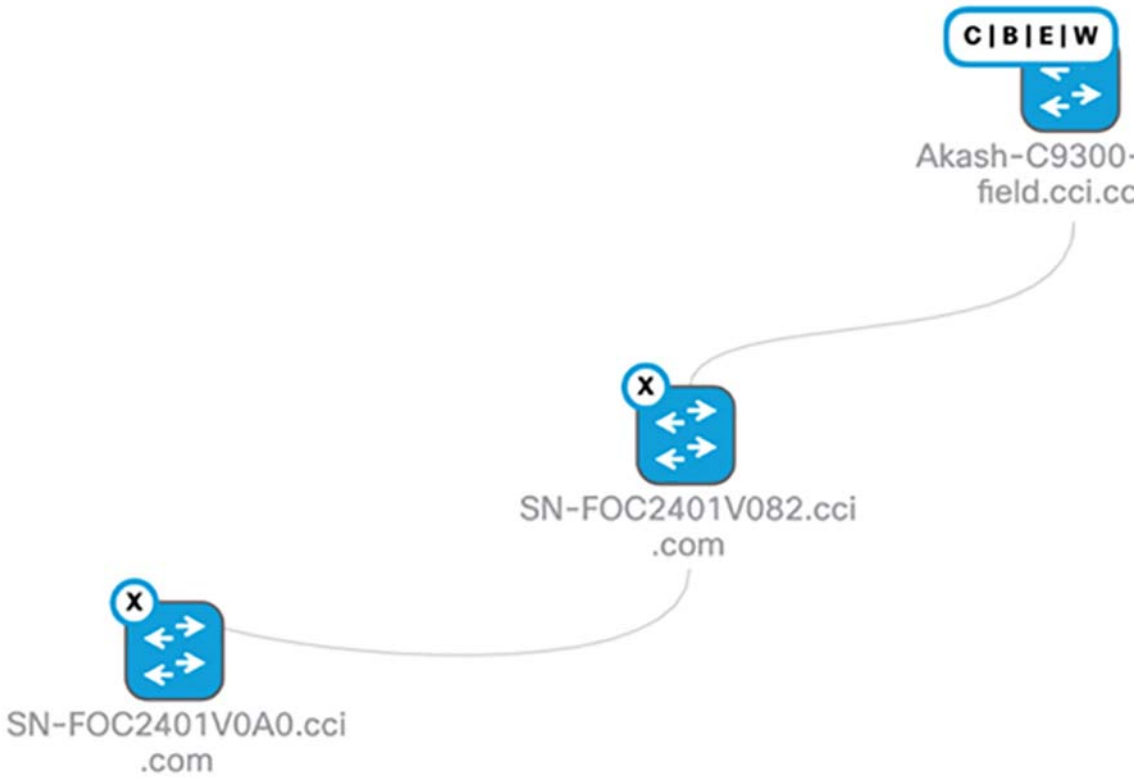
Figure 63 Onboarding first node of Daisy chain



3. After the onboarding completes for first node, power up the second node connected to the first node and repeat the above steps to onboard it onto Cisco DNA Center.

Multiple IE switches can be added to this chain by repeating the above steps. Once daisy chain onboarding of all required IE switches is complete, verify the fabric topology. The fabric topology should appear as shown in Figure 64:

Figure 64 Linear Daisy chain containing two nodes



This completes the linear daisy chaining of Extended nodes or Policy Extended nodes .

Refer to the following URL for more details on daisy-chaining topology limitations and restrictions:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html#pgfId-457899

STP Ring creation

To onboard an STP ring of ENs & PENs, the IE switches which have to be the member of the ring must be first onboarded as a linear daisy chain as described in the previous section. The linear daisy chain for the final ring topology can be obtained by breaking the ring at any desired point. For optimization, it is recommended to break the ring in the middle and onboard the two parts of the ring as two separate linear daisy chains. For example, the intended final ring shown in Figure 66, the two linear daisy chains can be chosen as shown in Figure 65.

Figure 65 Recommended Linear-daisy chains to form an STP ring

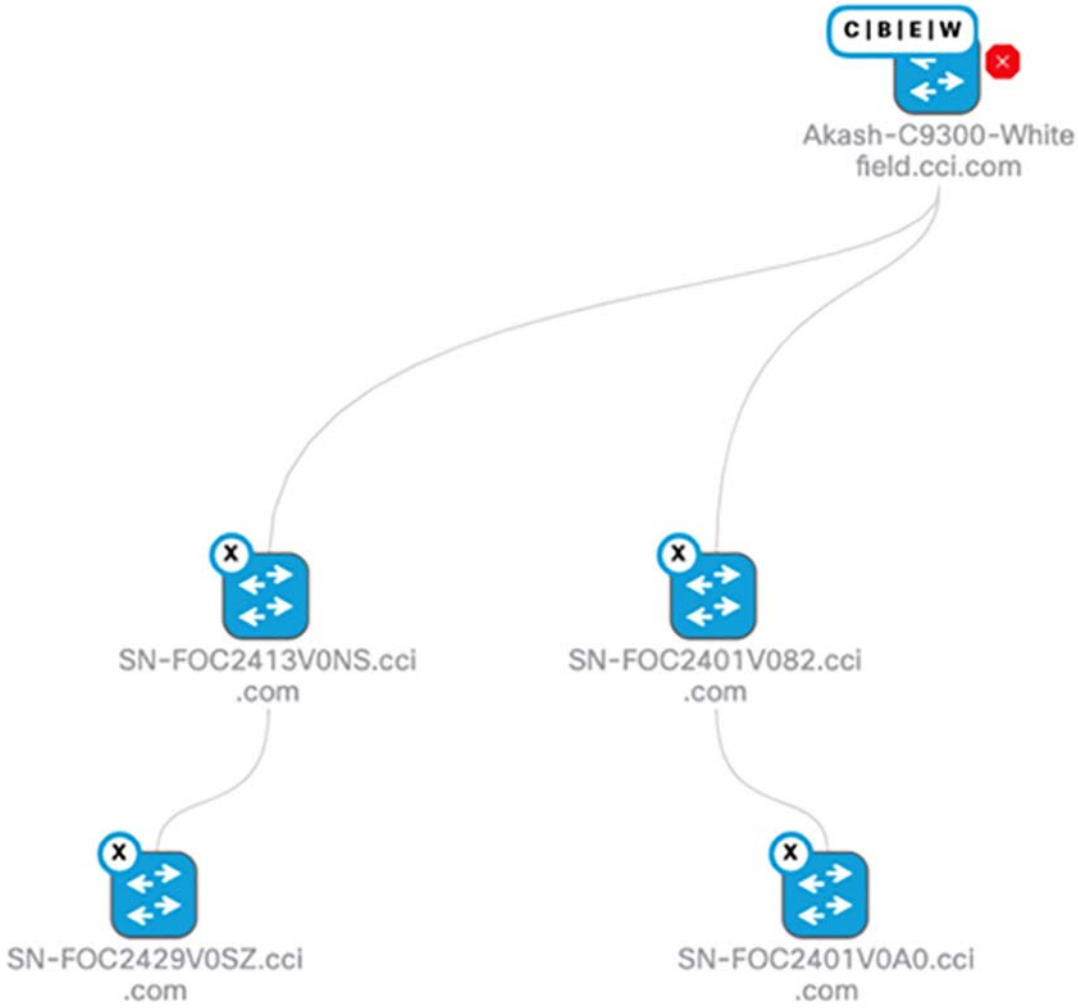
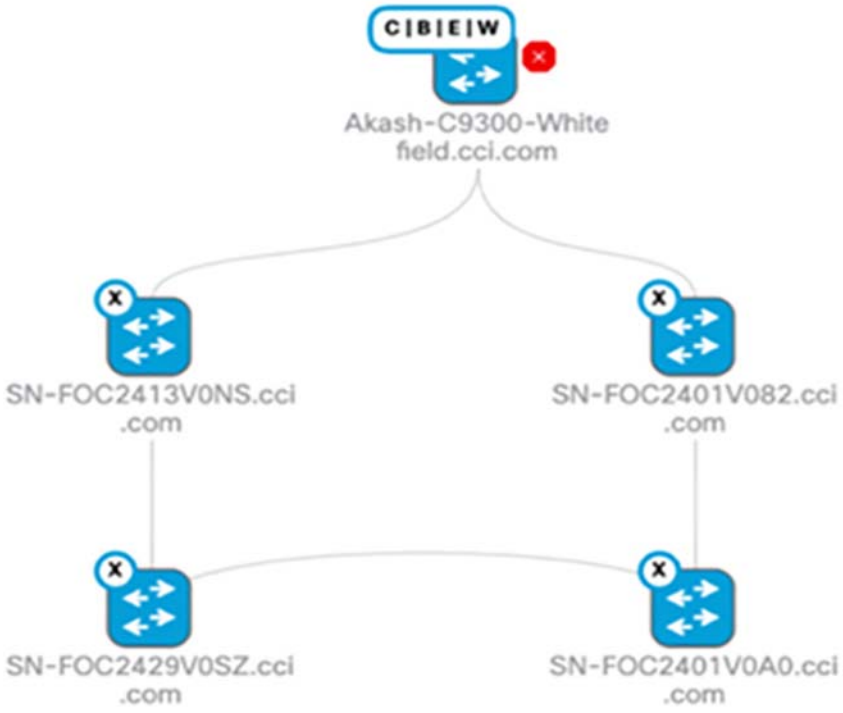


Figure 66 Intended Final STP ring



Following are the steps required to be followed for obtaining the above mentioned STP ring of ENs or PENs:

1. Onboard the member devices of the ring in the form of two daisy chains as described previously. DO NOT connect the interfaces of the last nodes of the two chains before the onboarding process of both linear chains is complete. This will create two upstream links for some of the member devices and may violate the pre-requisite of having exactly one upstream switch for Cisco DNA Center to discover the device via PnP, and causing onboarding to fail.
2. Close the ring by bringing up the interfaces connecting the last nodes of the two daisy chains (For example, the devices SN-FOC2429V0SZ and SN-FOC2401V0A0 from the Figure 66 above).
3. Create a template with the configuration for converting the interfaces brought up in Step 2 above into a port-channel interface.

   For detailed steps on how to configure using Templates refer to the chapter “Create Templates to Automate Device Configuration Changes” at the following URL:

   https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01000.html
4. To create the template navigate to **Tools ->Template Editor-> Icon.** The content to be added in the template is as follows for Policy Extended Nodes ring:

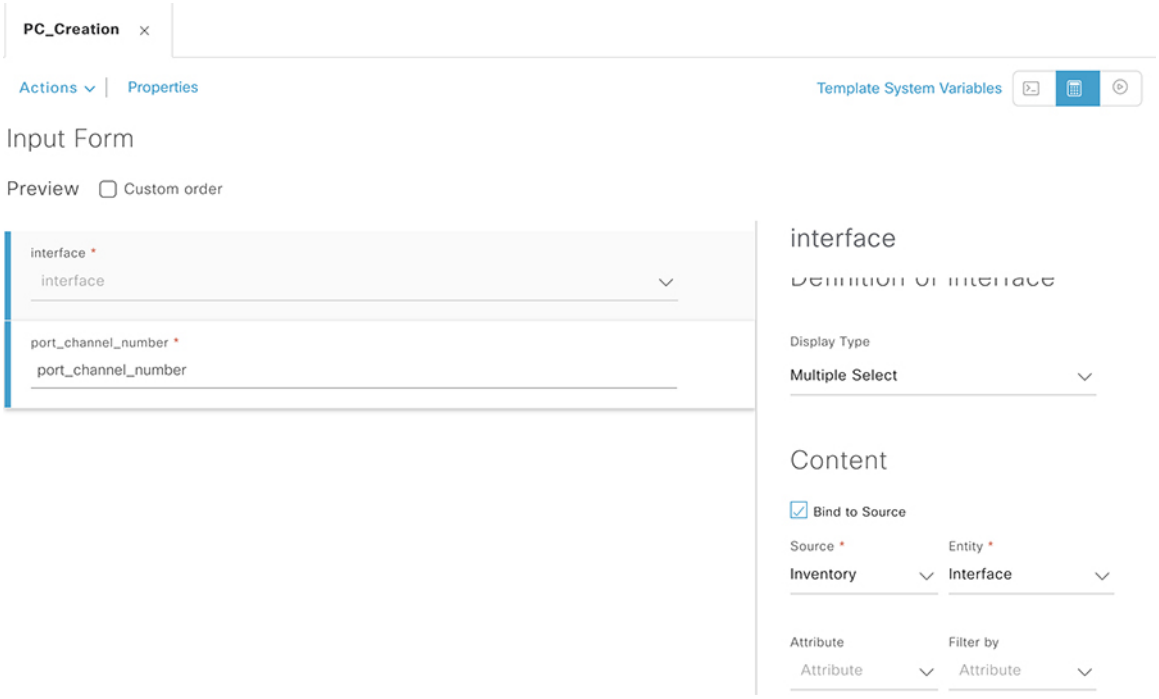
```
default interface $interface
  interface $interface
  switchport mode trunk
  cts manual
  policy static sgt 8000 trusted
  channel-group $port_channel_number mode desirable
```

   The content to be added in the template is as follows for Extended Nodes ring:

```
default interface $interface
  interface $interface
  switchport mode trunk
  channel-group $port_channel_number mode desirable
```

5. Click the **Input Form** pane next to the Template System Variables and check **Bind to Source** under Content in the right pane. Select Source **Inventory and Entity** as interface from the dropdown as shown in the diagram below.

Figure 67 Creating Template for STP ring



6. Click on **Actions->Save->Commit** .

7. Associate the template to a network profile by going to **Design->Network Profile->Add Profile ->Day N Template->Add Template** and then selecting the device type as **Switches and Hubs** and choosing the Template created in step 2. Finally click on **Add**.

8. Associate this Network Profile to the site name where the daisy chain has been onboarded.

9. Navigate to **Provision->Inventory** and enable the checkbox for the two devices followed by **Actions->Provision device** and complete the steps as shown in Figure 68 & Figure 69 below. Choose the interface on each of the two nodes and assign a port-channel number for both devices and then click on **Next->Deploy.**

Figure 68 Provisioning Template for creating Port-channel between the two last nodes of daisy chains

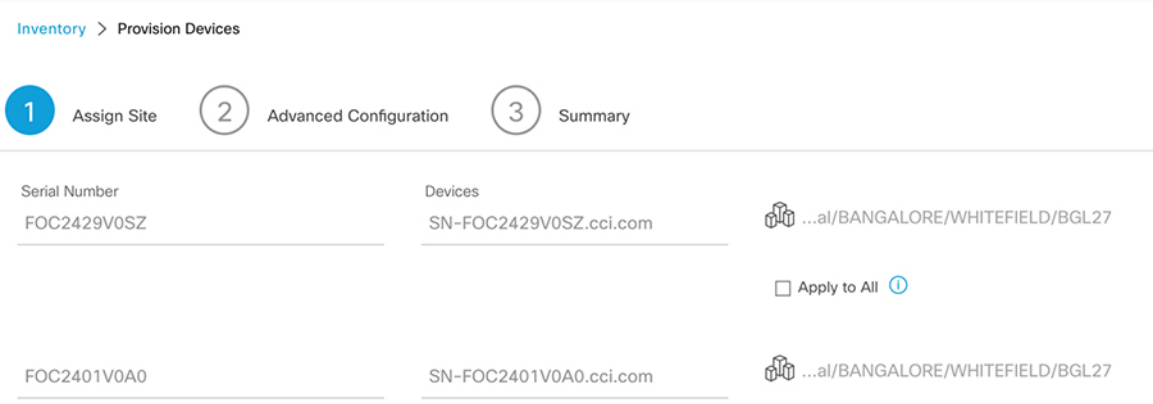


Figure 69 Provisioning Template for creating Port-channel between the two last nodes of daisy chains

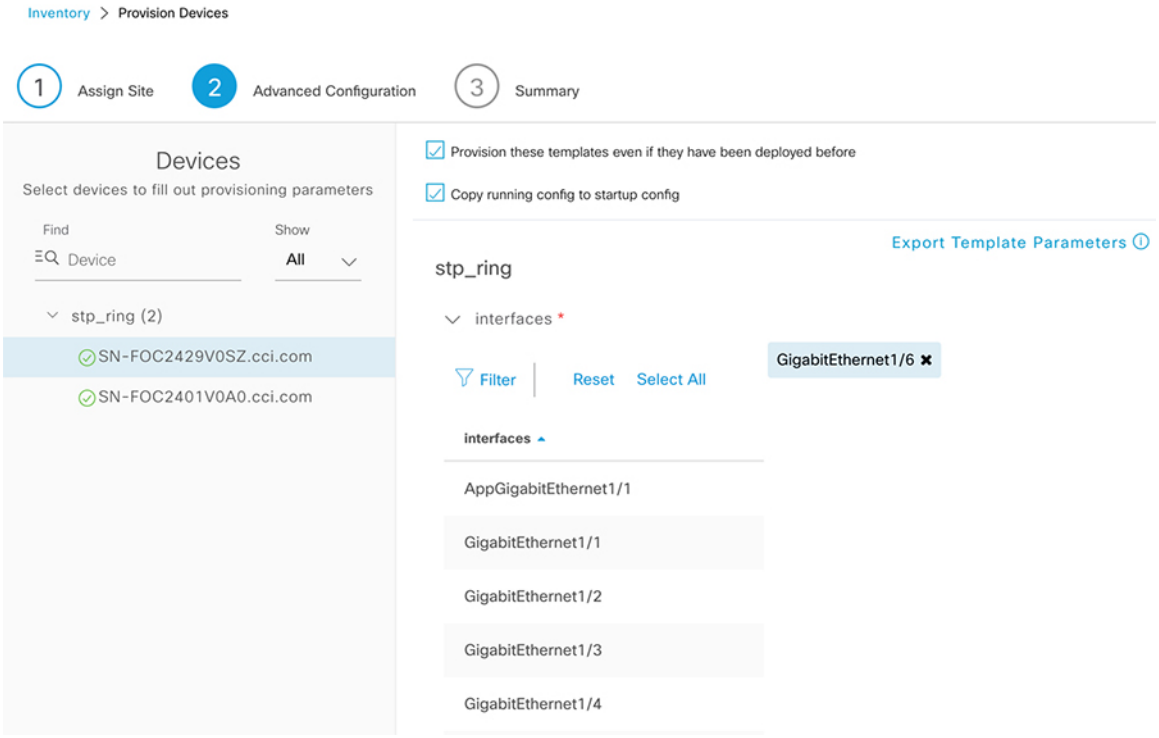


Figure 70 Provisioning Template for creating Port-channel between the two last nodes of daisy chains

This will close the two linear chains into a STP ring .

Cisco switches run STP by default and hence the only STP configuration that is required in the ring is assigning the FiaB switch as the root bridge. For this we will create another template and associate it with a Network Profile, associate the device type matching the FiaB and then assign it to the site. The same steps as described in above section has to be followed for applying the template to the device. The configuration to be added in the template is:

```
spanning-tree vlan 1-1001,1006-4094 root primary
```

10. After the template is ready for deployment go to **Provision->Inventory->Select the FiaB switch -> Actions ->Provision Device->Next ->Deploy** to deploy the template to FiaB switch

11. Verify that the FiaB switch has become the root bridge for all configured VLANs. This can be done by issuing “show spanning-tree” CLI command on the switch. The root ID will match the bridge ID for all VLANs in the output as shown below:

```
Akash-C9300-Whitefield#show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     2416.9d7f.2800
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     2416.9d7f.2800
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Te1/1/2             Desg FWD 2000      128.30   P2p
Ap1/0/1             Desg FWD 20000     128.41   P2p
Po4                 Desg FWD 2000      128.3052 P2p
Po5                 Desg FWD 10000     128.3053 P2p
Po7                 Desg FWD 20000     128.3055 P2p
Po8                 Desg FWD 20000     128.3056 P2p
Po9                 Desg FWD 20000     128.3057 P2p

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID     Priority    24626
              Address     2416.9d7f.2800
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24626  (priority 24576 sys-id-ext 50)
              Address     2416.9d7f.2800
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Te1/1/2             Desg FWD 2000      128.30   P2p
Po4                 Desg FWD 2000      128.3052 P2p
Po5                 Desg FWD 10000     128.3053 P2p
Po7                 Desg FWD 20000     128.3055 P2p
Po8                 Desg FWD 20000     128.3056 P2p
Po9                 Desg FWD 20000     128.3057 P2p
```

----some outputs have been omitted-------

This completes the STP ring creation of ENs or PENs in a CCI PoP site.

Note: For a ring size of more than 20 nodes, the spanning-tree max age timer must be changed. The STP max age timer should be increased from the default value of 20 to a maximum value of 40 depending on the number of nodes. Following is the command to set the timer using CLI:

```
spanning-tree vlan 1-1001,1006-4094 max-age 40
```

REP Ring Onboarding

Extended nodes (EN) and Policy Extended Nodes (PEN) in SD-Access extend the Fabric Edge for IoT devices and provide SD-Access to IE switches, ENs and PENs run in Layer 2 switch mode and do not natively support fabric technology. An EN/PEN is configured by an automated workflow. After configuration, the extended node device is displayed on the fabric topology view. Port Assignment on the extended nodes is done on the Host Onboarding window.

The following are the supported hardware and minimum supported software versions on the EN/PEN:

- Cisco Industrial Ethernet 4000, 4010, 5000 series switches: 15.2(7)E0s with LAN base license enabled

- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: IOS XE 17.1.1s
- Cisco Catalyst IE 3300 series switches: IOS XE 16.12.1s

Note: Both a Network Advantage and a DNA Advantage license is required on IE3400 switches for onboarding it them as Policy Extended Nodes (PENs). This section discusses the steps to onboard an EN or PEN in an Ethernet access ring.

Prerequisites for extended node onboarding:

- Configure a network range for the extended node. Refer to <<Step 4. Configure IP Address Pools>> for steps to configure the IP Address Pool. This configuration comprises adding an IP Pool and reserving the IP Pool at the site level. Ensure that the CLI and SNMP credentials are configured.
- Assign the extended IP address pool to INFRA_VN under the **Fabric > Host Onboarding** tab. Select **Extended Node** as the pool type. Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.
- Ensure that the Fabric site is configured with “No Authentication” mode for onboarding IE switches in to SD Access fabric as EN or PEN

Configure the DHCP server with the extended IP address pool and Option-43. Refer to section " DHCP Controller Discovery" in the *Cisco Digital Network Architecture Center User Guide*, Release 2.2.3 at the following URL:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01101.html?bookSearch=true#id_90877

Ensure that the FiaB is provisioned and that the extended node IP pool default gateway configured on the FiaB (Edge) is reachable from the Cisco DNA Center.

Complete the following steps to onboard EN or PEN:

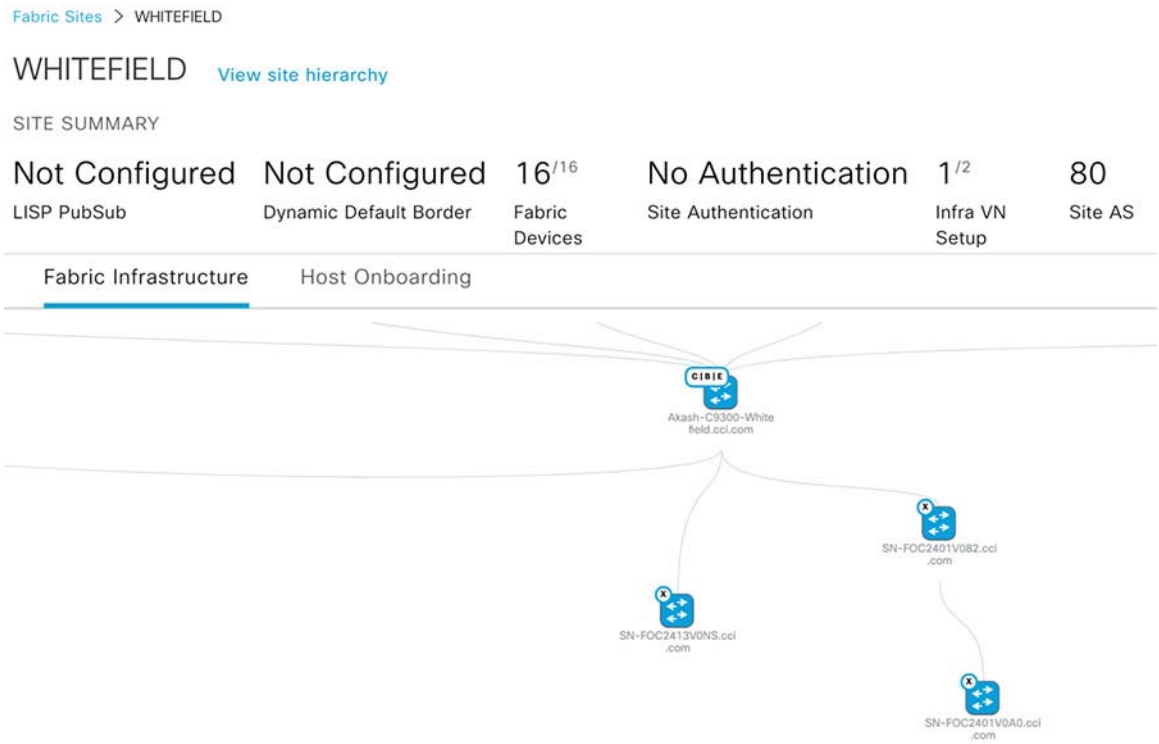
1. Connect the EN/PEN devices to the fabric edge device (FiaB in this case) in a the form of a Daisy Chain format. You can have multiple links from the extended node device to the fabric edge.
2. Power-up the extended node device if it has no previous configuration. If the extended node switch has any previous configurations, execute the following steps on the extended node switch before starting the onboarding process:

```
delete /force sdflash:vlan.dat
delete /force sdflash:*.cer
delete /force sdflash:pnp*
delete /force /recursive sdflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pnp-tech-time
delete /f flash:pnp-tech-discovery-summary #Delete all the certificates in NVRAM delete /f
nvram:*.cer
#Clear the crypto certificates in config mode crypto key zerosize
no crypto pki certificate pool
#Change the VTP mode to Transparent in config mode vtp mode off
vtp mode transparent exit
#Do write erase and reload
write erase
reload (enter no if asked to save)
```

The Cisco DNA Center adds the EN or PEN device to the Inventory and assigns the same Site as the fabric edge. The EN or PEN is then added to the fabric. Now the EN or PEN is onboarded and ready to be managed.

After the configuration is complete, the EN or PEN appears in the Fabric topology with a tag (X) indicating that it is an extended node, as shown in Figure 71.

Figure 71 Cisco DNA Center Fabric Infrastructure View of Extended Node



Note: If any errors exist in the workflow while configuring an EN or PEN, an error notification is displayed as a banner on the topology window. Click **See more details** on the interface to check the errors.

Configure REP Ring topology for Extended Nodes & Policy Extended Nodes:

To enable redundancy on the extended nodes, configure a Resilient Ethernet Protocol (REP) Ring for a fabric site. The Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to the Spanning Tree Protocol (STP). REP provides a way to control network loops, handle link failures, and improve convergence time. It controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment.

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. An example Closed REP ring topology configuration validated in this implementation is described in this section.

REP Ring Configuration using REP Workflow:

- A REP ring can be created in a CCI PoP site using Cisco DNA Center REP Workflow feature.

Note: REP Workflow for creating a REP ring in a CCI PoP site/fabric site is supported from Cisco DNA Center 2.3.2.x release onwards. You must upgrade the Cisco DNA Center to the release 2.3.2.x or higher to use this feature for creating REP rings.

Limitations of REP Ring Workflow:

- Configuring an ring topology of all switches is must by physically connecting all of the switches in a ring before using the REP workflow.
- A device connected in a REP Ring can't be deleted from the fabric until the REP Ring that it's a part of is deleted.
- To delete or insert a member into the REP Ring, first delete the REP ring, add, or delete a member (as required) and then create the REP Ring again.
- Multiple rings within a REP ring are not supported.
- A ring of rings is not supported.
- A node in a REP ring can have other nodes connected to it in a daisy chain manner; but a node in a daisy chain can not have a ring of nodes connected to it.
- A mix of extended node (ENs) devices and policy extended node (PEN) devices in a REP Ring isn't not supported. A REP Ring can have all devices either as extended node or as policy extended node.
- By default, a maximum of 18 devices can be onboarded in a single REP ring. To onboard more than 18 devices, increase the BPDU timer using the spanning-tree *vlan <infra_ VN_ VLAN> max-age 40* command. Use the Cisco DNA Center templates to configure the command.

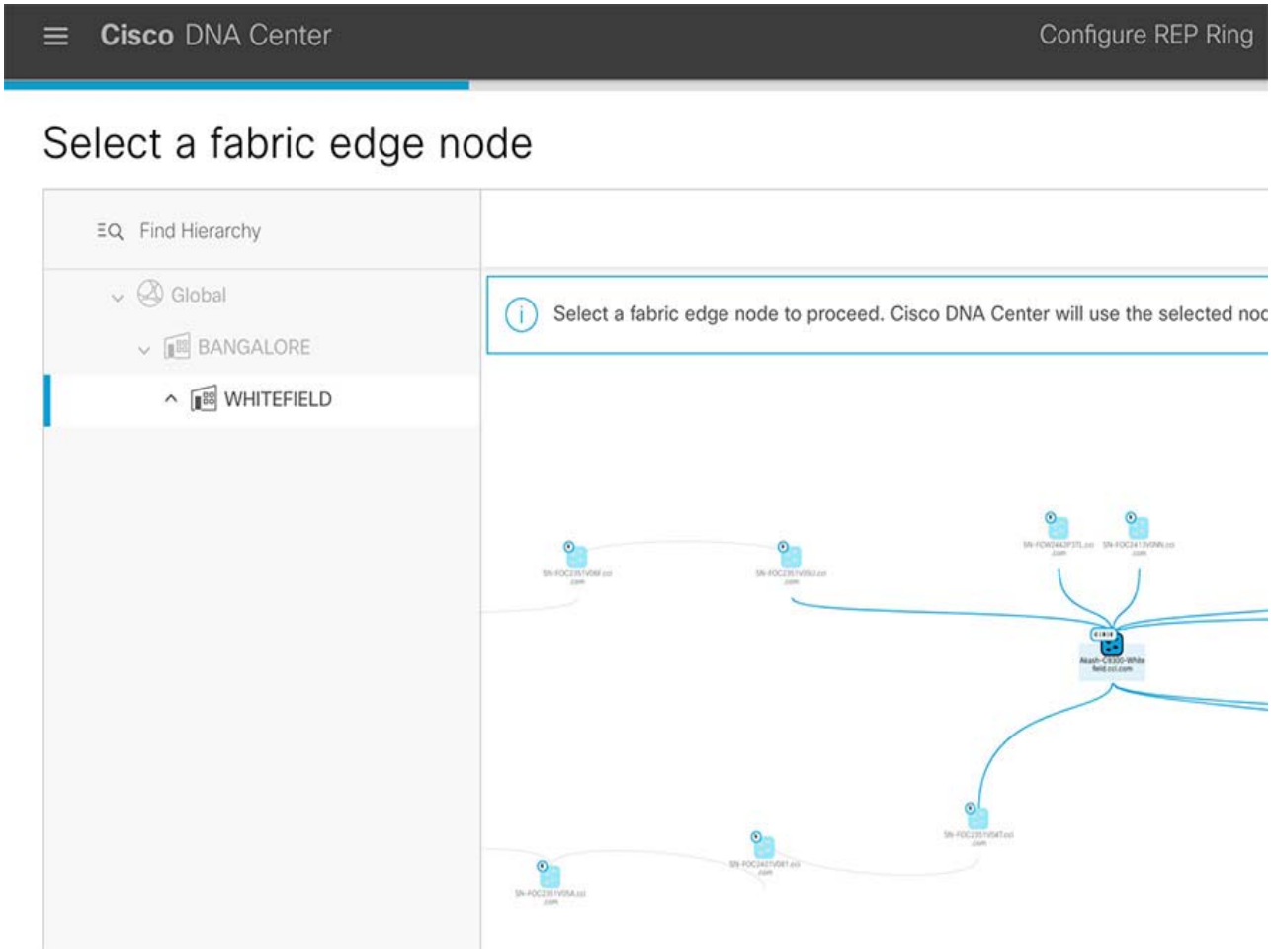
Follow the below steps to configure the REP ring using the workflow.

1. In the Cisco DNA Center GUI, click the Menu icon and choose Workflows > Create REP Ring.

   Alternatively, you can navigate to the Fabric Site topology view, and then select the Fabric Edge node or the FIAB node on which you want to create the REP ring and click Create REP Ring under the REP Rings tab.

2. In the workflow wizard, click **Let's Do it**.
3. Select a Fabric Site from the drop-down list and then click **Next**.
4. Select a fabric edge node in the topology view and then click **Next.**

Figure 72 Cisco DNA Center REP workflow – Fabric Edge selection

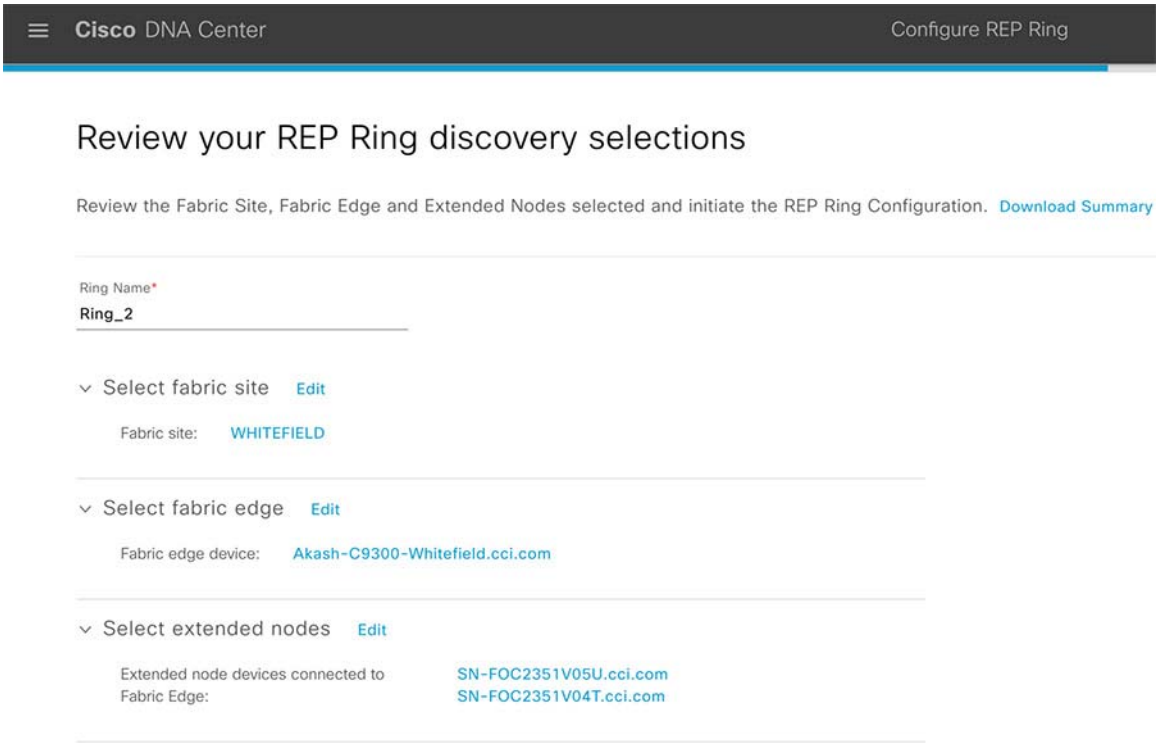


5. Select the extended nodes that connect to the fabric edge device and then click **Next**.

   You can select two extended nodes to connect to the fabric edge (One would be the beginning of the REP Ring and the other would end the REP Ring).

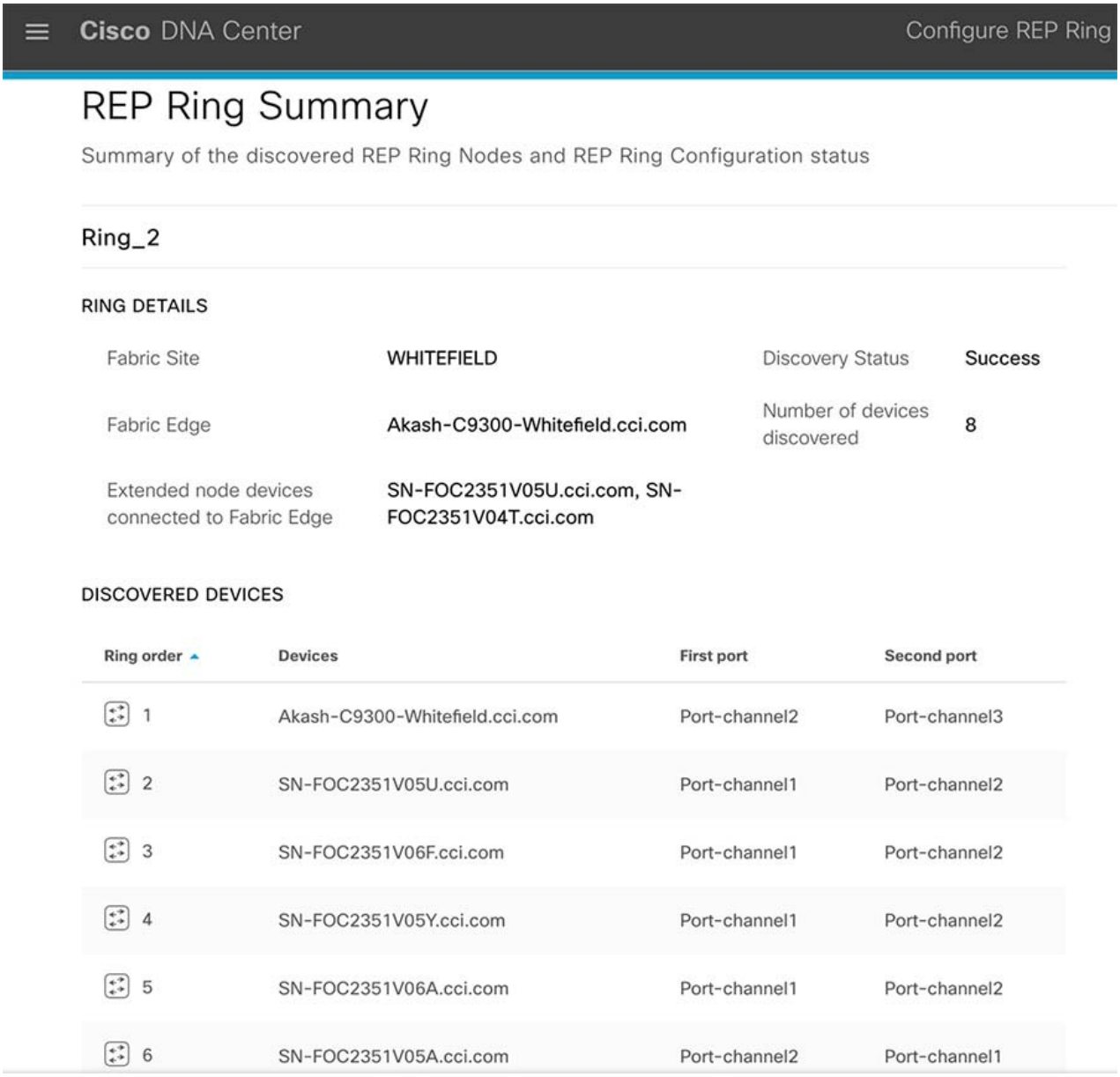
6. Review and edit (if required) your fabric site, edge, and extended node selections.

Figure 73 Cisco DNA Center REP Workflow – REP Ring Review



7. To initiate the REP ring configuration, click Provision.
8. A REP Ring Configuration Status window shows a detailed configuration progress.
9. A REP Ring Summary window displays the details of the REP ring that is created along with the discovered devices. Click **Next.**

Figure 74 Cisco DNA Center REP workflow – REP Ring Summary



10. After the creation of the REP ring, a success message is displayed.

To verify the creation of the REP ring, go to the Fabric Site window and click on the fabric edge. In the slide-in window, under the REP Ring tab, you can see the list of all REP rings that exist on that device. Click on a REP Ring name in the list to view its details like the devices present in the ring, ports of each device that connect to the ring, and so on.

Figure 75 shows a REP ring fabric topology view once the REP ring is provisioned successfully using REP Ring workflow feature in Cisco DNA Center UI.

Figure 75 REP Ring Topology View in Cisco DNA Center SD-Access Fabric

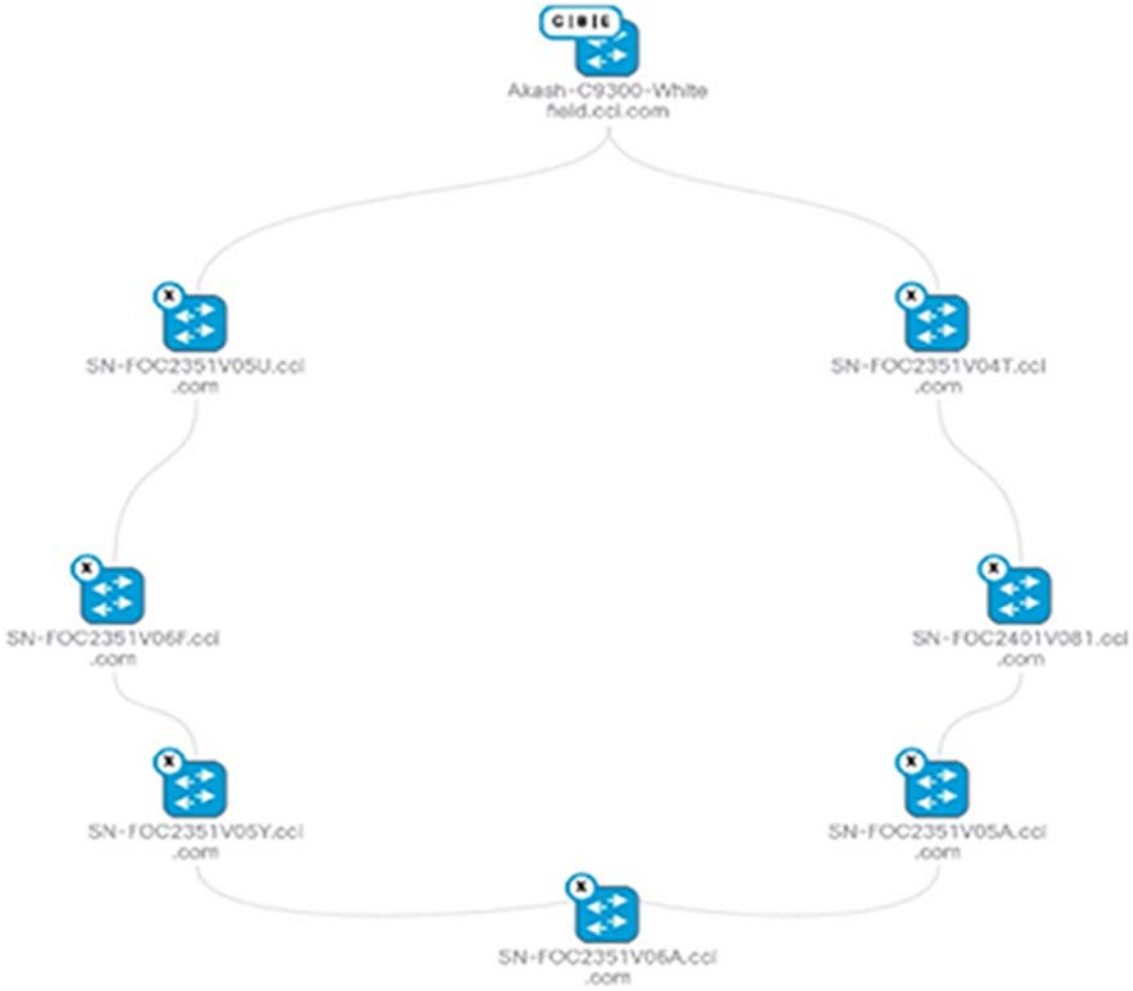


Figure 76 REP Ring Topology View in Cisco DNA Center SD-Access Fabric

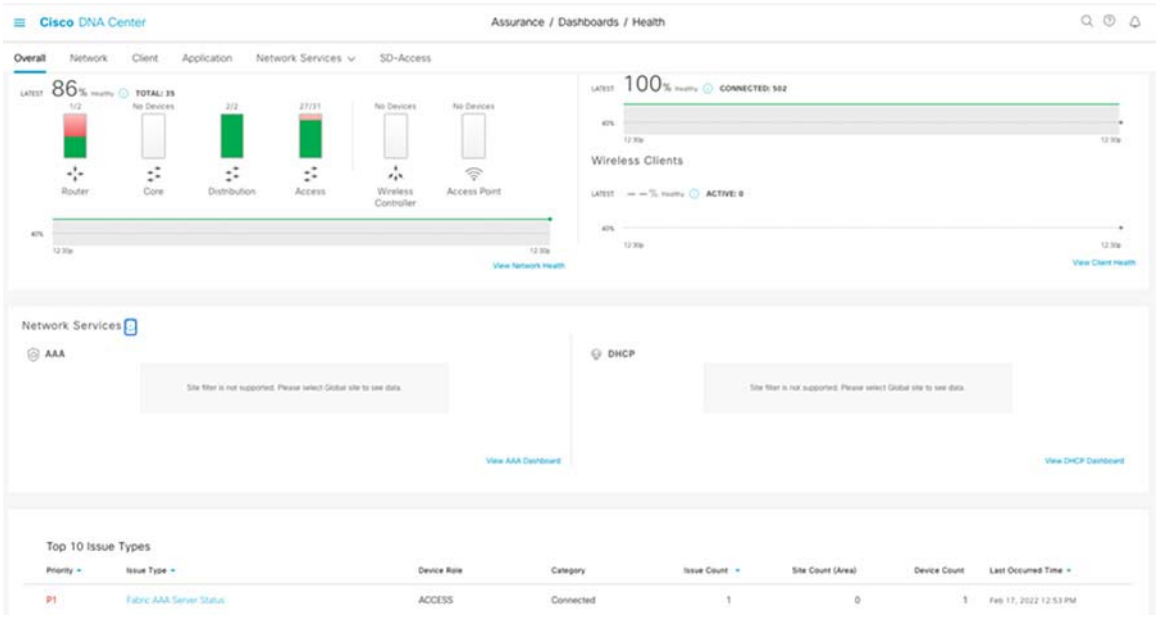
Network Assurance

Using the Assurance features of Cisco DNA Center provides a detailed view of the network health. The overall network health can be viewed as well as an individual device health in Device 360. Assurance focuses on network visibility aspect of the network by identifying the issues, trends in the network. Assurance also focuses on the operational efficiencies by focusing on faster troubleshooting. Assurance provides the following benefits:

- Provides actionable insights into network, client, and application related issues. These issues consist of basic and advanced correlation of multiple pieces of information, thus eliminating white noise and false positives.
- Provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of a problem, after which possible actions are provided to resolve the problem. The focus is on highlighting the issue rather than monitoring data. Quite frequently, Assurance performs the work of a Level 3 support engineer.
- Provides in-depth health scores for a network and its devices, clients, applications, and services. Client experience is assured both for access (onboarding) and connectivity.

In CCI network where there will be IE nodes in a fabric site, it will be important to have a single view of the network health. Some examples of the network health are shown below:

Figure 77 Device 360 Network Health



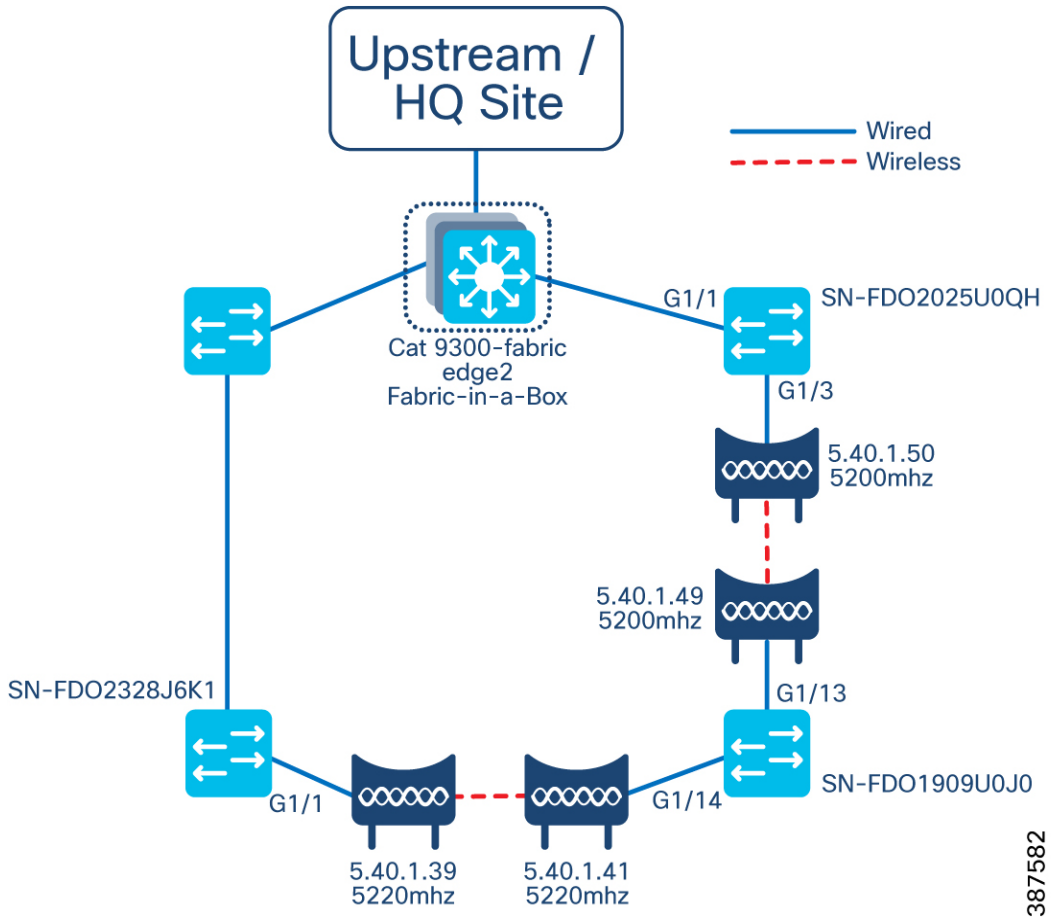
For more detailed information about using Cisco DNA Assurance, refer to the Cisco DNA Assurance User Guide, Release 2.2.3 at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug.html

Cisco Ultra-Reliable Wireless Access Network

This section describes the initial configuration of CURWB radios, telemetry monitoring with FM Monitor, and the integration with DNA Center. This configuration deployment uses the FM3500 Endo in a PTP capacity for establishing wireless connectivity between Infrastructure Extended Nodes (EN) within the access layer. The IE switches connected behind them can be onboarded and managed using Cisco DNA Center. The following reference topology wais used in this deployment.

Figure 78 Reference Topology

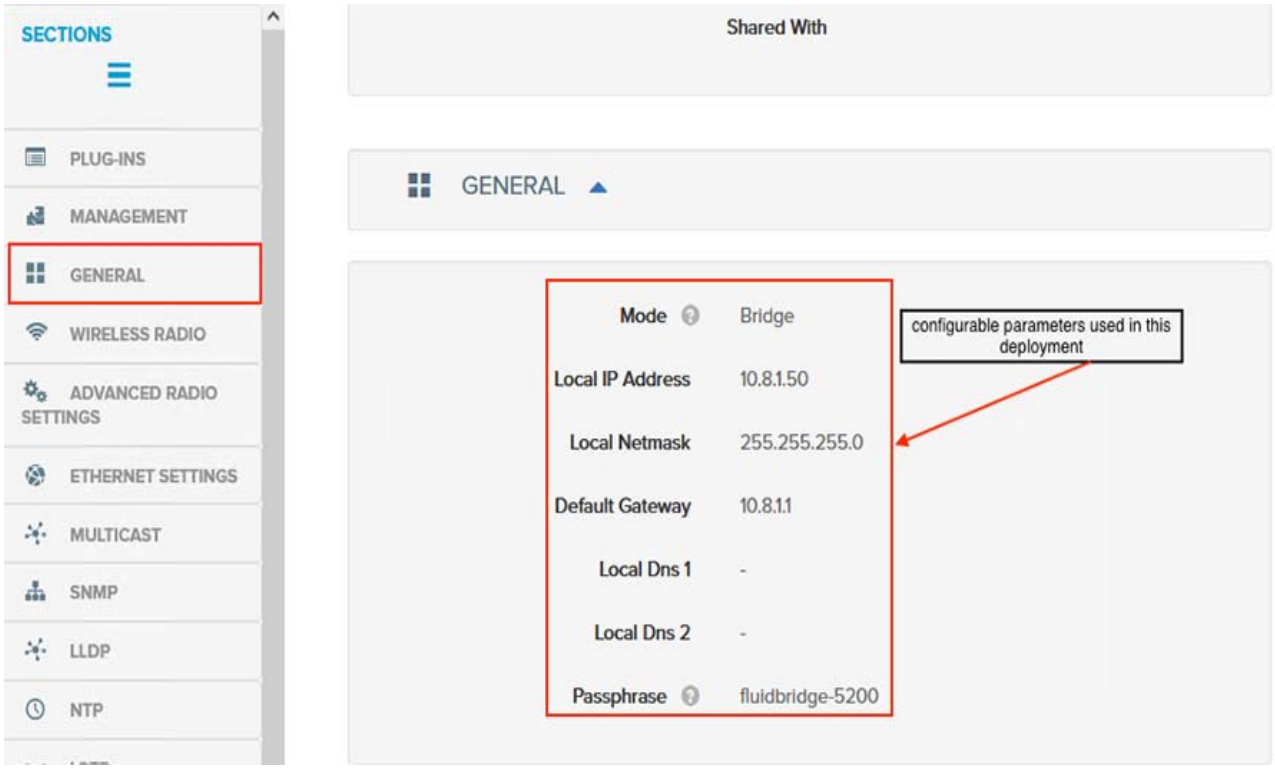


General Settings

This deployment uses RACER to perform the initial configuration. RACER is a centralized, Internet-based configuration software platform that is accessed from the Partner Portal. Devices can be configured online only. If a device must be configured offline, then a separate configuration file can be uploaded to the device using the offline configurator. Refer to your device-specific guide for the instructions on this process. The General Mode window contains controls to monitor/enable configuration of the following settings:

- Operational mode of the unit
- LAN parameters
- Passphrase

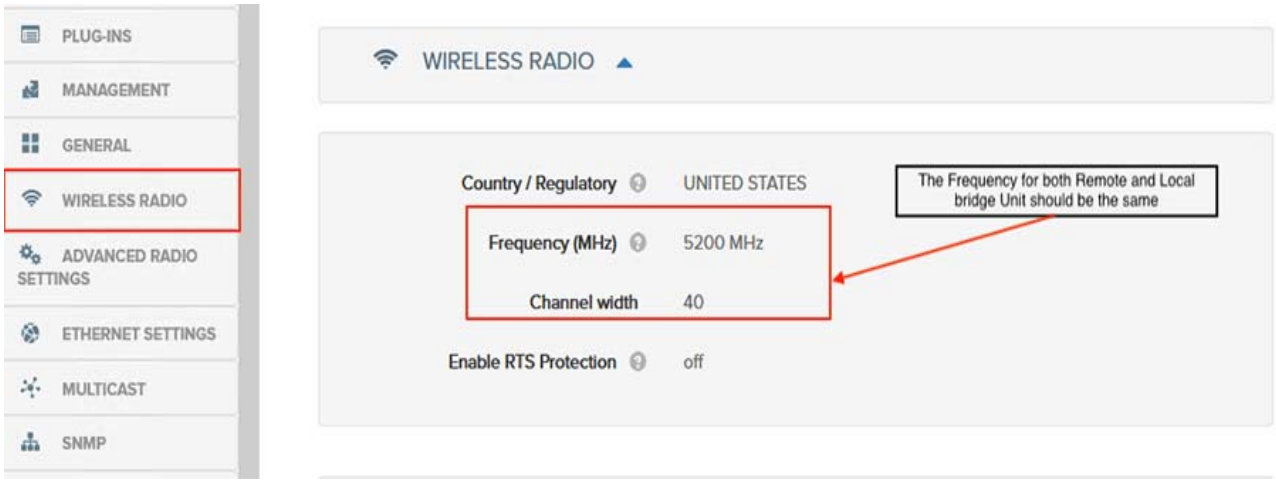
Figure 79 CURWB General Settings



The CURWB devices used in this deployment are part of the network underlay. The management interface on all bridge units are configured on the same subnet. All units that are part of the same network should also have the same passphrase.

Wireless Radio

Wireless Radio Settings

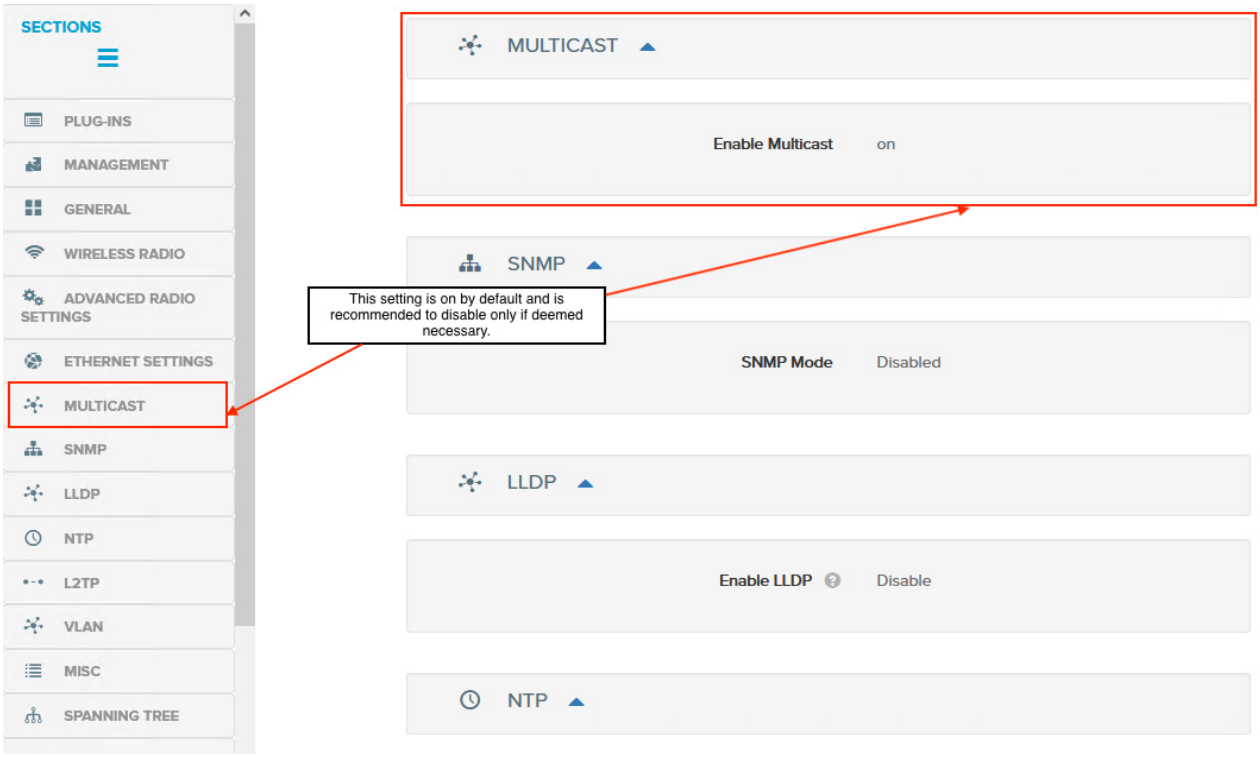


The frequency between the local and remote units must be the same. If configuring multiple bridge pairs, each pair should be on a separate frequency.

Multicast

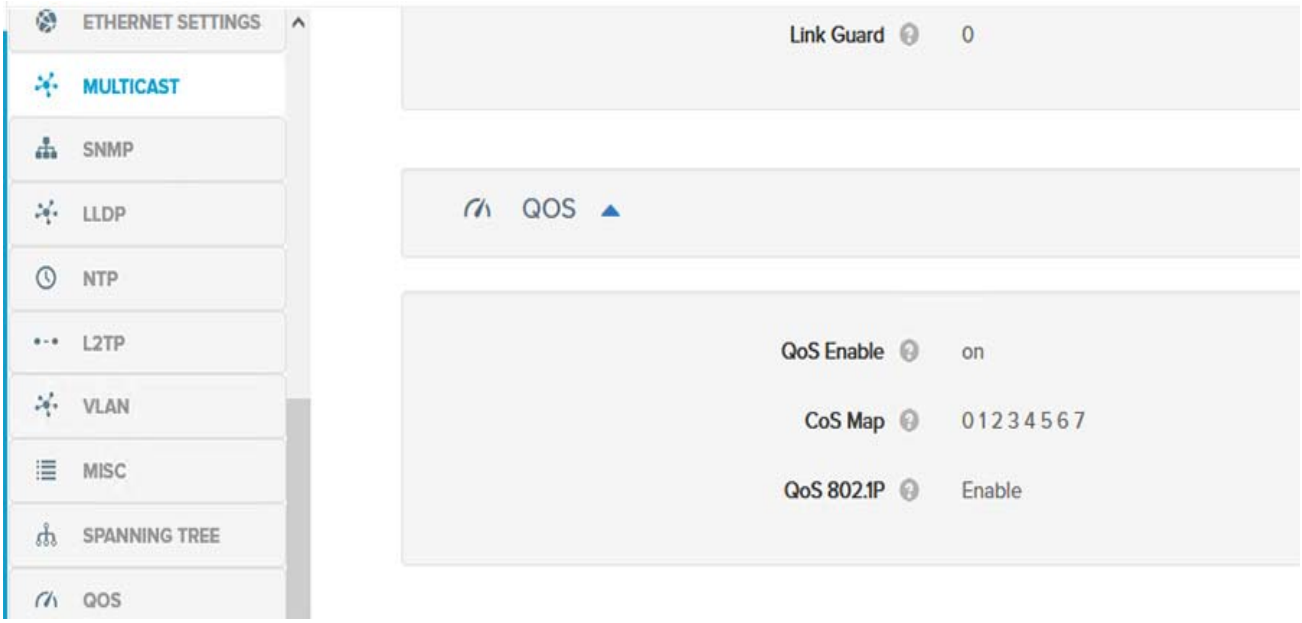
This setting is on by default and is recommended to disable only if deemed necessary.

Figure 80 Multicast



QoS

Figure 81 QoS enabled

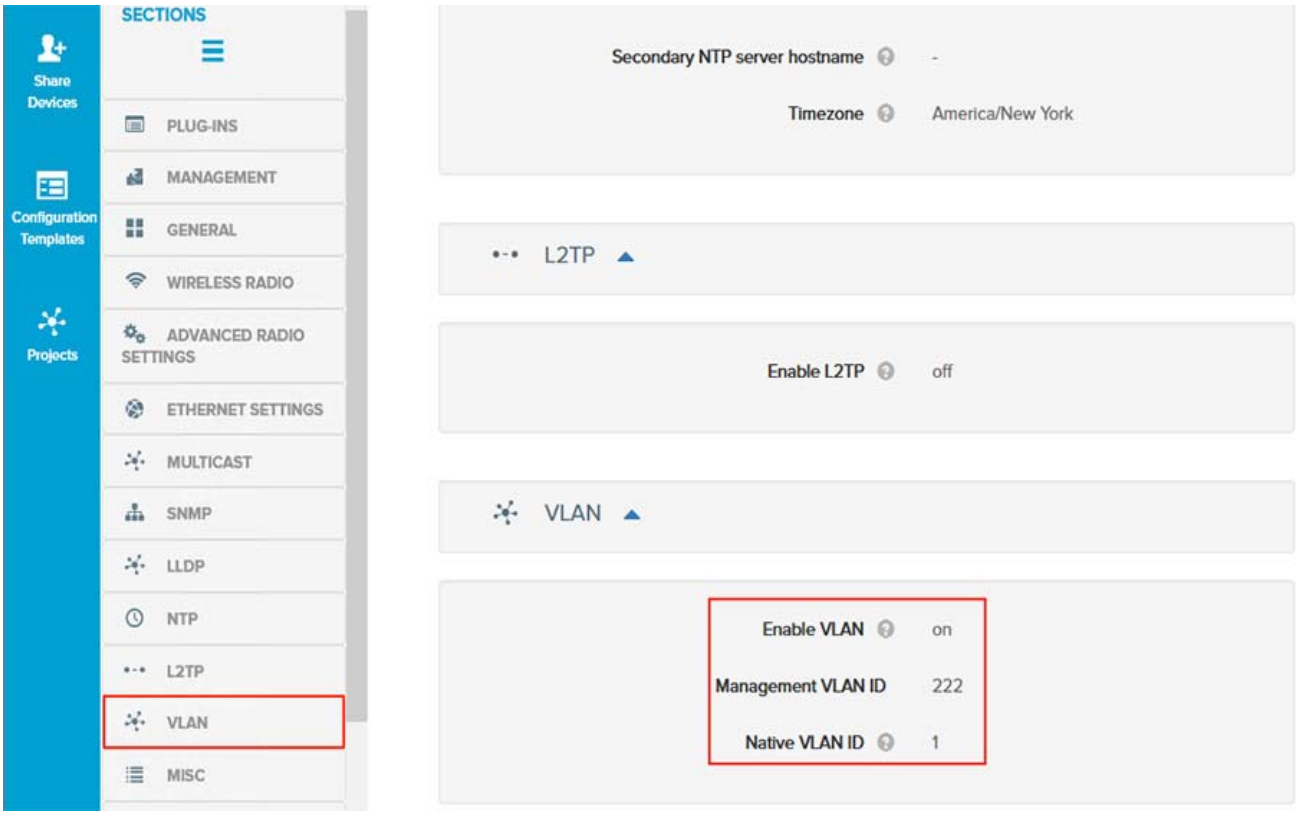


The screenshot above shows the QoS 802.1p is enabled. This allows the CURWB radio to read the COS value from the VLAN tag, otherwise the DSCP/TOS value is read from the layer 3 IP packet.

VLAN

If the VLAN plug-in is assigned the VLAN settings tab will be configurable and required to allows the unit to be connected to one or more virtual networks. Even without the plug-in, the CURWB radios can connect to a VLAN access network. The plug-in gives you the option to specify the management VLAN and native VLAN while also preserving the existing VLAN tags. With VLANs enabled, ensure the management subnet VLAN ID is added to the configuration. Note: this plug-in is required for integration within DNA Center for extended node onboarding via CURWB.

Figure 82 VLANs



In this deployment, the CURWB radio management VLAN ID is 222 and this VLAN is not used anywhere else within the network. Configure the VLAN ID and SVI on the fabric edge PoP as part of the network underlay. In this scenario, the native VLAN is set to 1 which matches what is configured on the fabric edge. See the following configuration example taken from the Fabric PoP N Edge:

CURWB Management VLAN

```
 vlan 222
 name CURWB_MGMT
interface Vlan222
 description FM-3500
 ip address 10.8.1.1 255.255.255.0
!
```

CURWB management subnet added to underlay EIGRP

```
router eigrp 20
network 10.8.1.0 0.0.0.255
```

Plug-ins

In this deployment, the FM-VLAN was installed as it is required for connection to multiple virtual networks. Please refer to your device user guide for other required plug-ins. Plug-ins can be added individually, through CSV, or via the RACER template.

Configuration Settings

Integration with DNA Center

After CURWB radios have been configured as bridge links, an IE switch can be connected to the CURWB ethernet port, onboarded through PNP and managed through DNA Center as an Extended Node. The wireless connection between bridge units acts as a transparent relay in lieu of ethernet or fiber links.

Onboarding and provisioning a newly-discovered switch are the same processes as with a wired switch and requires no special configuration to support the CURWB connection. The Extended node requires an ip IP address from DHCP to start the pnp PNP process.

Option 43 includes three type- length- values (TLV). The first value is 5A1D;B2;K4; which specifies the PNP option. The second is the Cisco DNA Center IP address. The third is the port which could be 80 (HTTP) or 443 (HTTPS). Here is an example:

```
5A1D;B2;K4;I<Cisco DNA Center IP>;J80;
```

To onboard an Extended node over the wireless bridge, connect the ethernet port of the local CURWB unit to the Fabric Edge Node or an existing Extended Node.

Connect the ethernet port of the remote CURWB unit to the switch port of IE switch to be onboarded. If the configuration settings on the CURWB radios (local & remote) are correct, then the zero-touch provisioning script should start the onboarding process of the IE switch behind the radio. After the onboarding is complete, verify that port channel config has been pushed down to the connected interface and that the IE switch appears within DNA Center inventory.

Figure 83 Extended Node with CURWB connection

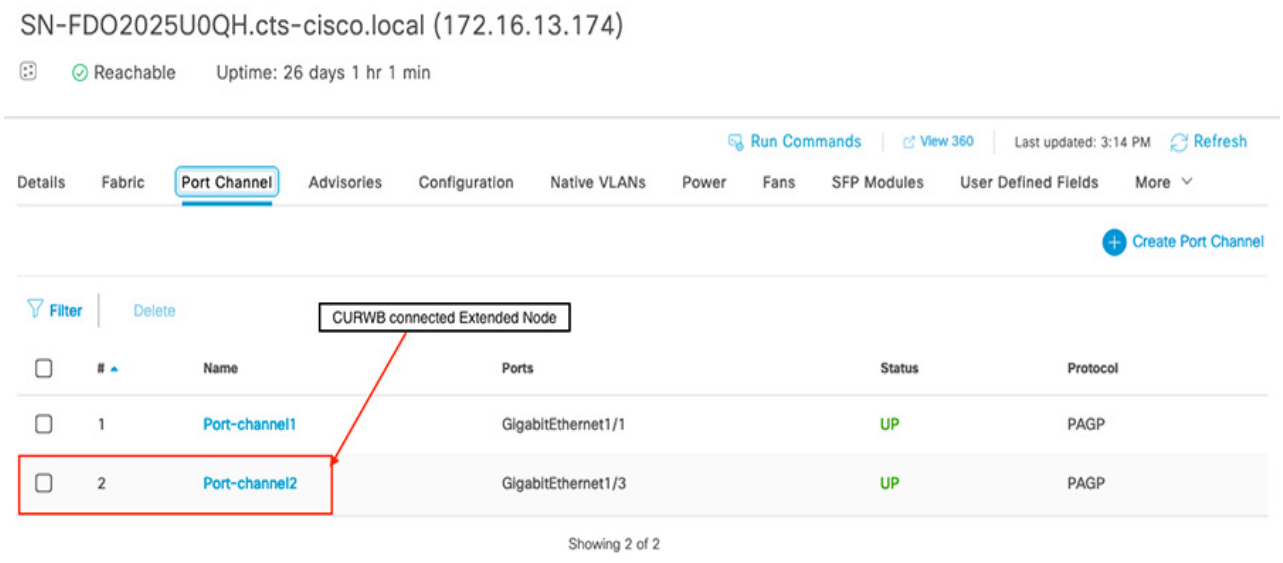
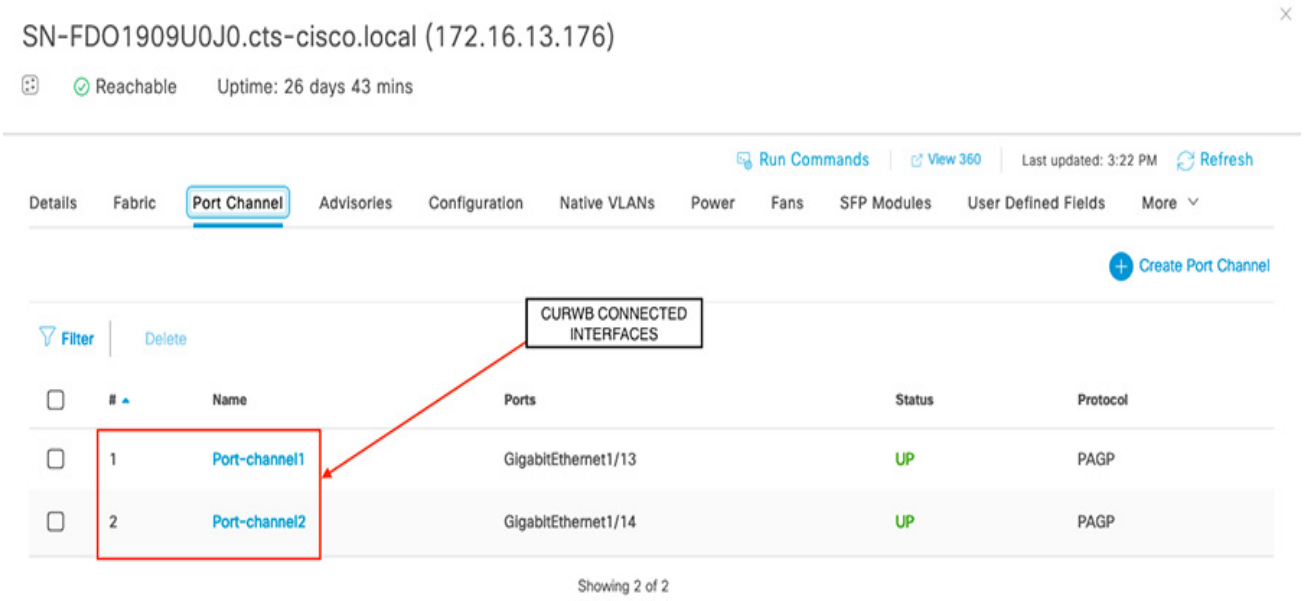


Figure 84 CURWB connected interfaces



The same port channel and interface configuration are displayed on the CLI of the Extended node.

CURWB management Layer 2 VLAN

The CURWB management VLAN must be configured on the Extended node and allowed on interfaces carrying management VLAN traffic. This can be done manually, or optionally, via template in DNA Center. By default, all VLANs, 1 to 4094 are forwarded on trunk interfaces. Unless pruning is desired only creation of the layer 2 VLAN is required on the switch. See the following example.

CURWB LAYER 2 VLAN

```
Vlan 222
Name CURWB_MGMT
!
```

Figure 85 CURWB template created optionally via DNAC Center with VLAN variable

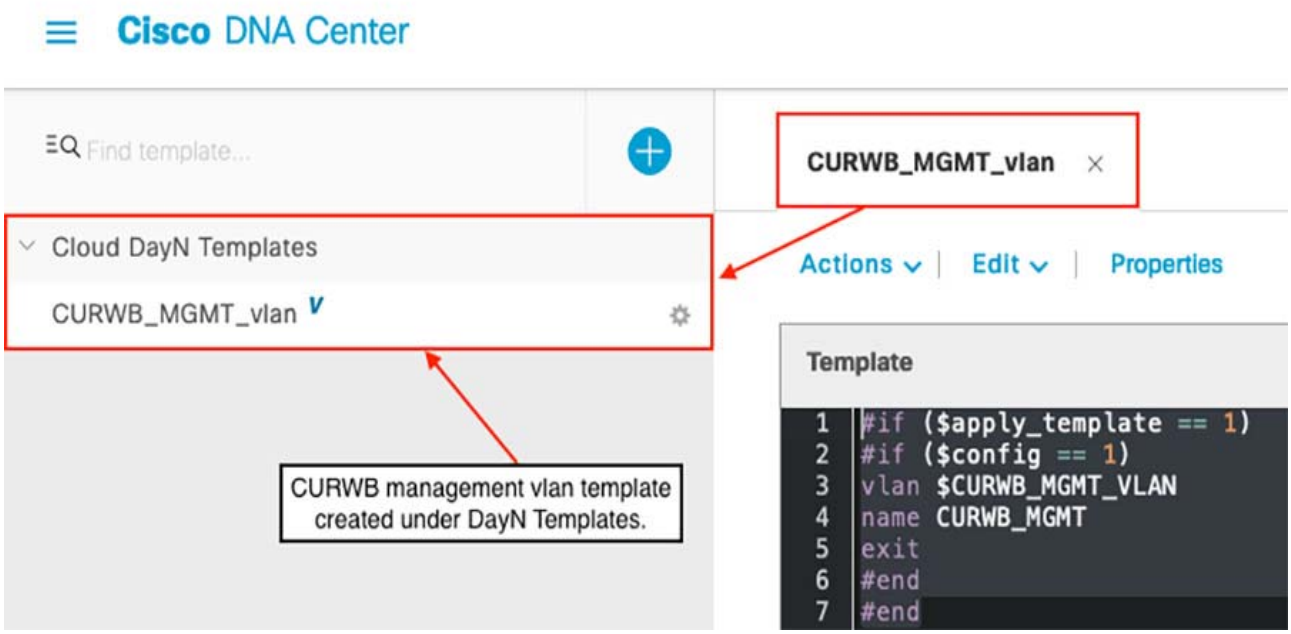
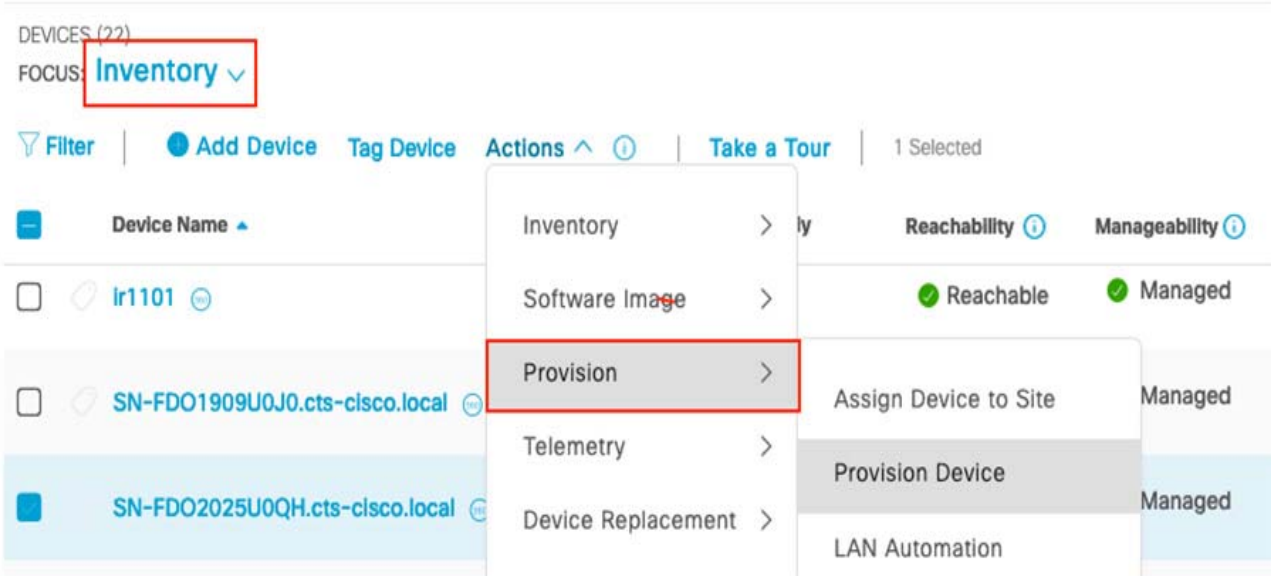
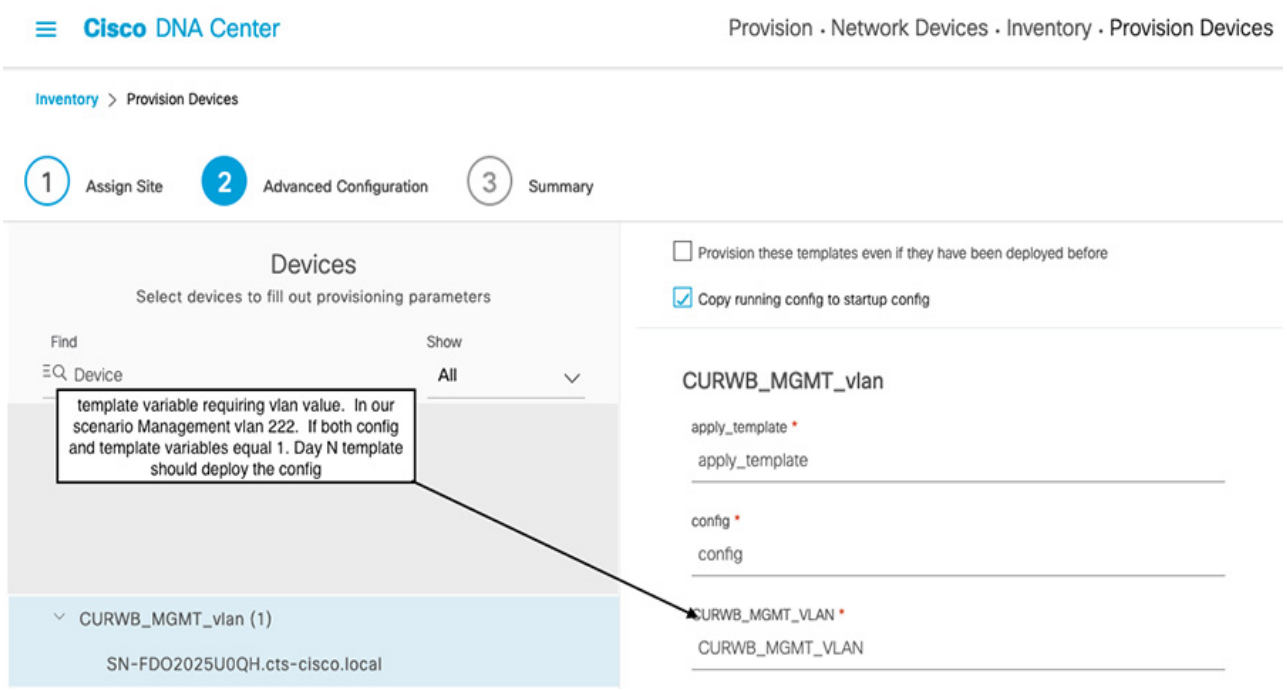


Figure 86 Optional CURWB management VLAN template deployed via DNA – C Inventory



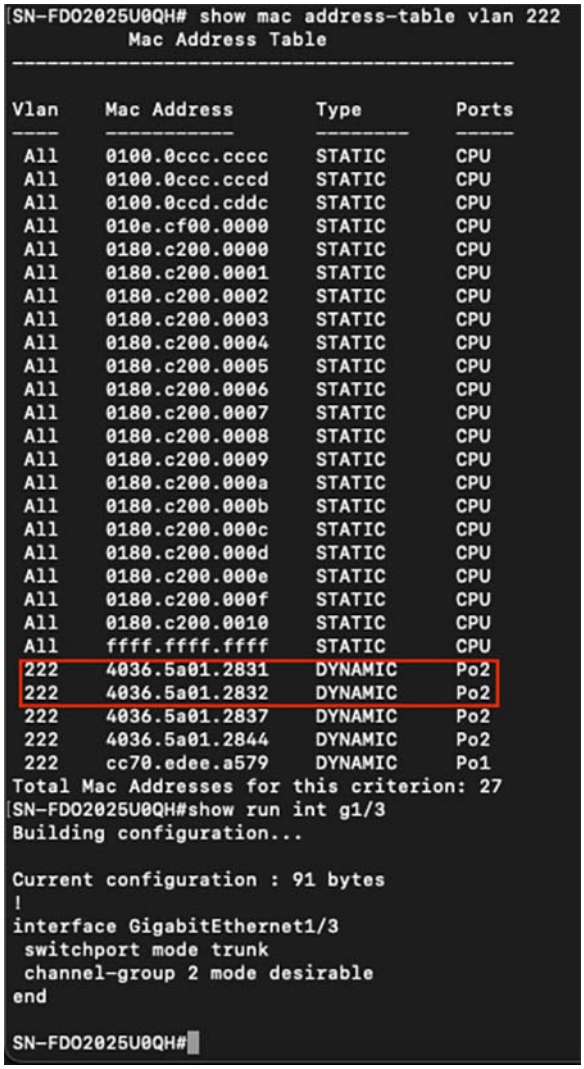
Select the newly-onboarded switch within the device inventory. In the screenshot above it is the Extended Node with device name SN-FDO2025U0QH.

Figure 87 CURWB DayN template - Advanced configuration



After configuring the management VLAN on the Extended Node manually or via template deployment, the CURWB radio MAC address displays in the MAC table with VLAN 222.

Figure 88 CURWB layer 2 MAC Addresses



```
SN-FDO2025U0QH# show mac address-table vlan 222
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0ccd.cddc    STATIC      CPU
 All    010e.cf00.0000    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
 222    4036.5a01.2831    DYNAMIC     Po2
 222    4036.5a01.2832    DYNAMIC     Po2
 222    4036.5a01.2837    DYNAMIC     Po2
 222    4036.5a01.2844    DYNAMIC     Po2
 222    cc70.edee.a579    DYNAMIC     Po1
Total Mac Addresses for this criterion: 27
SN-FDO2025U0QH#show run int g1/3
Building configuration...

Current configuration : 91 bytes
!
interface GigabitEthernet1/3
 switchport mode trunk
 channel-group 2 mode desirable
end

SN-FDO2025U0QH#
```

In the screen capture above, the CURWB radio is connected to interface Gigabit Ethernet 1/3 with port-channel 2. The MAC address table displays the corresponding radio MAC address with the radio management VLAN tag, VLAN 222 in this case.

QoS and Traffic Shaping

QoS can only be enabled through the RACER configuration or CLI, and not the web Configurator. Enabling QoS on the radio is recommended. Marking and queuing is best left to the connected switch.

It is important to note that although the current IE switching platforms supports Gigabit Ethernet speeds, the CURWB radios have a maximum throughput capacity of 500 Mbps which is a best-case scenario. Actual throughput speeds may vary due to the nature of the wireless environment in which they are deployed. Plan to shape the traffic to 10% below the max capacity to increase stability over the wireless bridged nodes. In the following example, a traffic policy was implemented at 150 mbps based off a link capacity of 166 mbps and configured on the switch connecting to the CURWB radios.

A parent shaper using the Default class map is used to match all traffic.

Policy-Map FM_port_shaper

```
    Class class-default
      Shape average 150000000 (bps)
```

A Service policy is applied in the Egress direction on CURWB facing interfaces.

```
interface GigabitEthernet1/3
 switchport mode trunk
 channel-group 2 mode desirable
service-policy output FM_port_shaper
```

CURWB radios can transmit telemetry traffic and situational alerts to the FM monitor dashboard in real time. For QoS, this traffic is sent as Best Effort from the management VLAN. The following configuration is used in this deployment to help prioritize the telemetry traffic leaving the radio and reduced latency and delay in reaching the destination Monitor application.

Access list permitting the CURWB management network to FM Monitor dashboard

```
ip access-list extended ef_FM_Telemetry
permit ip 10.8.1.0 0.0.0.255 host 172.16.155.2
```

Class map must match the access-group defined in the access list

```
Class-Map match-all FM-Telem_to_EF
   Match access-group name ef_FM_Telemetry
```

Policy map must contain the class previously defined and marked according to desired DSCP/COS value

```
Policy Map FM-Telem_to_EF
    Class FM-Telem_to_EF
      set dscp ef
```

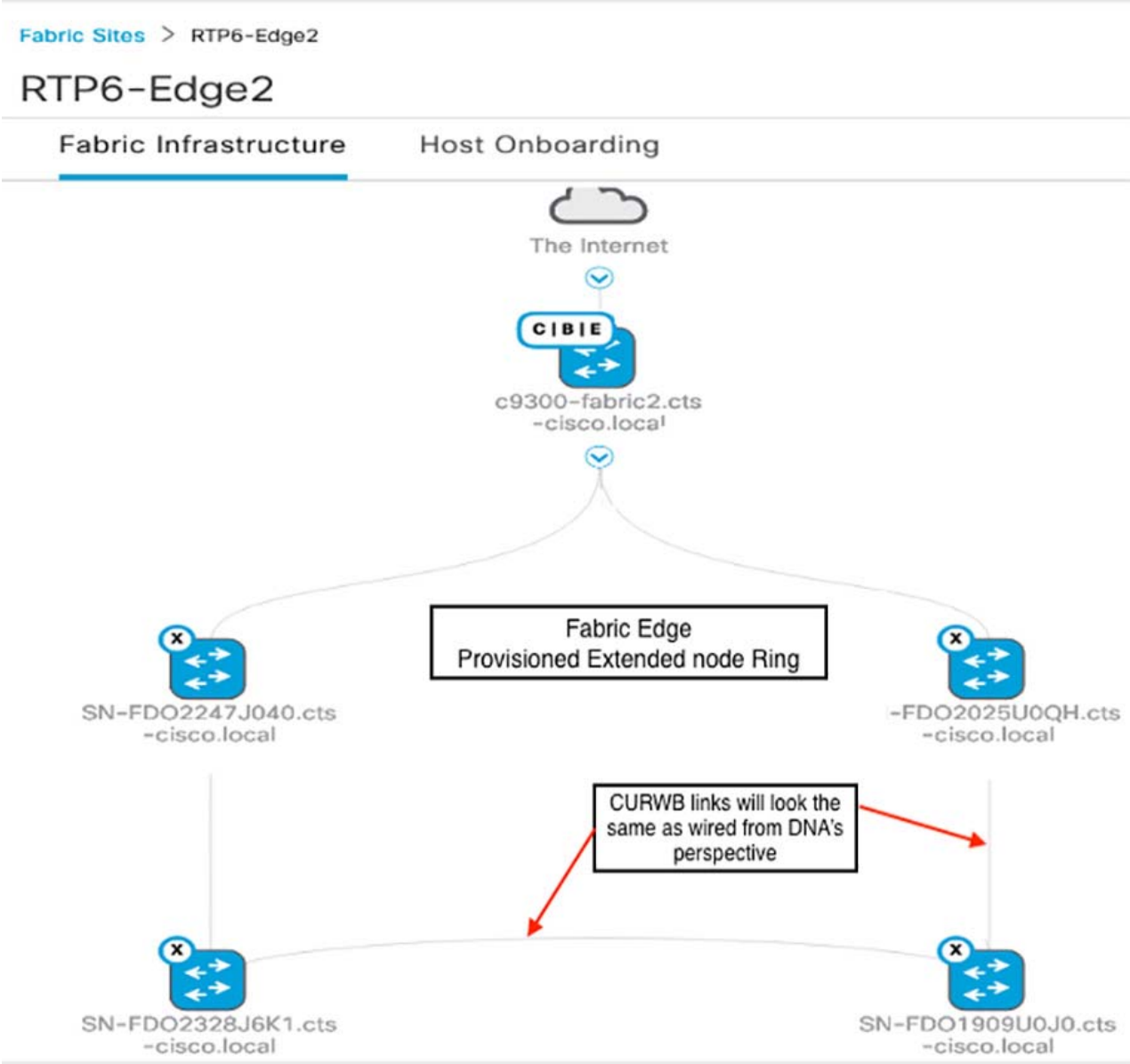
Service policy to be applied in the Ingress direction on all CURWB facing interfaces

```
interface GigabitEthernet1/3
 switchport mode trunk
 channel-group 2 mode desirable
 service-policy input FM-Telem_to_EF
 service-policy output FM_port_shaper
```

REP Ring and Daisy Chain Workflows

The process above describes the steps to configure CURWB and onboard a single EN over wireless bridge links. To form Ring and Daisy Chain Topologies, connect additional ENs in daisy chain format and repeat the steps as needed to onboard additional ENs over the wireless bridge.

Figure 89 DNAC Fabric Edge topology view

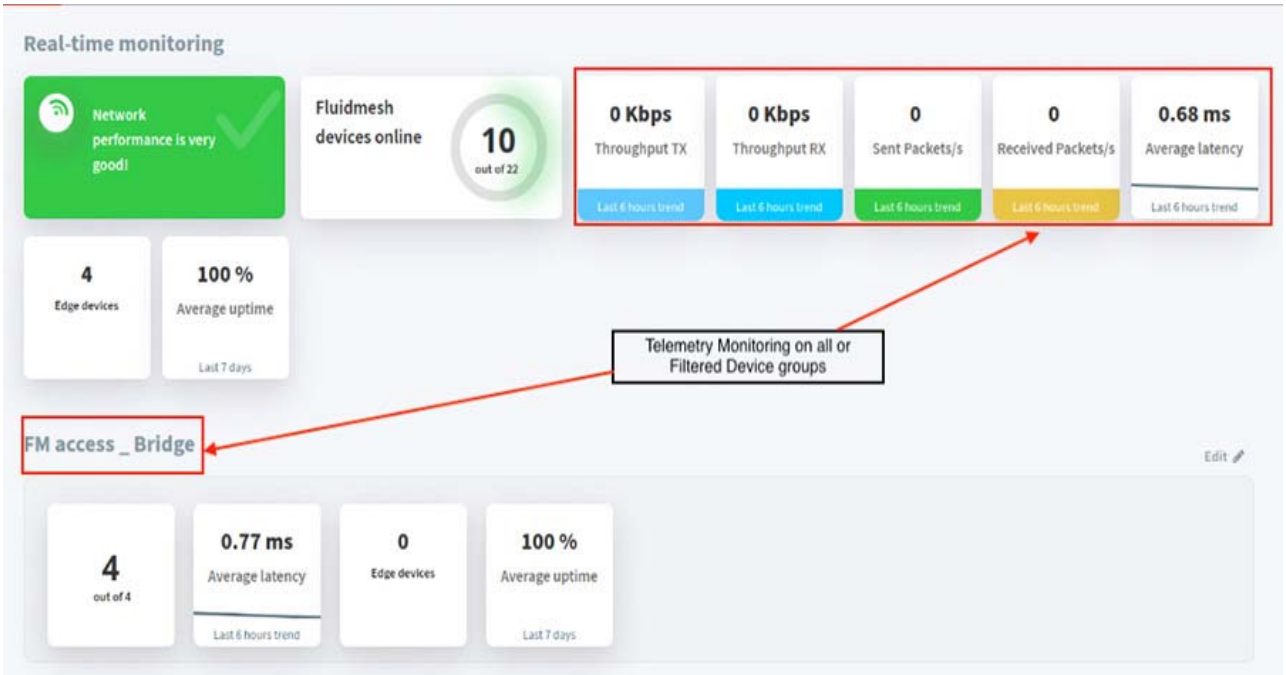


The CURWB connected interfaces and the wired ethernet interfaces form the 5-ring Extended node topology from DNA Center shown in the above screen capture.

FM Monitor

Cisco FM Monitor is a network wide, on-premises monitoring dashboard, allowing any CURWB customer to proactively maintain and monitor one or multiple more CURWB networks. The dashboard displays in real time, situational alerts and telemetry data in real time from every CURWB device in a network. It can work as a standalone system or in parallel with a Simple Network Management Protocol (SNMP) monitoring tool. For more details please review your device user guide.

Figure 90 FM Monitor Dashboard



FM Monitor displays and tracks real-time Key Performance Indicators (KPIs) within each administrative cluster, including the number of active radios, number of connected IP edge devices, end-to-end latency, jitter, upload/download throughput in real time, and system uptime . The following table view displays the CURWB units used in this deployment.

Figure 91 Table View

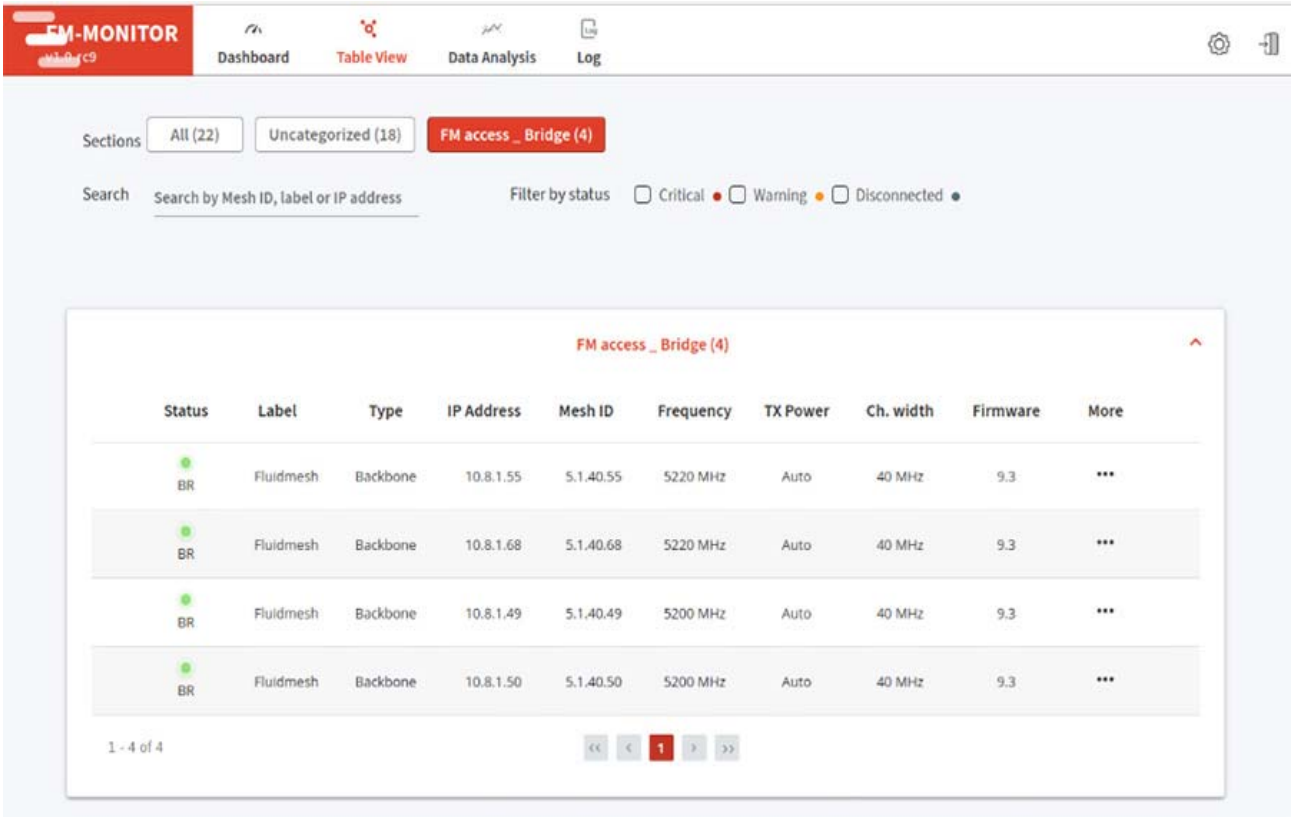


Figure 92 More Device Telemetry

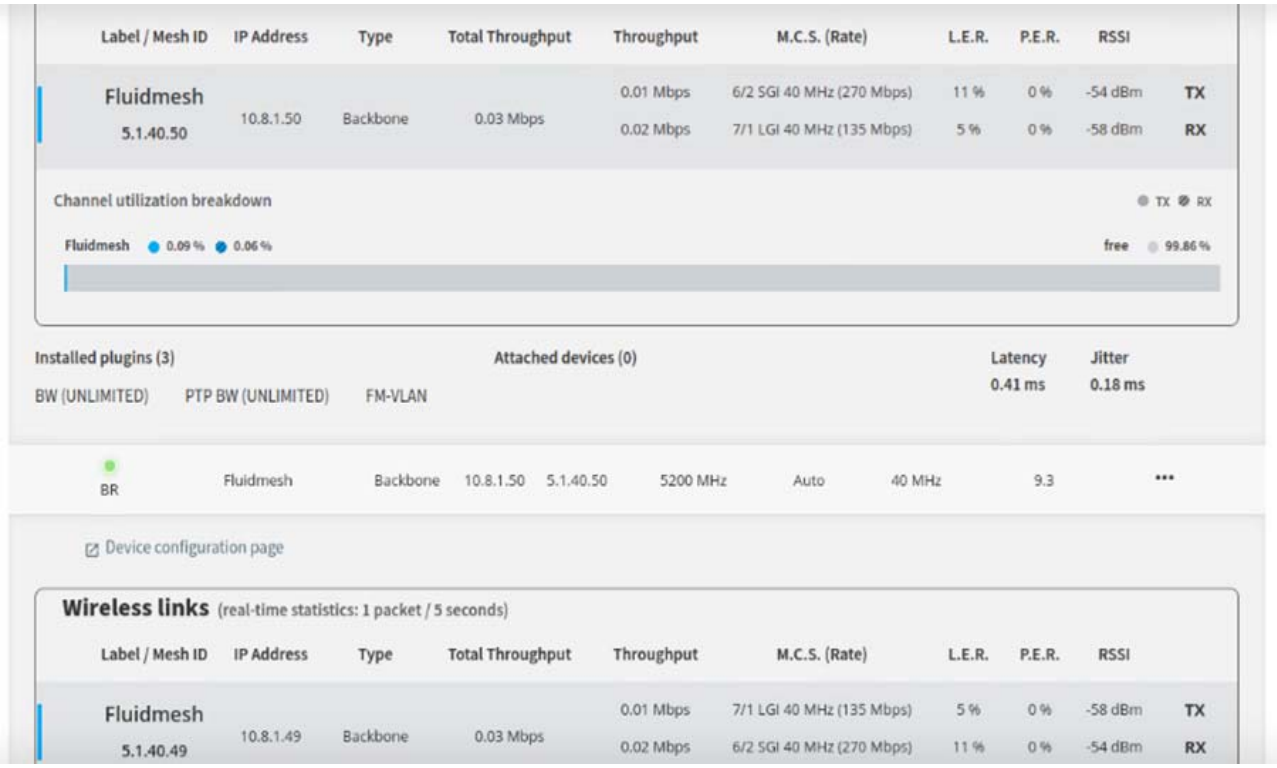
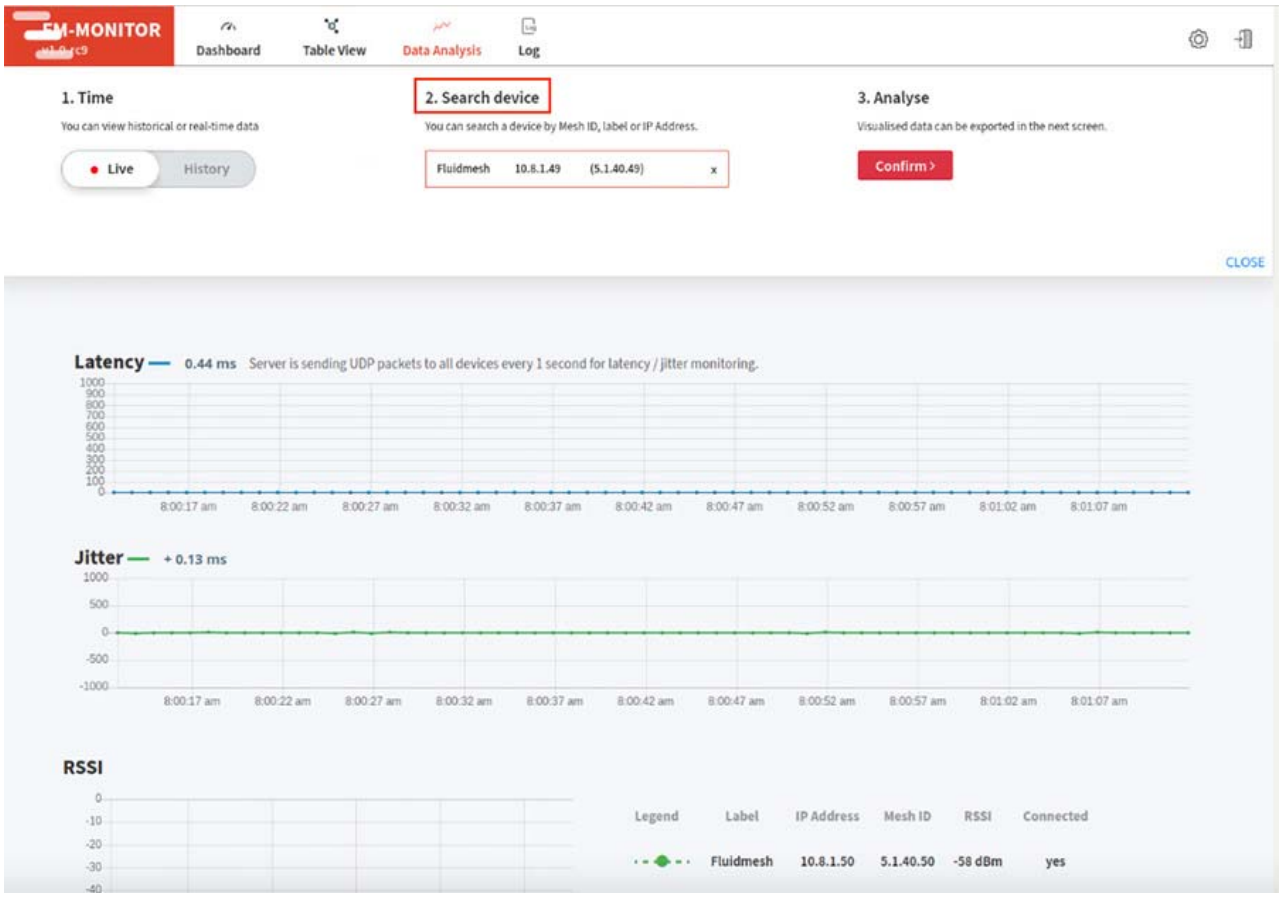


Figure 93 Data Analysis



To add a CURWB radio for monitoring, click the Settings icon and then click the Devices widget. The “add new device button” message appears in the upper right of the display window. Click this field and input the CURWB IP address. If the device is reachable, a success message is displayed, and the status will displays as green (online).

Figure 94 Adding a Device to Monitor

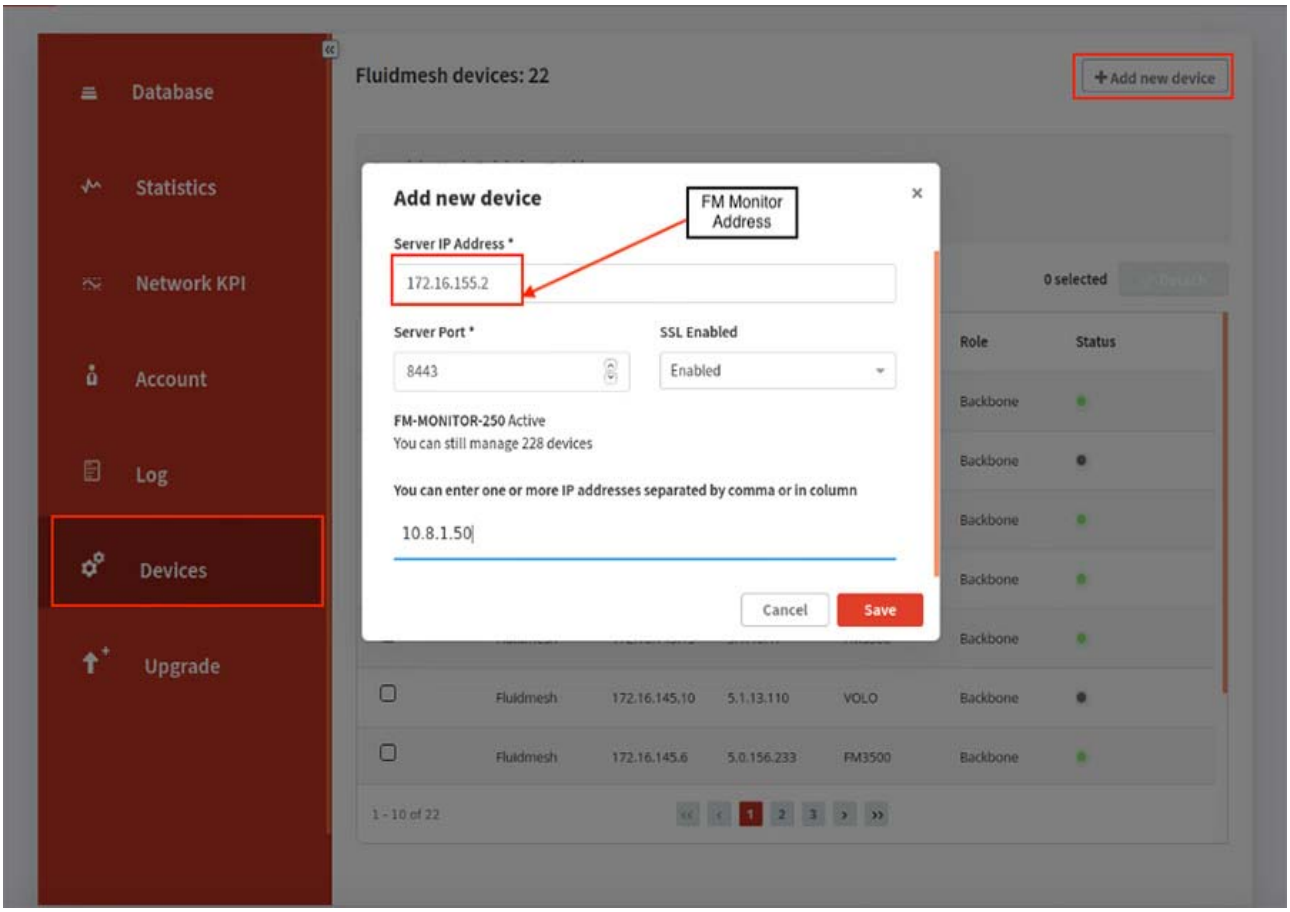
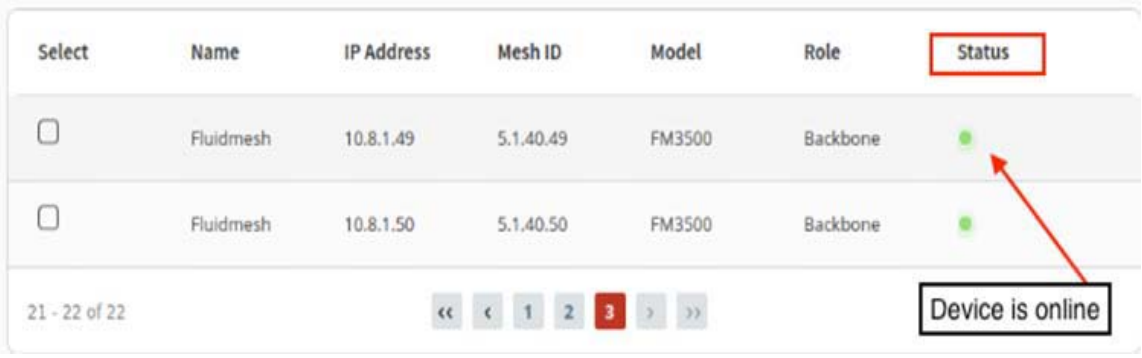


Figure 95 FM Monitor added CURWB radios



Implementing Cisco Resilient Mesh Access Network

Refer to Implementation of the Field Area Network, page 176 for more details about CR-Mesh access network implementation.

Implementing LoRaWAN Access Network

LoRaWAN is a media access control (MAC) protocol for wide area networks defined by the LoRa Alliance (https://www.lora-alliance.org) on top of the LoRa radio physical layer. The LoRa Alliance is an open and nonprofit standards association that includes hundreds of registered members from service providers, solution providers, service integrators, application developers, and sensor and chipset manufacturers. It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections.

Cisco Wireless Gateway for LoRaWAN is a module from Cisco Internet of Things (IoT) extension module series (IXM Gateway). It can be connected to the Cisco 809 and 829 Industrial Integrated Services Routers (IR800 series) or be deployed as standalone for low-power wide-area (LPWA) access. It is a carrier-grade gateway for indoor and outdoor deployment, including harsh environments.

- https://www.cisco.com/c/en/us/solutions/internet-of-things/lorawan-solution.html

There are two LoRaWAN gateway deploy modes as below:

- Virtual interface mode—IR800 series including the LoRaWAN module as a virtual interface
- Standalone mode—The LoRaWAN module working alone as an Ethernet backhaul gateway or attached to a cellular router through Ethernet.

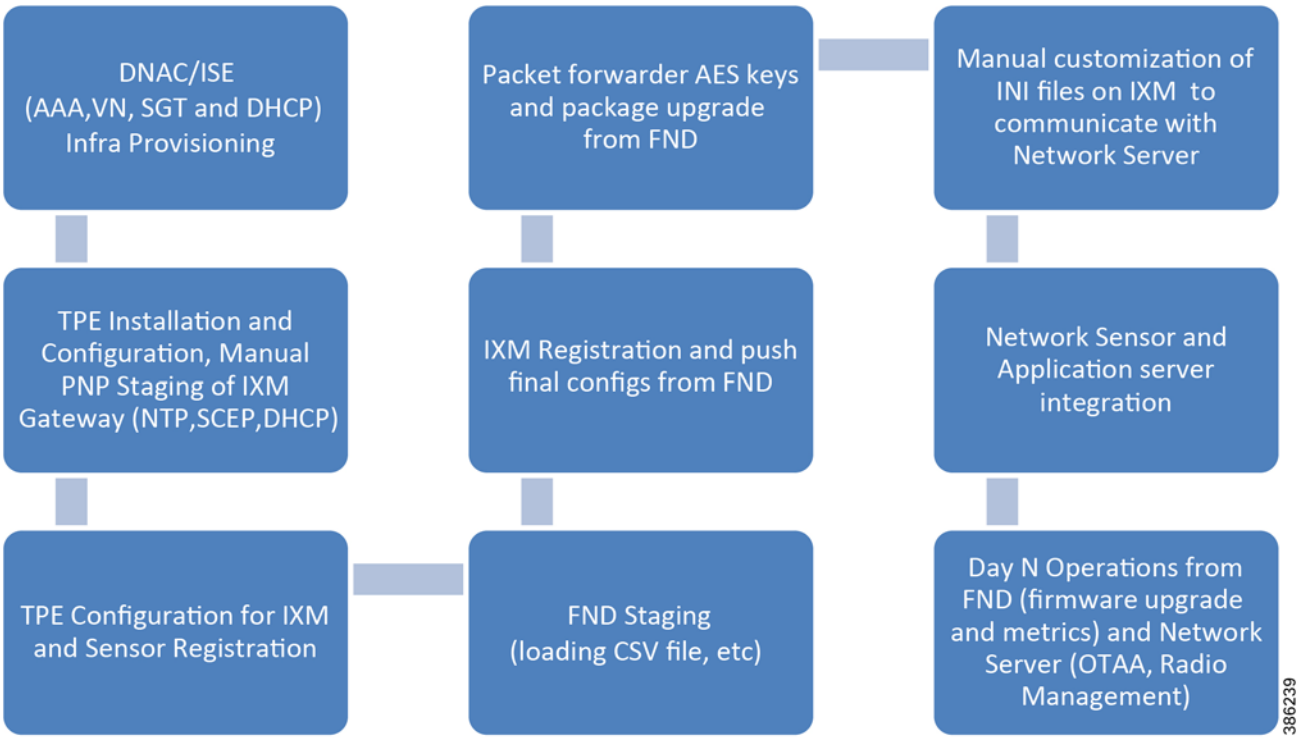
FND can manage IXM Gateway in both virtual and standalone mode, the deployment options of IXM are as shown in Table 16.

Table 16 LoRaWAN Deployment Options

Gateway Management with FND	Deployment Options	Backhaul
One Box Management (Stand Alone Mode)	IXM connected to IE Switch for Ethernet BackHaul	IXM connected to CCI Access Ring for Ethernet Backhaul and PoE
	IXM connected to IR1101/IR829 for Cellular Backhaul	IR1101 as Remote PoP Gateway IXM is connected to IR1101 for POE and Cellular connectivity
Two Box Management (Virtual Interface Mode)	IR829+ IXM as Virtual LPWA	IR829 as Remote PoP Gateway and IXM as Extended LPWA interface

The LoRaWAN access network implementation workflow is shown in Figure 96:

Figure 96 LoRaWAN Access Network Implementation Workflow



The transport of LoRa traffic from LoRaWAN (IXM) gateway to reach ThingPark Enterprise (TPE) and FND is via CCI Backhaul (local PoP) or Cellular Backhaul (Remote PoP). IXM is deployed at local PoP and remote PoP (discussed in later section) and forwards LoRa traffic from sensors in range towards TPE with the help of the Long Range Relay (LRR) packet forwarder that is installed on the gateway.

This section will discuss the Installation and Configuration of TPE, on-boarding of IXM Gateway in TPE and FND in Local PoP. LoRa Gateway is operated in Stand-alone mode and connected to CCI Network. Here the CCI Network will provide the reachability to TPE and FND (Users can connect IXM to IR1101 or IR 829 for Cellular backhaul which will be discussed in Remote PoP Section).

Note: LoRaWAN operating in Virtual mode behind IR8x9 is discussed in Remote PoP with LoRaWAN Access Network, page 252.

Installing and Configuring TPE

TPE is used for managing IXM gateway, sensors, and applications. TPE helps configure RF channels on the IXM gateway and allows coupling sensors and applications so that sensor data gets forwarded to their respective application.

Prerequisites:

In CCI, IXM Gateway is connected to the CCI network over cellular backhaul and TPE is installed in the Data Center (obtain installation and configuration guide from Actility). After installing TPE, IXM needs to be configured to connect it to TPE (obtain IXM installation and configuration guide from TPE dashboard download link). Sensors and applications are configured on TPE. The IXM gateway in range of sensors transports data to application via TPE.

Note: Currently, TPE supports only Over The Air Activation (OTAA).

For details about ThingPark Enterprise, refer to the following URL:

- https://www.actility.com/enterprise-iot-connectivity-solutions/

Onboarding a Cisco IXM Gateway for TPE Connectivity

Onboarding Cisco IXM Gateways includes the following steps:

1. Bring up the Cisco IXM Gateway .
2. Perform the initial configuration on Cisco IXM Gateway.
3. Install the packet forwarder.
4. Perform the LRR packet forwarder configuration.

For details on how to perform each of these steps refer to :

- https://www.thethingsnetwork.org/docs/gateways/cisco/setup.html

Refer to the sample Cisco IXM gateway configuration below:

```
cci#show running-config
!
enable secret 8 ****
!
hostname cci
!
ip domain lookup
ip domain name actility.local
!
ip name-server 10.0.1.6
!
interface FastEthernet 0/1
ip address dhcp
          exit
!
username admin password 8 ****
!
ip ssh admin-access
!
ntp server address 10.0.1.1
!
clock timezone America/Los_Angeles
```

Bringing up IXM -TPE Connectivity

To bring up the connectivity between Cisco IXM and TPE following these steps:

1. Ensure reachability between IXM and TPE exists.
2. Edit the credentials.txt (found at ln $ROOTACT/usr/etc/lrr –in standalone mode of IXM) to reflect the configured credentials as below:

   1st line: enable password

   2nd line: user account on IXM LoRaWAN GW

   3rd line: password for the user account

   A sample of the same is shown in example below:

```
credentials.txt:
        cisco
        admin
```

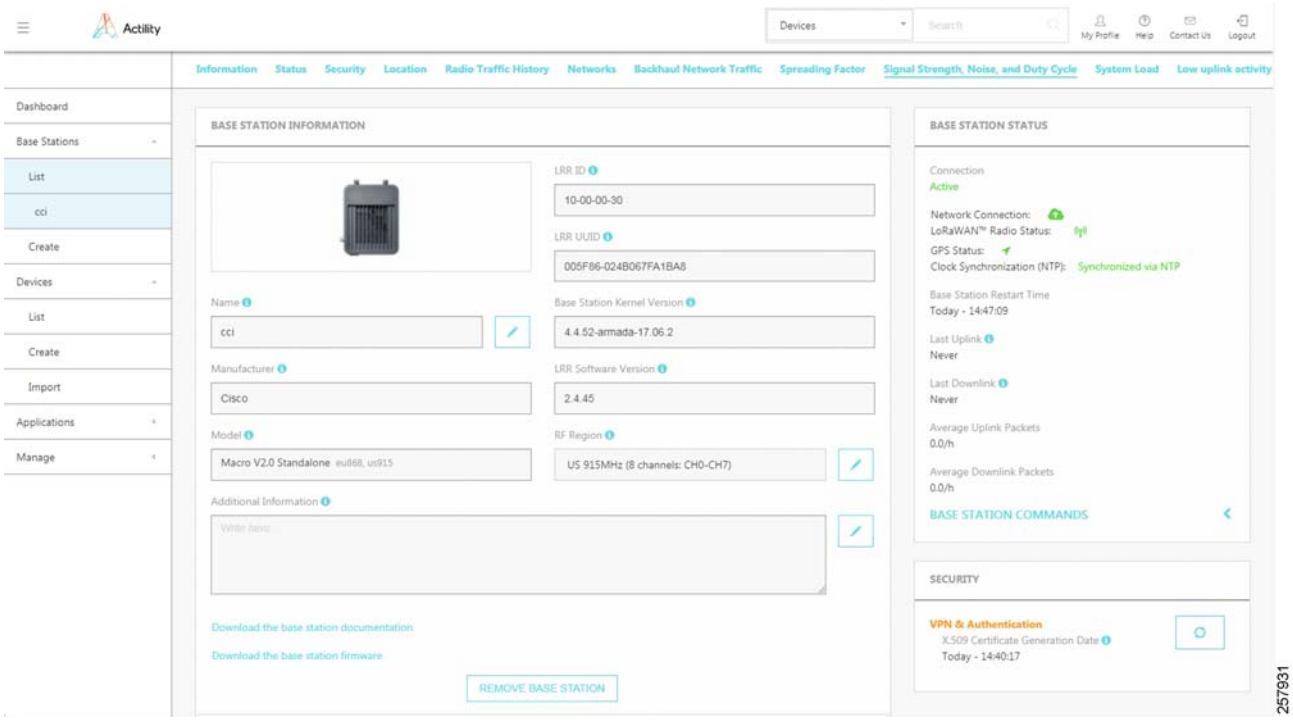
```
cisco
```

3. Edit the $ROOTACT/usr/etc/lrr /lrr.ini file to reflect the TPE address set-up the FTP address as shown in example below:

```
lrr.ini:
;
File generated by moreini.x 2019/03/12 07:20:03;
[download:0]
ftpaddr=172.16.3.2
ftppass=[558d3b006f639a810bbb8e33caa6a769]
ftpport=21
ftpuser=ftp-lrc
use_sftp=0
[download:1]
ftpaddr=
[ifacefailover]
enable=0
[laplrc:0]
addr=tpe-cci.actility.local
iec104t1=60
port=2404
type=${LK_TCP_CLIENT}|${LK_SSP_SLAVE}|${LK_SSP_RECONN}|${LK_TCP_NONBLK}
[laplrc:1]
addr=
[lrr]
nblrc=1
uidmode=fromtwaonly
usegpstime=0
[services]
checkvpn2=0
ipfailover=0
[suplog]
networkconfiginterfile=/tmp/mdm/pktfwd/firmware/usr/etc/lrr/interfaces.config
networkconfigntpfile=/tmp/mdm/pktfwd/firmware/usr/etc/lrr/ntp.conf
networkconfigtpe=1
networkconfigvpnfile=/tmp/mdm/pktfwd/firmware/usr/etc/lrr/vpn.cfg
nfr920=0

[support:0]
addr=172.16.3.2
ftpaddr=172.16.3.2
ftppass=[791551405f8f938548a7d4cef3ccf779]
ftpport=21
ftpuser=ftp-support
pass=[2ca6e5f79a74b74382bc2eeebb21085b]
pass_crypted_k=0
port=22
use_sftp=0
user=support
[support:1]
addr=
ftpaddr=
[trace]
level=1
[versions]
configuration_version=
custom_build_version=
hardware_version=cisco_standalone
os_version=2.0.32
```

4. Set up the base station following the steps given in the installation guide TP_Enterprise_BS_Installation_Guide_cisco_CISCO_cixm.1_v2.2 (downloaded from the TPE dashboard when setting up the prerequisite).
5. Push the Rf region file from the TPE dashboard to the IXM. Confirm and wait for a successful push.
6. Check the lgw.ini and channels.ini files are now in $ROOTACT/usr/etc/lrr.
7. Restart the packet forwarder.
8. After completion of the steps the Base station must be shown as active in the connection status of the TPE dashboard as shown in Figure 97.

Figure 97 Actility Base Station Detailed View–Connected



An application must be created before provisioning a LoRa sensor.

Following are the steps to be followed in TPE to create the application:

1. On the TPE go to **Applications-> Create-> Generic application**.
2. Fill the details of the Application to be created and click **Save.**
3. The application is now setup and will appear as shown in Figure 98 when navigating to **Application -> List**.

Figure 98 Application in TPE

Setting up an example PNI sensor in TPE

Before beginning to setup the PNI sensor, make sure the sensor is installed and activated.

Refer to the following URL for the steps:

- https://www.pnicorp.com/wp-content/uploads/PNI-PlacePod-Vehicle-Detection-Sensor-User-Manual-1.pdf

To setup the PNI sensor in the TPE perform the following steps.

1. Go to **Devices -> Create.**
2. Fill in the sensor related details.
3. In Application select the application in previous step.
4. Finally click **Save**.

The sensor is now setup and the sensor data must now be traversing to the application.

FND Configuration for IXM Gateway

IoT FND supports the following configurations for the Cisco Wireless Gateway for LoRaWAN:

- Firmware upgrade.
- Hardware monitoring and events report.
- IP networking configuration and operations (for example, IP address and IPsec).
- Initial installation of the Thingpark LRR software.

This section contains the following topics:

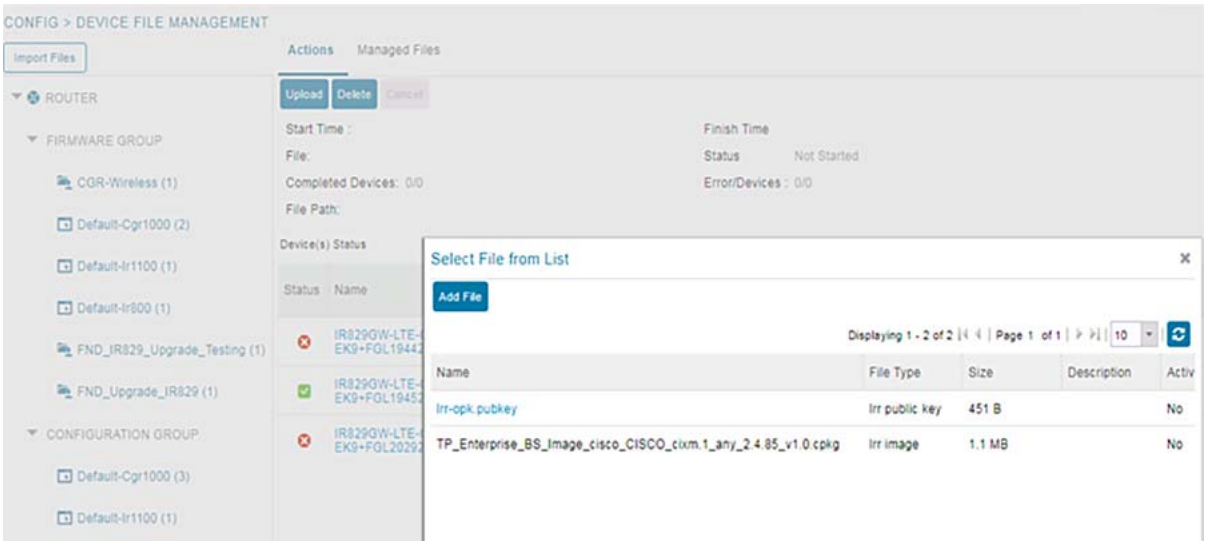
Preparing FND for IXM ZTD

In CCI scenario, we are on-boarding IXM Gateway without using TPS (Tunnel Provisioning Server), the IGMA based configurations has been provisioned on Gateway manually. After provisioning of IGMA based configuration, gateway triggers registration request from the device. SCEP enrollment is used for certificate-based authentication.

Procedure:

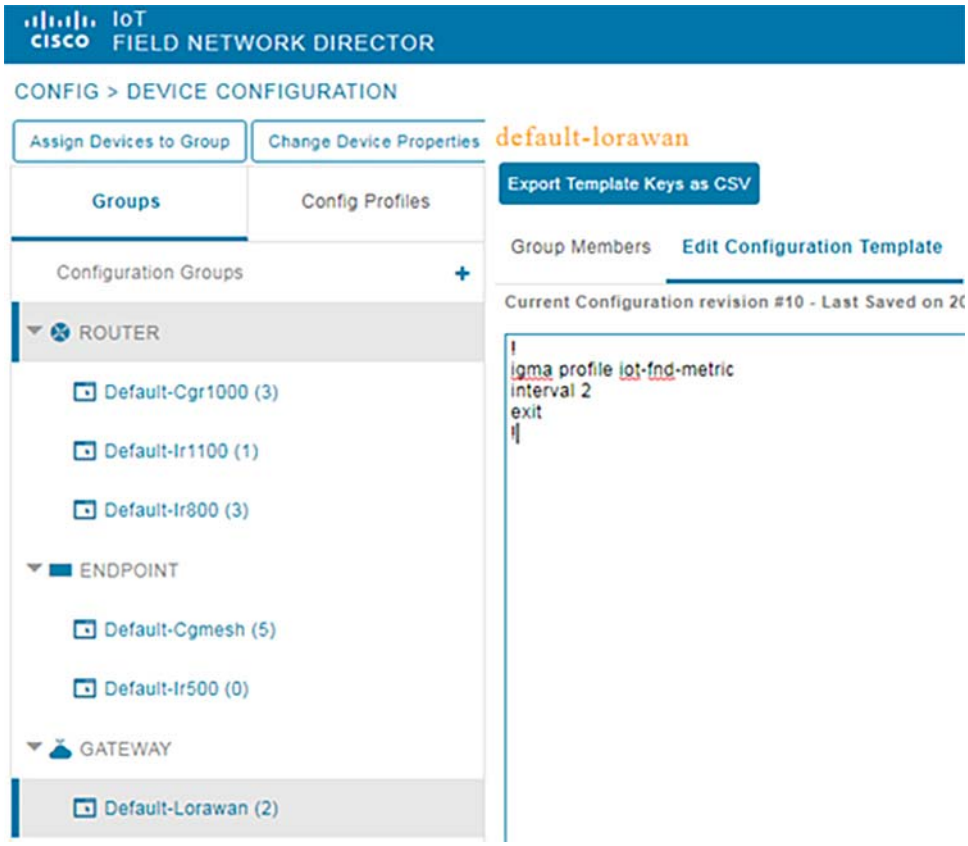
Step 1: Add the Actility LRR and public key to FND by clicking the import button on the File Management page. On **FND UI,** select **Config -> Device File Management -> Actions**, click **Upload**. Select **Add File** option, Upload Actility LRR and public key, and select **Upload File** option.

Figure 99 Uploading LRR Image and Public Key into FND



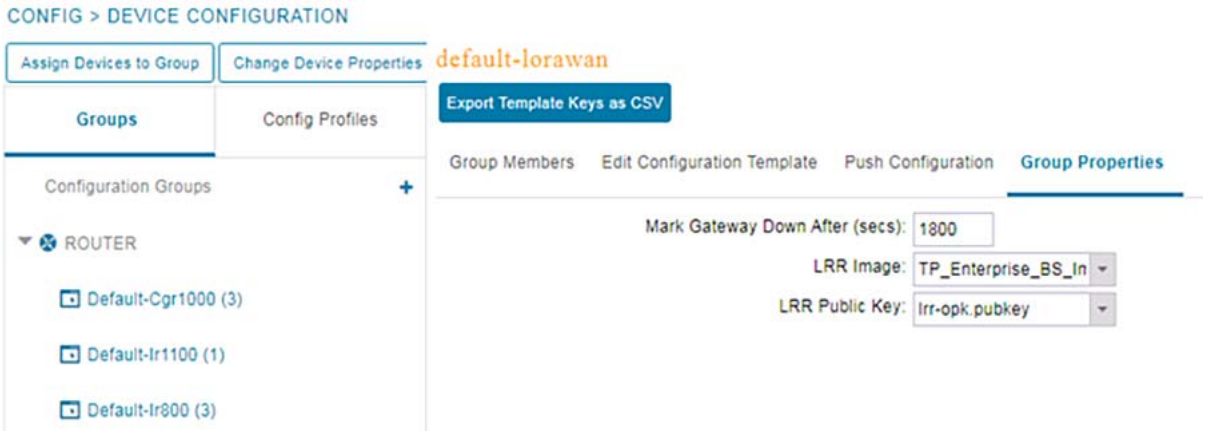
Step 2: On FND UI, select **Config -> Device Configuration** page, select **default-lorawan** and **Edit Configuration Template**, and update the Device Configuration group with the following parameters and save the changes. Figure 100 shows a sample configuration.

Figure 100 Default Configuration Template in FND for IXM



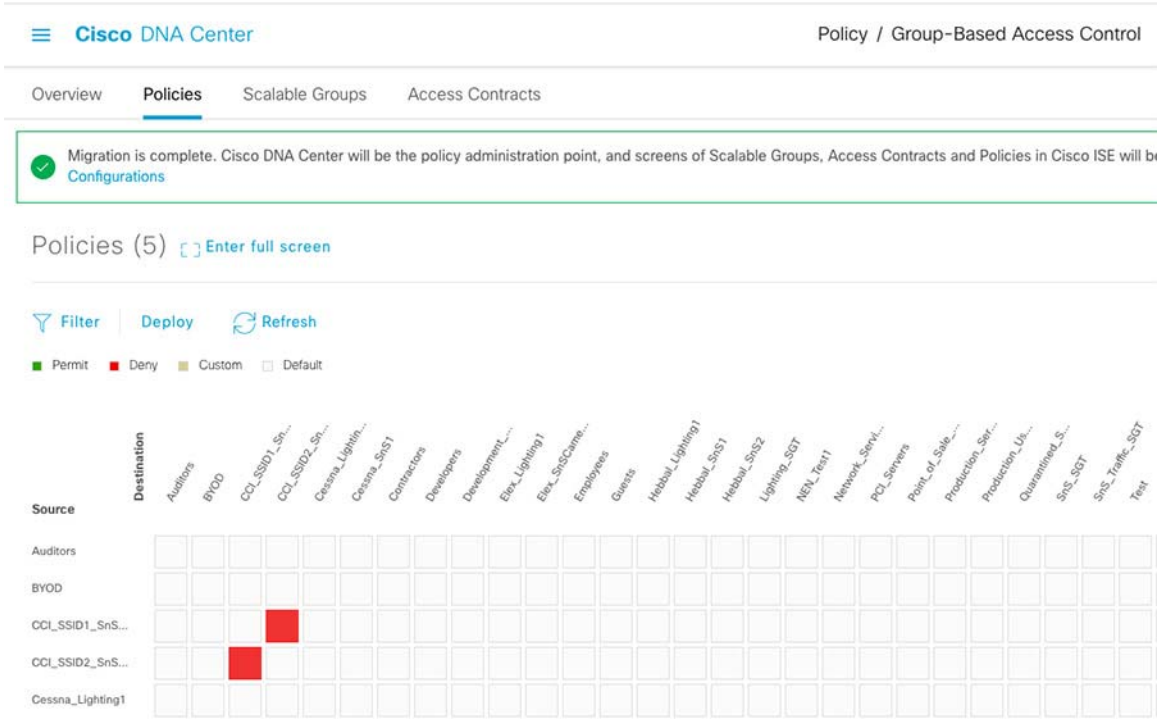
Step 3: On FND UI, select **Config** -> **Device Configuration** page, select **Default-Lorawan**, **Edit Group properties**, and select **LRR Image** and **LRR Public Key**, which user uploaded in step 1 as shown in Figure 101.

Figure 101 Default Configuration with Group Properties for LRR Image and Public Key Upload in FND for IXM



Step 4: The Provisioning Settings page will have the FND common name populated in IoT-FND URL as shown in Figure 102 (not mandatory to use this step for verification).

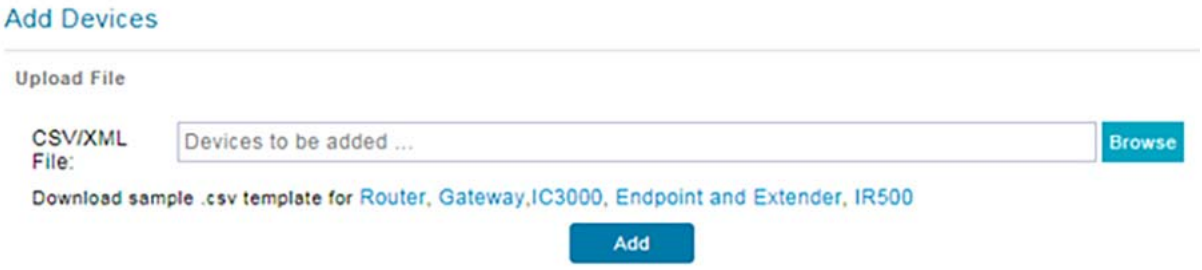
Figure 102 Provisioning Settings in FND



Step 5: Add the IXM Gateway into FND as a **Lorawan Device** using CSV file. Select **Devices**-> **Field Devices**-> **Add Devices** and insert csv file with the following details:

```
eid,deviceType
IXM-LPWA-900-16-K9+FOC123456R5,lorawan

 eid is combination of device type + Serial number of device. User can get this details using 'show
version' command.

devicetype is lorawan.
```

Figure 103 Adding Devices into FND



Step 6: The user needs to provision configuration on IXM Gateway for triggering registration request. Make sure the firewall allows ports 9120, 9121, 9122, all of the SSH, telnet, and DHCP ports. User has to obtain certificates from the CA (the same ones used to issue certs for FND). Execute the **show ipsec certs** command to verify.

1. Basic Reachability to FND and RSA CA Server and IP Addressing.

```
hostname Gateway
```

```
!
ip domain lookup
ip domain name cimconccibgl.cisco.com
ip host cci-iot-fnd.cimconccibgl.cisco.com 10.10.100.90
!
interface FastEthernet 0/1
 ip address dhcp

ip default-gateway 172.21.90.1
!
```

2. Configure Username, NTP, and Enabling SSH.

```
username cisco password 8 ****
!
ip ssh authentication-retries 3
ip ssh admin-access
ip ssh port 22
ntp server ip 10.40.100.100
```

3. SCEP Enrollment to obtain CA certificates from CA server.

User can get certificates in two ways:

- One way is manually install the CA server certificate using USB manually.
- Another way is via SCEP.

In this guide we have used SCEP to obtain the certificates.

```
!
ipsec cert scep http://172.17.70.10:80/certsrv/mscep/mscep.dll us ca mil cisco iot FOC123456R5 true
ndes true 2048
!
ipsec enable
!
```

Note: In the above SCEP enrollment it is best practice to give device ID as Name Of the Certificate.

4. IGMA profile has to be provisioned after SCEP.

The below configure is used to trigger the registration request from device.

```
igma secure enable
!
igma event destination cci-iot-fnd.cimconccibgl.cisco.com 5683
!
igma profile iot-fnd-register
 active
 add-command show fpga
 add-command show inventory
 add-command show ip interface FastEthernet 0/1
 add-command show ipsec status info
 add-command show platform status
 add-command show radio
 add-command show version
 interval 2
 url https://cci-iot-fnd.cimconccibgl.cisco.com:9121/igma/register
 exit
!
```

Note: If user is unable to provision igma profile, enter enable mode and configure the following command to enable igma.

```
Gateway#igma start
```

5. The user needs to add HER configuration manually, for example the tunnel crypto profiles and transform sets. Refer to the following URL for HER-based configuration (this step is not mandatory for IXM Gateway for Registration).:

- https://www.cisco.com/c/en/us/td/docs/routers/interface-module-lorawan/software/configuration/guide/b_lora_scg/b_lora_scg_chapter_01010.html

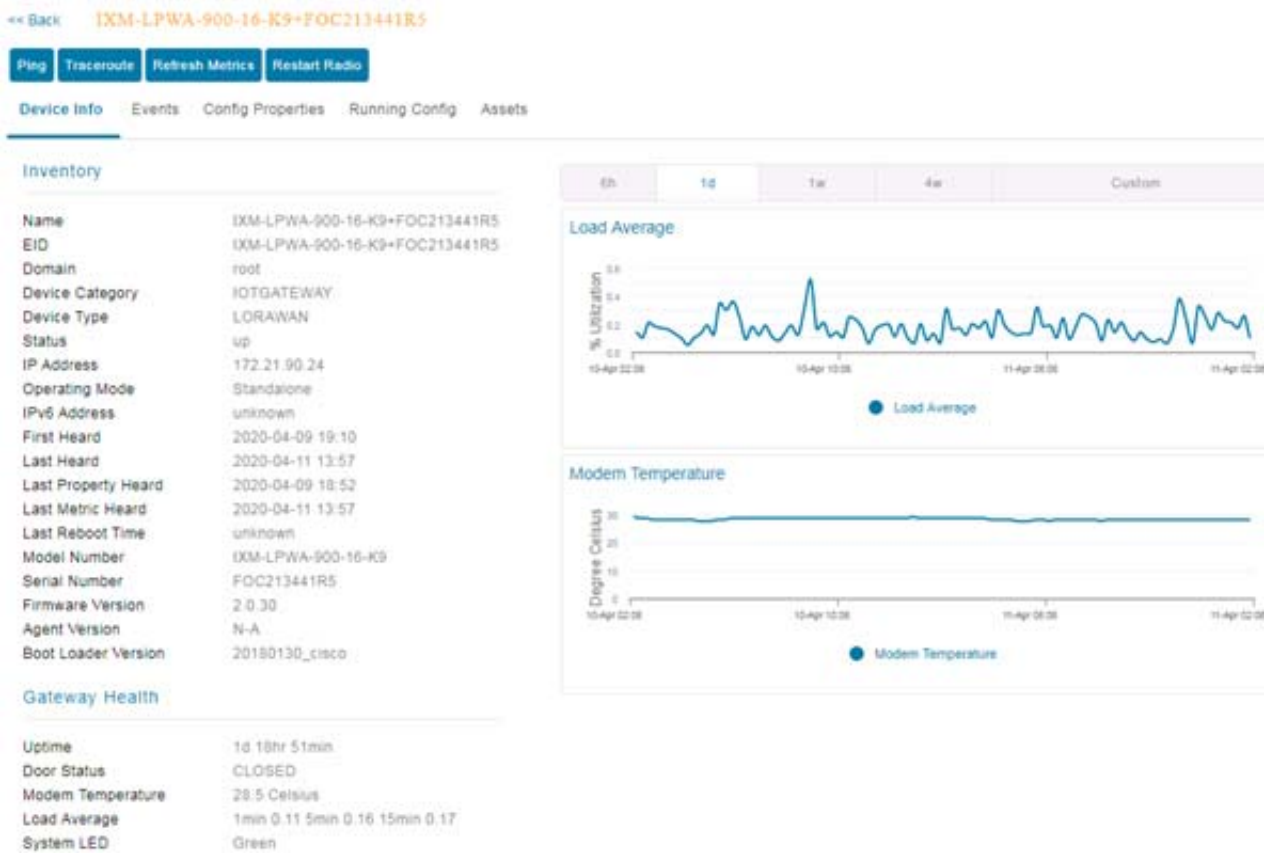
Step 7: Once the Modem is registered, the IXM will show as up in the FND. Check the following events if there are issues during provisioning.

Figure 104 Registration Request from Device in FND

2020-04-09 18:11:33:678	Registration Request	INFO	Registration request from LoRaWAN Gateway LoRaWAN Gateway Registration Request from EID [IXM-LPWA-900-16-K9+FOC213441R5].
2020-04-09 19:13:52:462	Registration Success	INFO	Registration of LoRaWAN Gateway successful.LoRaWAN Gateway Registration Success for EID [IXM-LPWA-900-16-K9+FOC213441R5].
2020-04-09 18:23:53:746	Registration Success	INFO	Registration of LoRaWAN Gateway successful.LoRaWAN Gateway Registration Success for EID [IXM-LPWA-900-16-K9+FOC213441R5].
2020-04-09 19:13:52:455	Up	INFO	LoRaWAN Gateway is up

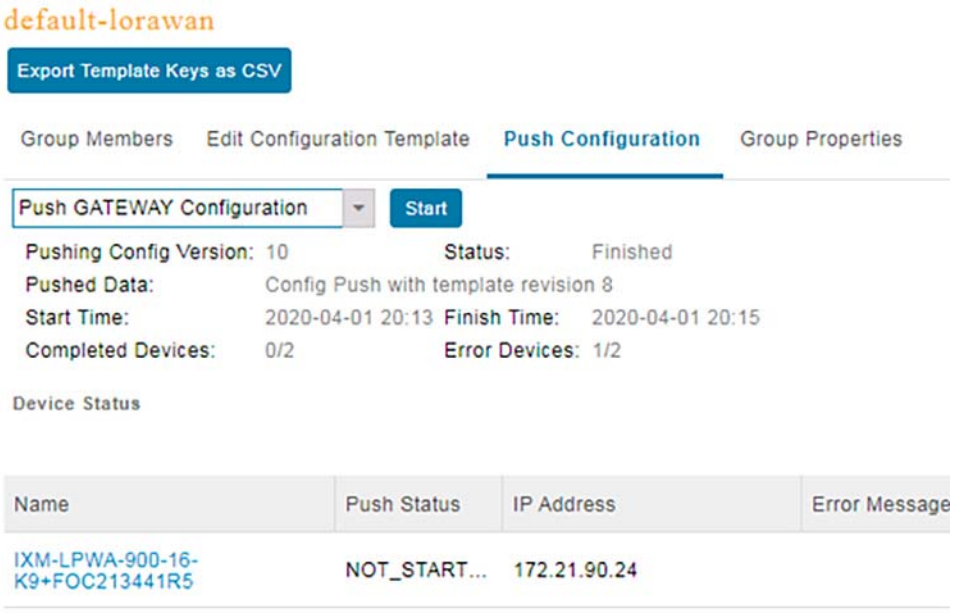
Step 8: Detailed IXM Gateway information can be viewed by clicking on the **IXM Gateway** tab.

Figure 105 IXM Gateway Dashboard Tab



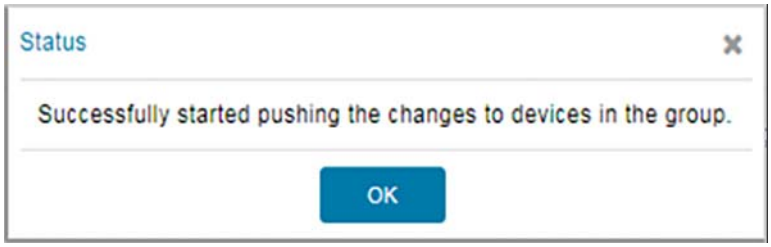
Step 9: If configuration update is required, follow the same procedure in Step 2, but in this case you invoke a configuration push. Select **Push Configuration tab**. On the drop-down menu, select **Push GATEWAY Configuration** and select **Start**.

Figure 106 IXM Gateway Configuration Push Tab



After the configuration push, the tab will show if the configuration is successfully pushed on to the device.

Figure 107 IXM Gateway Configuration Push Successful in FND



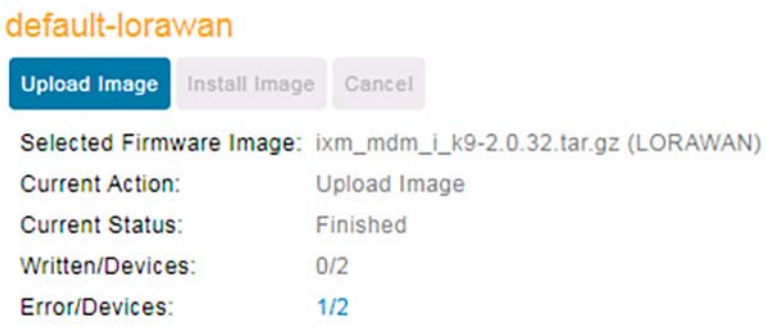
IXM Modem Firmware Update

Procedure:

Step 1: Load the Firmware Image into FND.

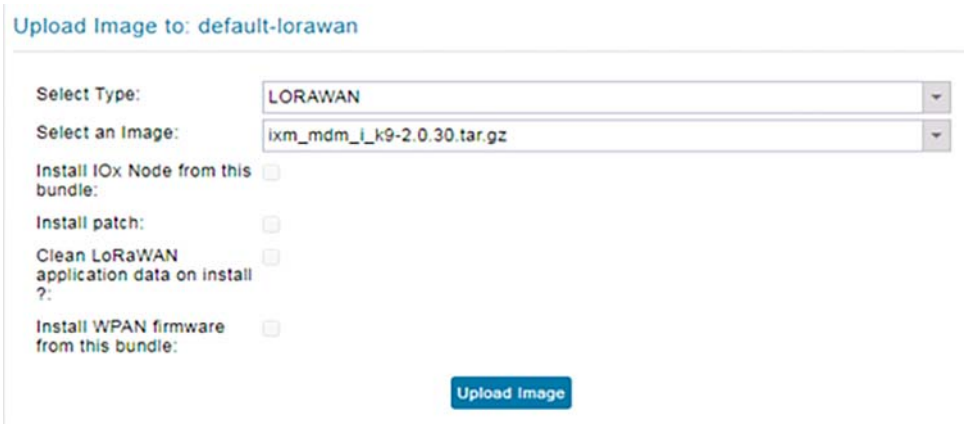
On FND UI, Select **Config -> Firmware Update** and select **Upload Image**.

Figure 108 IXM Gateway Image Upload Tab in FND



Step 2: Push the firmware to the IXM Gateway by selecting **LORAWAN** on the **Select Type** drop-down menu and select a firmware image on the **Select an Image** drop-down menu. If you want to erase the LRR or pubkey, select the clean install option as shown in Figure 109.

Figure 109 IXM Gateway Image Upload Tab in FND-2



Step 3: After upload is complete, install the image by clicking the **Install Image** button.

Figure 110 IXM Gateway Image Install

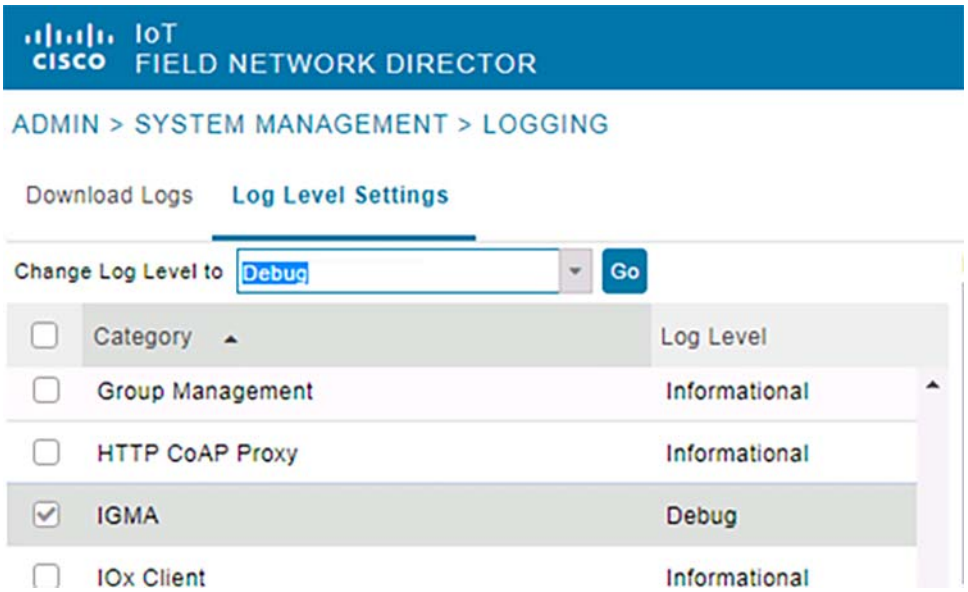
When the upgrade starts, a screen similar to Figure 111 is displayed.

Figure 111 IXM Gateway Successful Image Install

Troubleshooting

Enable the debug categories shown in Figure 112 on FND before troubleshooting.

Figure 112 FND Logging



1. FND does not have any messages from the IXM.
   - Make sure the IGMA profile is pointing to the correct FND profile and the name resolution is correct.
   - Make sure the FND can be pinged.
2. FND Registration failed.
   - Check the FND configuration template for command accuracy

Sample Running Configuration:

```
!
hostname Gateway
!
```

```
crypto ipsec profile primary
 ipaddr 192.168.200.1 iketime 86400 keytime 86400 aes 256
 exit
ip domain lookup
ip domain name cimconccibgl.cisco.com
ip host cci-fnd-oracle.cimconccibgl.cisco.com 10.10.100.90
ip host cci-iot-fnd.cimconccibgl.cisco.com 10.10.100.90
!
interface FastEthernet 0/1
 shutdown
 ip address dhcp
 exit
!
ip default-gateway 172.21.90.1
!
username cisco password 8 ****
!
ip ssh authentication-retries 3
ip ssh admin-access
ip ssh port 22
!
ntp server ip 10.40.100.100
ipsec cert scep http://172.17.70.10:80/certsrv/mscep/mscep.dll us ca mil cisco iot FOC213441R5 true
ndes true 2048
!

igma secure enable
!
igma event destination cci-iot-fnd.cimconccibgl.cisco.com 5683
!
igma profile iot-fnd-metric
 active
 add-command show fpga
 add-command show inventory
 add-command show ip interface FastEthernet 0/1
 add-command show ipsec status info
 add-command show led status
 add-command show packet-forwarder info
 add-command show packet-forwarder status
 add-command show platform status
 add-command show radio
 add-command show version
 interval 15
 url https://cci-iot-fnd.cimconccibgl.cisco.com:9121/igma/metric
 exit
!
igma profile iot-fnd-register
 add-command show fpga
 add-command show inventory
 add-command show ip interface FastEthernet 0/1
 add-command show ipsec status info
 add-command show platform status
 add-command show radio
 add-command show version
 interval 2
 url https://cci-iot-fnd.cimconccibgl.cisco.com:9121/igma/register
 exit
  !
```

For more details refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/interface-module-lorawan/software/configuration/guide/b_lora_scg.pdf

Implementing Wi-Fi Access Network

CCI covers two different Wi-Fi deployment types: Cisco Unified Wireless Network (CUWN) with Mesh, and SDA Wireless. This section covers the implementation of both CUWM Wi-Fi Mesh and SDA Wireless Wi-Fi (non-mesh) access networks.

Prerequisites:

- For CUWN deployment with Centralized WLC, WLC should be deployed in shared as covered in Implementing Centralized Wireless LAN Controller for Cisco Unified Wireless Network, page 46.

Implementing Cisco Unified Wireless Network Access in a PoP

The CUWN solution supports client data services, client monitoring and control, and rogue access point detection, monitoring, and containment functions. CUWN uses lightweight access points (APs), Cisco Wireless LAN Controllers (WLCs). In CCI, CUWN is deployed as “Over the Top (OTT)” as a non-native service. In this mode, the SD-Access fabric is simply a transport network for the wireless traffic. CUWN also leverages Cisco Prime Infrastructure for managing OTT Wi-Fi access network.

In a wireless mesh deployment, multiple APs (with or without Ethernet connections) communicate over wireless interfaces to form a mesh access network. The Flex+Bridge mode is used in CCI Wi-Fi Mesh network.

Refer to the following URLs for more details on Wi-Fi mesh:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_mesh_87.html
- https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_mesh_88.html

This section covers the CUWN implantation with C9800 WLC. The configuration steps are the same both for Centralized WLC deployment model and the Per-PoP WLC deployment mode.

For C9800 configuration guidance, refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html#anc34

Connecting AP to the IE Switch

In CUWN Mesh, Root Access point (RAP) Ethernet port is connected to the ring IE switches. In Cisco DNA Center 1.3.x, a dedicated AP VLAN with the name AP_VLAN and VLAN ID 2045 is created with a corresponding SVI interface. After you perform the VN-to-IP pool assignment under INFRA_VN for an AP pool, the IP address is assigned to the SVI interface.

In this example, VLAN ID 2045 is the SDAs INFRA_VN vlan, which we are associating to the AP infra Pool.

Refer to the section “Provisioning Devices using Cisco DNA Center Templates” for the steps to create and apply Day-N configuration templates in Cisco DNA Center.

Configure the below CLIs (example configs for IOS-XE) on the switch port on which RAP is connected. This can be configured either manually or using DAY-N templates. It is recommend to use DAY-N configuration templates to configure the following commands on IE switch ports on which RAP is connected.

```
interface $INTERFACE
 switchport trunk native vlan $NVLAN
 switchport mode trunk
 device-tracking attach-policy IPDT_MAX_10
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 no macro auto processing
end
```

Joining the Mesh APs (RAP of MAP) to C9800 WLC:

This section provides the configuration steps required to join a mesh Access Point (AP) as a Root AP (RAP) or Mesh AP (MAP) to the Catalyst 9800 Wireless LAN Controller (WLC) in Flex+Bridge mode.

A mesh AP needs to be authenticated for it to join the 9800 controller. AP will first join WLC in local mode and then we convert it to Flex+Bridge, also known as mesh mode.

For configuration guidance, refer to the following URLs:

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215100-join-mesh-aps-to-catalyst-9800-wireless.html

Configurations:

Configure RAP/MAP MAC addresses under Device Authentication:

1. Navigate to **Configuration -> Security -> AAA -> AAA Advanced -> Device Authentication**, select **Device Authentication** and select **Add**. Type in the Base Ethernet MAC address of the AP to join to the WLC, leave the **Attribute List Name** blank, and finally select **Apply to Device**.

Configure the authentication and authorization method list:

2. Navigate to **Configuration -> Security -> AAA -> AAA Method List -> Authentication** and select **Add**. The AAA Authentication pop-up appears. Type in a name in the **Method List Name**, select **802.1x** from the Type* drop-down and **local** for the Group Type, and select **Apply to Device**.
3. Navigate to **Configuration -> Security -> AAA -> AAA Method List -> Authentication** and select **Add**. The AAA Authentication pop-up appears. Type in a name in the **Method List Name**, select **credential download** from the Type* drop-down and **local** for the Group Type, and select **Apply to Device**.
4. Navigate to **Configuration -> Wireless -> Mesh -> Profiles** and select **Add**. The Add Mesh Profile pop-up appears. In the General tab set a name and description for the Mesh profile and check **Backhaul Client Access**.
5. Under the Advanced tab select **EAP** for the Method field. Select the Authorization and Authentication profile earlier, uncheck **Vlan Transparent** and check **Ethernet Bridging** (optional). Create a Bridge Group Name (BGN), check the **Strict Match**, and select **Apply to Device** as shown in Figure 113.

Figure 113 Mesh Profile on C9800 WLC

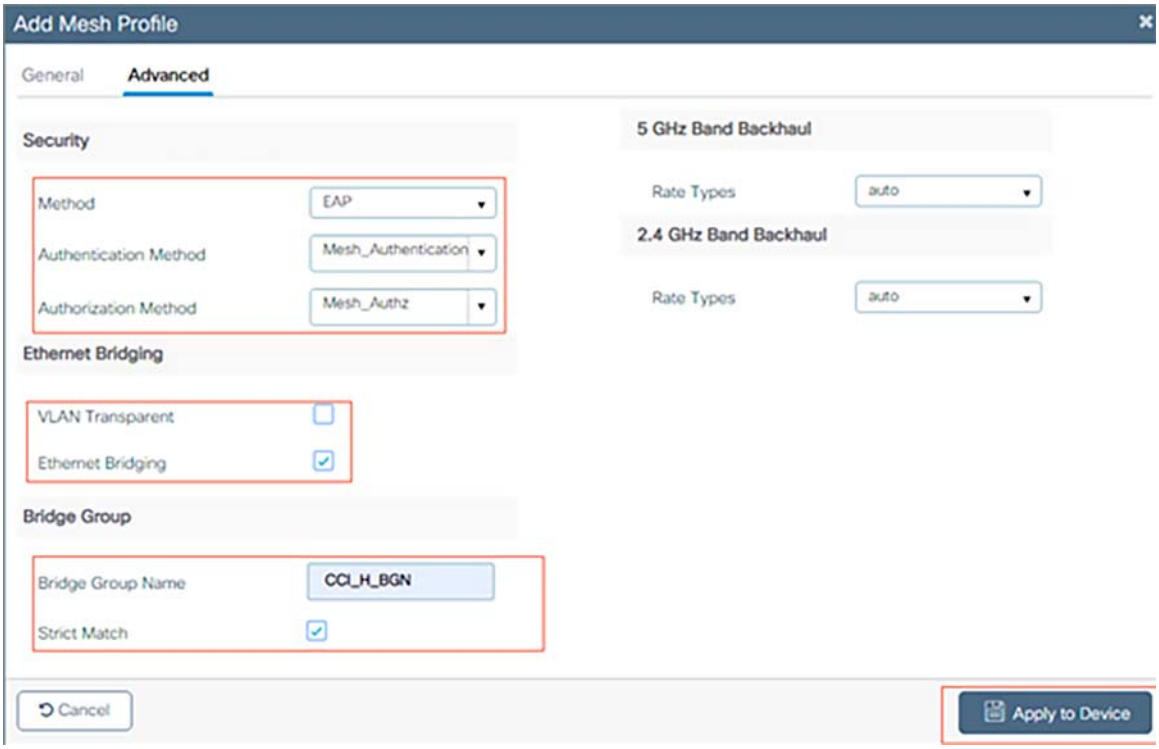


Figure 69 Mesh Profile on C9800 WLC

6. Navigate to **Configuration -> Tag & Profiles -> AP Join -> Profile** and select **Add**. The AP Join Profile pop-up appears. Set a name and description for the AP Join profile.

7. Navigate to the AP tab and select the **Mesh Profile** created earlier from the Mesh Profile Name drop-down. Ensure **EAP-FAST** and **CAPWAP DTLS** are set for the EAP Type and AP Authorization Type fields respectively and finally select **Apply to Device**.

8. Navigate to **Configuration -> Tag & Profiles -> Tags -> Site** and select **Add**. The Site Tag pop up appears. Type in a name and description for the Site Tag, select the **AP Join Profile** created earlier from the AP Join Profile drop-down. At the bottom of the Site Tag popup, uncheck the **Enable Local Site** checkbox to enable the Flex Profile dropdown. From the Flex Profile drop-down, select the **Flex Profile** you want to use for the AP.

Connect the AP to the network and ensure the AP is in local mode. To ensure the AP is in local mode issue the command **capwap ap mode local**.

Note: The AP must have a way to find the controller with either Layer 2 broadcast, DHCP Option 43, DNS resolution, or manual setup.

In CCI deployment, DHCP option 43 is used for the AP pool to find the WLC. We use DHCP Option 43 to help the AP obtain controller IP address from the DHCP server. In addition to offering it an IP address, DHCP server may also return one or more controller IP addresses to the AP.

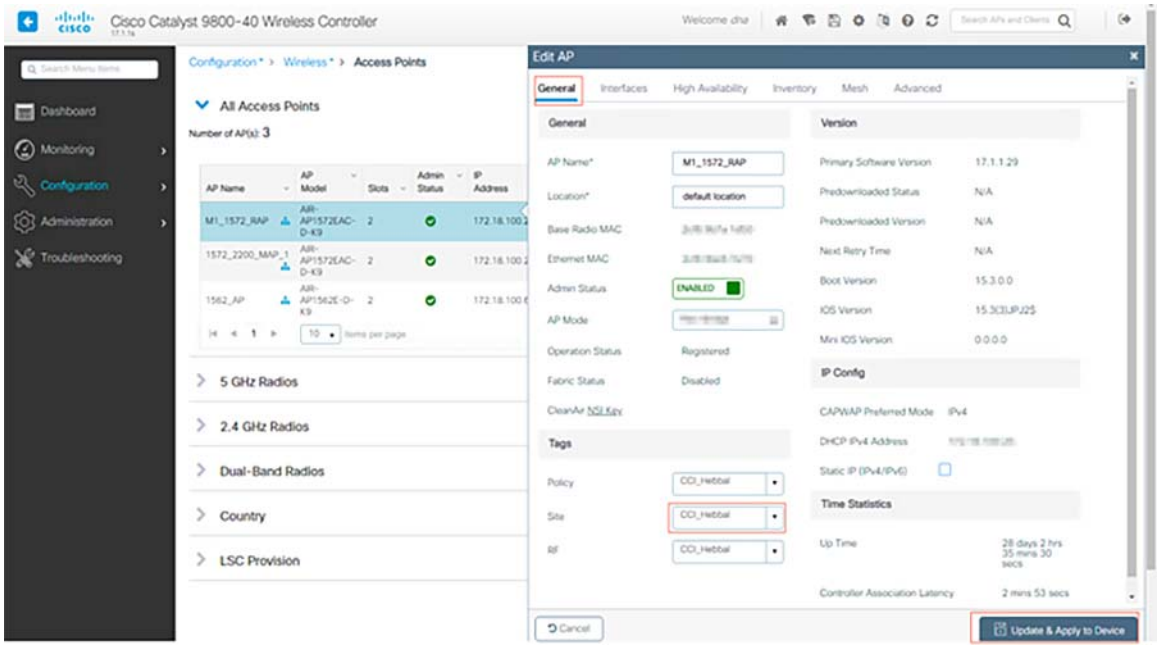
Refer to the following URL for information on configuring option43 on DHCP Server:

- https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html

The AP joins the WLC, ensure it is listed under the AP list, navigate to **Configuration -> Wireless -> Access Points > All Access Points.**

1. Select the AP; the AP popup appears. Select the **Site Tag** created earlier under the **General -> Tags -> Site** tab. Within the AP popup, select **Update and Apply to Device**.

Figure 114 Applying the Site Tag to AP

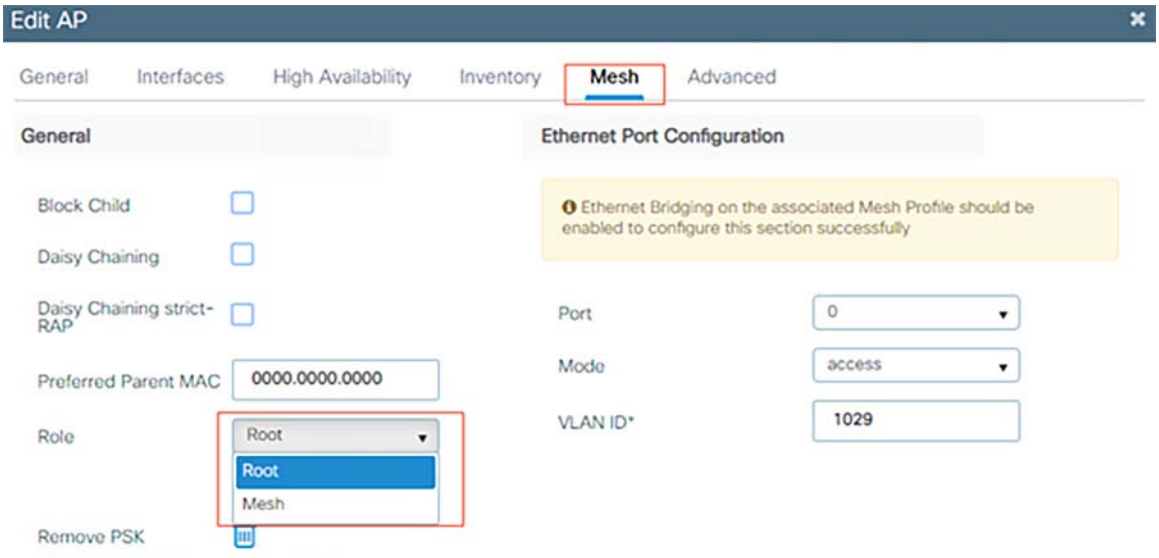


The AP reboots and must join back the WLC in Flex + Bridge mode.

We can now define the role of the AP: either root AP or mesh AP. The root AP is the one with a wired connection to the switch while the mesh AP will join the WLC via its radio which will try to connect to a root AP. A mesh AP can join the WLC via its wired interface once it has failed to find a root AP via its radio, for provisioning purposes.

2. Select the AP; the AP popup appears, Under **Mesh -> Role**, from the drop-down menu choose **Root** for RAP and **Mesh** for MAP, and then select **Update and Apply to Device**.

Figure 115 Selecting the Role of AP in Mesh



Mesh Verification on WLC CLI:

```
WLC_C9800-40_1#show wireless mesh ap tree
=========================================================================
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=========================================================================
[Sector 1]
-----------
AP<MAC>[0, 0, CCI_H_BGN, 173, 0000.0000.0000, 0%, 0]
|- AP<MAC> [1, 80, CCI_H_BGN, 173, 0000.0000.0000, 0%, 0]
| - AP<MAC> [2, 80, CCI_H_BGN, 173, 0000.0000.0000, 0%, 0]
Number of Bridge APs : 3
Number of RAPs : 1
Number of MAPs : 2
(*) Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller
```

WLAN Configuration

For more details on C9800 WLC configuration guidelines, refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html

Step 1 : Declare Client VLANs. Add the needed VLANs to the WLC where the wireless clients are assigned.

a. Navigate to **Configuration -> Layer2 -> VLAN -> VLAN -> + Add.** Add all the required VLANs and change the State to **Activated**

Note: If you do not specify a **Name**, the VLAN automatically gets assigned the name VLANXXXX, where XXXX is its VLAN ID.

Repeat this step to create all the required VLANs.

In CCI network, to get the VLAN information of the VN networks:

b. Navigate to **Provision -> Fabric**, select desired PoP Site, and click on FiaB C9300 switch. On Run Commands, type **show vlan brief** to fetch the VLAN details.

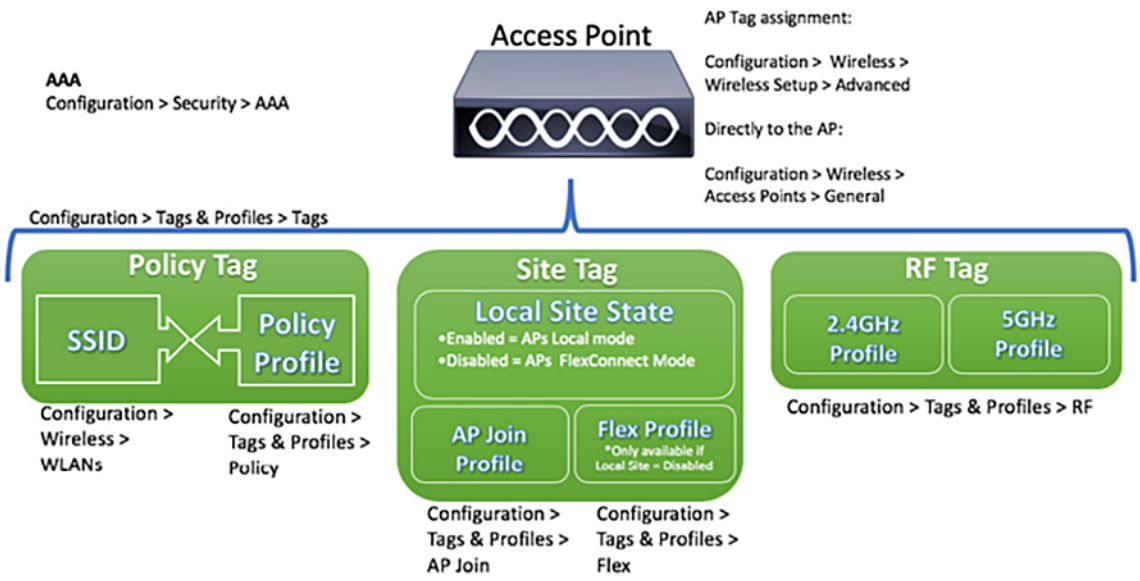
c. Verify the VLANs are allowed in your data interfaces.

– If you are using port channels, navigate to **Configuration -> Interface -> Logical -> PortChannel name -> General**. Make sure it is configured as Allowed Vlan = All.

– If you are not using port channels, navigate to **Configuration -> Interface -> Ethernet -> Interface Name -> General**. Make sure it is configured as Allowed Vlan = All.

Menu Based Configuration—Recommended for Existing 9800 WLCs Deployment

Figure 116 Visual Representation of WLAN Configuration Elements



Recommended flow of configuration:

1. Create SSID.
2. Create/Modify a Policy Profile.
3. Create/Modify a Policy Tag (link the SSID to the desired Policy Profile).
4. Assign the Policy Tag to the AP.

Step 1. **Create SSID**:

Navigate to **Configuration-> Tags & Profiles-> WLANs-> + Add**. Enter all the needed information (SSID name, security type and so on) and then click **Apply to Device**.

Step 2. **Create/Modify a Policy Profile**:

Navigate to **Configuration-> Tags & Profiles-> Policy.** Either select the name of a pre-existing one or click **+ Add** to add a new one. Ensure it is enabled, set the needed VLAN and any other parameter we want to customize. Once done click on Update & **Apply to Device.**

Step 3. **Create/Modify a Policy Tag**:

Navigate to **Configuration-> Tags & Profiles-> Tags-> Policy**. Either select the name of a pre-existing one or click + Add to add a new one. Inside the Policy Tag, click **+Add**, from the drop down list select the WLAN Profile name you want to add to the Policy Tag and Policy Profile to which you want to link it. Then click the checkmark **Update & Apply to Device**.

Step 4. **Assigning the Policy Tag to the AP**:

Navigate to **Configuration-> Wireless-> Access Points-> AP name-> General-> Tags.** From the **Policy** dropdown list select the desired Policy Tag and click **Update & Apply to Device.**

Note: After changing the policy tag on an AP, it loses its association to the 9800 WLCs and join back within about 1 minute.

Configuring RF Profiles on 9800 WLCs:

Recommended flow of configuration:

1. Create/Modify the RF profiles for 2.4GHz / 5GHz.
2. Create/Modify a RF Tag.
3. If needed, assign the RF Tag to the AP.

Step 1. **Create/Modify the RF profiles for 2.4GHz / 5GHz**:

Navigate to **Configuration-> Tags & Profiles-> RF**. Either select the name of a pre-existing one or click + Add to add a new one. Modify the profile as desired, one per band (802.11a/802.11b). Then click **Apply to Device**. In CCI, we are using the pre-configured RF profiles

Step 1. **Create/Modify a RF Tag**:

The RF tag is the setting that allows you to specify which RF Profiles are assigned to the APs.

Navigate to **Configuration-> Tags & Profiles-> Tags-> RF**. Either select the name of a pre-existing one or click + Add to add a new one. Inside the RF Tag, select the RF Profile that we want to add. After that click **Update & Apply to Device**.

Step 2. **Policy Tag Assignment (optional)**:

You can assign a RF Tag directly to an AP.

Navigate to **Configuration-> Wireless-> Access Points-> AP name-> General-> Tags**. From the Site dropdown list select the desired RFTag and click **Update & Apply to Device**.

Verification:

Figure 117 WLAN Verification on C9800

```
WLC_C9800-40_1#show wlan summary

Number of WLANs: 11

ID   Profile Name                  SSID                          Status Security
-------------------------------------------------------------------------------------------------
1    CCI_CUWN_Test                 CCI_CUWN_Test                 UP     [WPA2][802.1x][AES]
2    CCI_OTT_SnSH                  CCI_OTT_SnSH                  UP     [WPA2][PSK][AES]
3    SSID_Guest                    SSID_Guest                    UP     [open],MAC Filtering,[Web Auth]
4    CUWN_Test10                   CUWN_Test10                   UP     [WPA2][802.1x][AES]
5    CCI_SSIDTest                  CCI_SSIDTest                  UP     [WPA2][802.1x][AES]
--More--
```

Other important Verification Commands:

You can alternatively use these commands to verify the configuration.

VLANs/Interfaces Configuration:

```
# show vlan brief
# show interfaces trunk
# show run interface <interface-id>
```

AAA Configuration

```
# show run aaa
# show aaa servers
```

WLAN Configuration

```
# show wlan summary
# show run wlan [wlan-name]
# show wlan { id <wlan-id> | name <wlan-name> | all }
```

AP Configuration

```
# show ap summary
# show ap tag summary
# show ap name <ap-name> tag { info | detail }
# show ap name <ap-name> tag detail
```

Tag Configuration

```
# show wireless tag { policy | rf | site } summary
# show wireless tag { policy | rf | site } detailed <tag-name>
```

Profile Configuration

```
# show wireless profile { flex | policy } summary
# show wireless profile { flex | policy } detailed <profile-name>
# show ap profile <AP-join-profile-name> detailed
```

Ethernet Bridging on Wi-Fi Mesh Network

Ethernet bridging should be enabled for the following scenarios:

1. Use mesh nodes as bridges
2. Connect Ethernet devices, such as a video camera on a MAP using its Ethernet port.

An Ethernet Bridging feature can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the AP through the Ethernet port. The MAP AP associates to the root AP through the wireless interface. In this way, wired clients obtain access to the wireless network. Wired clients with different VLANs behind the AP are also supported. To use an Ethernet-bridged application, enable the bridging feature on the RAP and on all the MAPs in that sector.

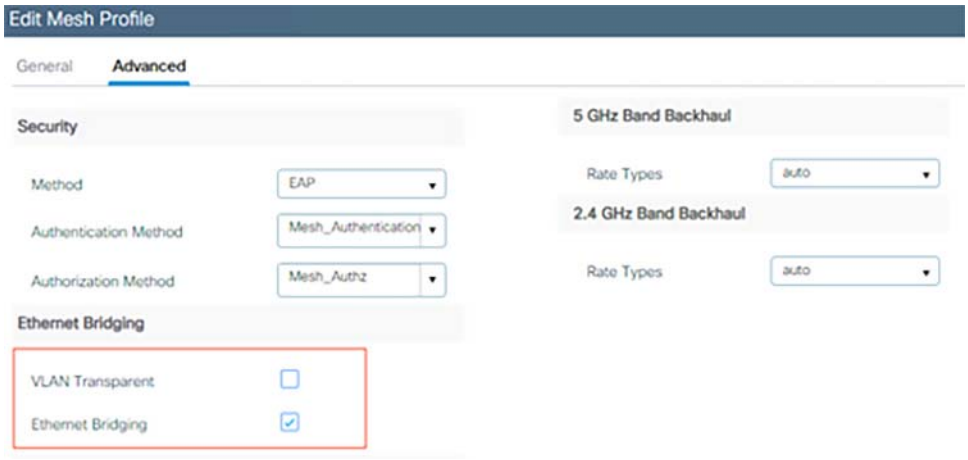
For more details on Ethernet Bridging, refer to:

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_mesh_87.html

Configuration:

a. Navigate to **Configuration->Wireless->Mesh->Profiles**, click the existing **Mesh Profile**. On the Advanced tab, uncheck **VLAN Transparent** and check **Ethernet Bridging**, as shown in Figure 118. Then click **Update & Apply to Device**.

Figure 118 Ethernet Bridging on Wireless Mesh



b. Navigate to **Configuration -> Wireless -> Access Points -> AP name -> Mesh** and configure the Ethernet port as shown below.

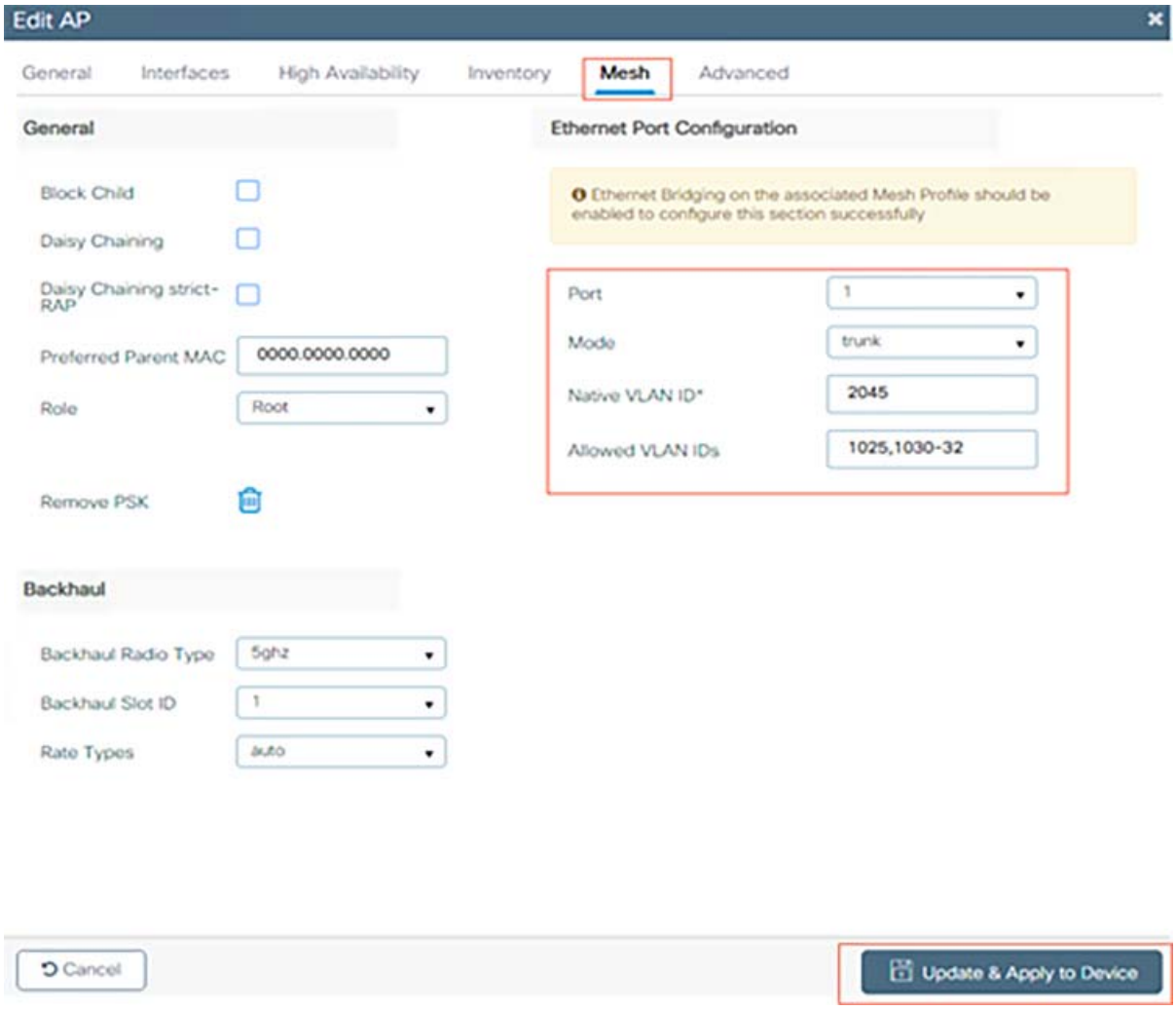
Access Ethernet ports in access mode:

AP Ethernet port is configured as access for some use cases where specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN, for example connecting a security camera.

Access Ethernet ports in trunk mode:

AP Ethernet port is configured as trunk port, in the cases where we want to connect an L2 switch to increase the port density and to bridge multiple vlans to the wired LAN over the Wi-Fi Mesh.

Figure 119 Mesh AP Ethernet Port configuration example



Integrating ISE with WLC

Authentication, Authorization, Accounting (AAA) server providing authentication, authorization and accounting services for wireless clients and infrastructure administrator access control. This section provide steps to configure C9800 WLC to work with ISE. For more information on Cisco Catalyst 9800 series, refer to the following URL.

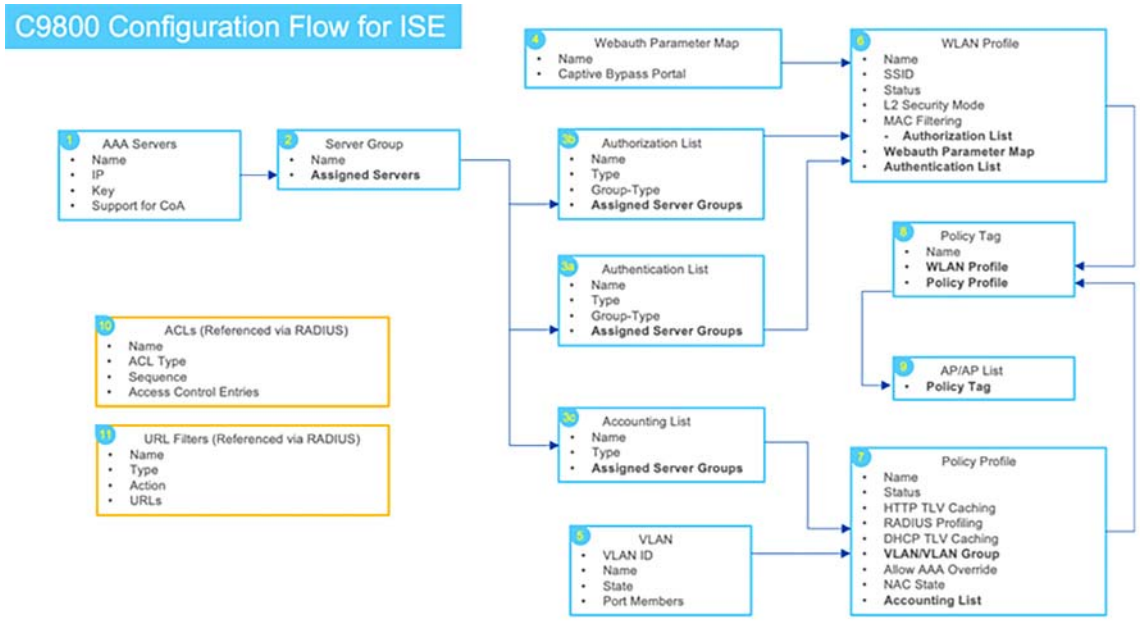
- https://www.cisco.com/c/en/us/products/wireless/catalyst-9800-series-wireless-controllers/index.html

The section assumes the C9800 WLC is accessible and AP is associated to the C9800. The document also assumes underlying network elements are already configured, which includes, VLANs, SVIs, Subnets, DHCP, routing, and DNS.

C9800 WLC Configuration

Following flow diagram shows the C9800 configuration on WLC at a high level. Each box represents individual configuration profile with relevant options shown and how each profile feeds into other profiles to make a working configuration. The bullet points within the profile that are in bold represents sub profile being fed into the profile. It also includes the suggested order to create the profiles that maps to the main section of the document.

Figure 120 C9800 WLC Configuration Flow for ISE



Steps 1 – 3:

Defining AAA

a. Go to **Configuration-> Security-> AAA-> Servers / Groups-> Servers**, Click **Add.**

Enter following information (Any configuration not defined in the table assumes default settings):

Name	CCI_ISE
Server Address	x.x.x.x
Key	***** (Match with ISE)
Support for CoA	Enabled

b. Click **Server Groups**, Click **Add.**

Enter following information:

Name	CCI_ISE_GRP
Group Type	RADIUS
Available Servers	CCI_ISE

c. Go to **Configuration-> Security-> AAA-> AAA Method List-> Authentication**, Click **Add.**

Create Authentication list using following information that will be used for both OPEN SSID and SECURE SSID:

Name	default
Type	dot1x
Group Type	group
Available Server Groups	CCI_ISE_GRP

d. Go to **Configuration-> Security-> AAA-> AAA Method List-> Authorization**, Click **Add**.

Enter following information for AAA Authorization list that will be shared for both SSIDs:

Name	default
Type	network
Group Type	group
Available Server Groups	CCI_ISE_GRP

Note: The Authorization name 'default' is significant here since there is no Authorization list that can be defined within the 802.1X WLAN. By using 'default' as name, C9800 can use the ISE to get additional authorization details such as for dACL operation. If default authorization list cannot be used or desired, then named authorization can be created and can be referenced via RADIUS server as a Cisco VSA. The Cisco VSA to use is 'Method-List={authorization-method-list}', which can be configured in ISE advanced Attribute Settings.

e. Go to **Configuration-> Security-> AAA-> AAA Method List-> Accounting**, Click **Add**.

Enter following information for AAA Authorization list that will be shared for both SSIDs:

Name	default
Type	Identity
Available Server Groups	CCI_ISE_GRP

Step4:

Create Webauth Parameter Map (Required for Guest Access)

1. Go to **Configuration-> Security-> Webauth-> Webauth Parameter Map**, Click **Add**.
2. Enter Name '**Captive-Bypass-Portal**, Click **Apply to Device**.
3. Click '**Captive-Bypass-Portal**' parameter map from the list.
4. Check **Captive Bypass Portal**, Click **Update & Apply**.

Step5:

Create VLANs. Go to **Configuration-> Layer 2-> VLAN-> VLAN**, Click **Add to add the required access vlans for the SSIDs.**

Step6:

Create WLANs

Go to **Configuration-> Tags & Profiles-> WLANs**, Click **Add**

General	Profile Name	CCI_CUWN_Test
	SSID	CCI_CUWN_Test
	Status	Enabled
Security > Layer 2	Layer 2 Security Mode	WPA + WPA2
Security > AAA	Authentication List	default

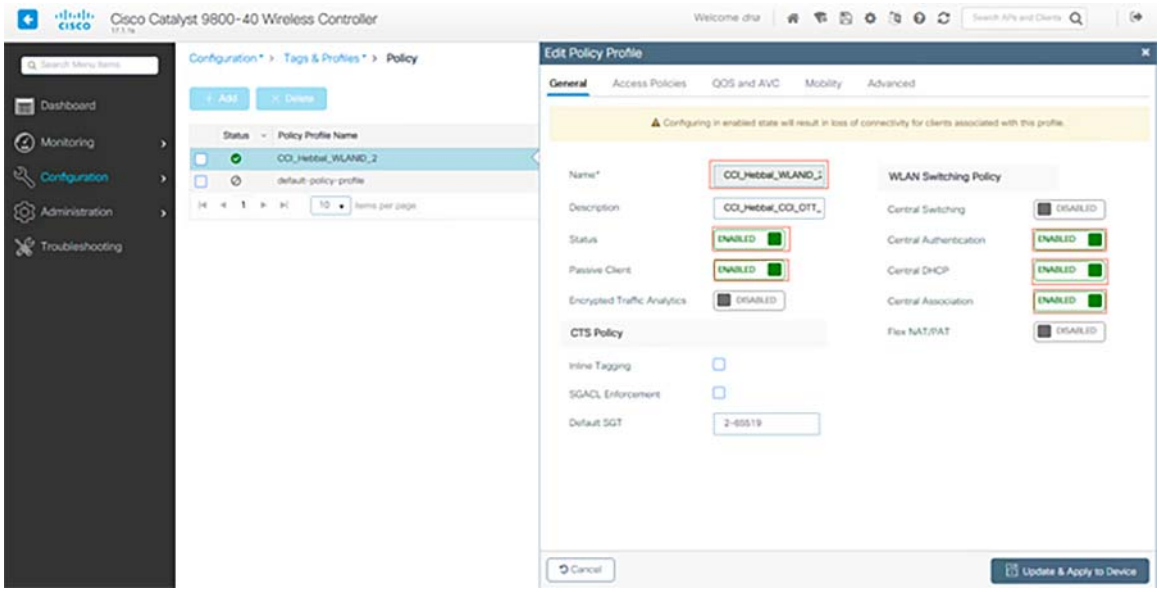
Click **Save & Apply to Device.**

Step 7: Create Policy Profiles

Go to **Configuration-> Tags & Profiles-> Policy**, Click **Add**.

Add Policy Profiles for WLANs using following table. Policy profile covers device sensor, default VLAN, CoA, and RADIUS Accounting. These profiles will be mapped to the WLANs using tags.

Figure 121 C9800 Policy Profile Configuration



Click **Save & Apply to Device**.

Step 8: Create Policy Tag

Go to **Configuration-> Tags & Profiles-> Tags**, under **Policy** Click **Add**.

Enter Name: **CCI_Hebbal.**

Within the '**ISE Enabled**' Tag window, click **Add** to map following WLANs to matching policy profiles. This ties the WLAN to the respective Policy Profile.

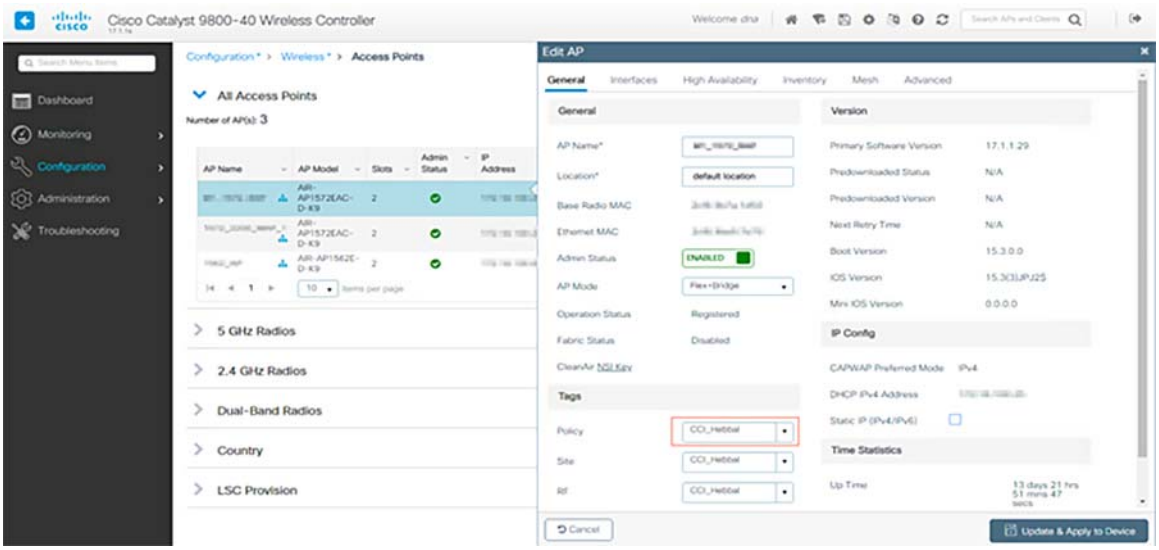
Click **Save & Apply to Device**.

Step 9: Assign Policy Tag to AP

Finally, apply the tag to the AP. This section shows instructions on tying it to a single AP. Using Advanced Wireless Setup Wizard on C9800, same tag can be applied to multiple APs at the same time.

1. Go to **Configuration -> Wireless -> Access Points**.
2. Click on the **AP Name or MAC address**.
3. Under **General-> Tags**, Select '**CCI_Hebbal**'.

Figure 122 C9800 Policy Tag assignment to AP



Click **Update & Apply to Device.**

ISE Configuration

Add WLC as network device on ISE

Step 1. Navigate to **Administration-> Network Resources-> Network Devices -> Add.**

Step 2. Enter WLC **Name**, check the **RADIUS Authentication Settings** option and enter the **Shared Secret**.

Scroll down and select **Save**.

Verification:

Figure 123 WLC and ISE Integration Verification

```
WLC_C9800-40_1#show aaa servers

RADIUS: id 1, priority 1, host [redacted], auth-port 1812, acct-port 1813, hostname CCI_ISE
     State: current UP, duration 240029s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 240029s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP
     Platform State from WNCD (6) : current UP
     Platform State from WNCD (7) : current UP
     Platform State from WNCD (8) : current UP, duration 646s, previous duration 0s
```

Create New User on ISE:

Step 1. Navigate to **Administration -> Identity Management -> Identities -> Users -> Add**.

Step 2. Enter the information. In this example, this user belongs to a group called ALL_ACCOUNTS but it can be adjusted as needed as shown in the image.

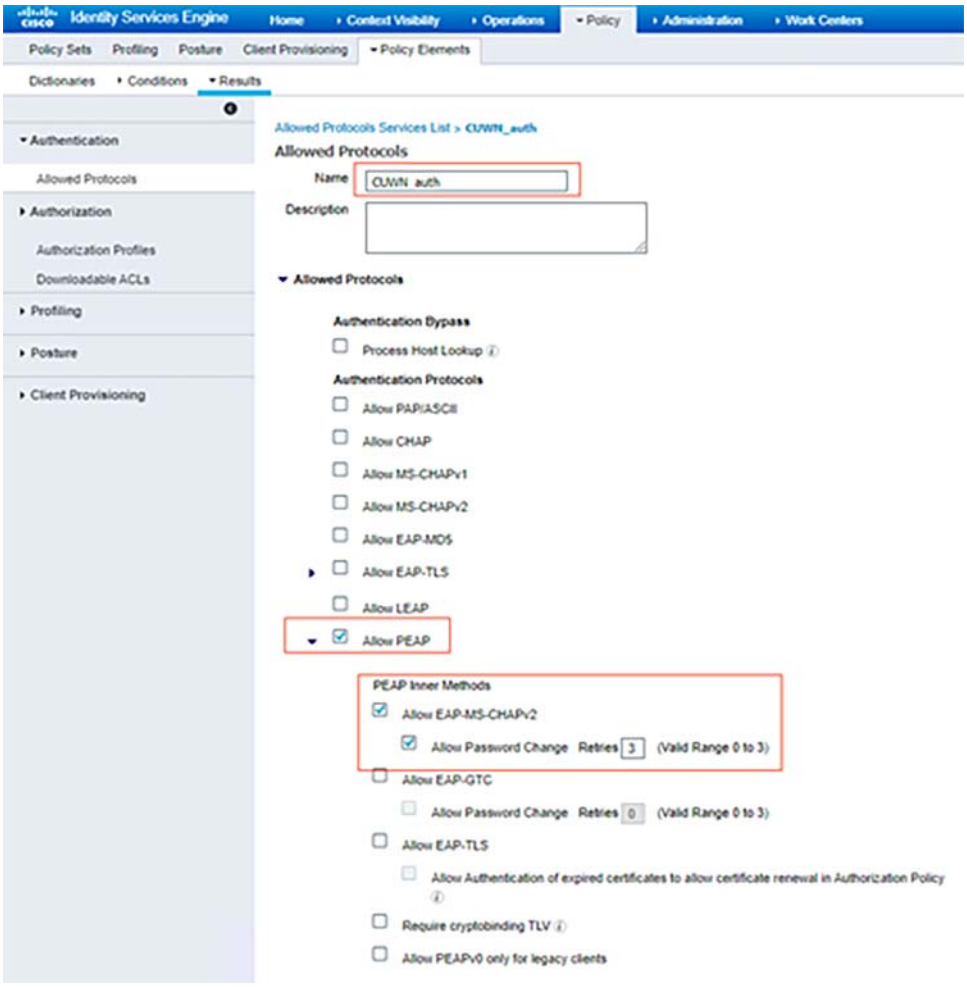
Create Authentication Rule:

Authentication rules are used to verify if the credentials of the users are right (verify if the user really is who it says it is) and limit the authentication methods that are allowed to be used by it.

Navigate to **Policy-> Policy Elements-> Results-> Authentication-> Allowed Protocols** as shown in Figure 124.

Add an authentication rule by selecting the protocols as shown in Figure 124.

Figure 124 Authentication Rule Configuration on ISE



Scroll down and **Save**.

Create Authorization Profile

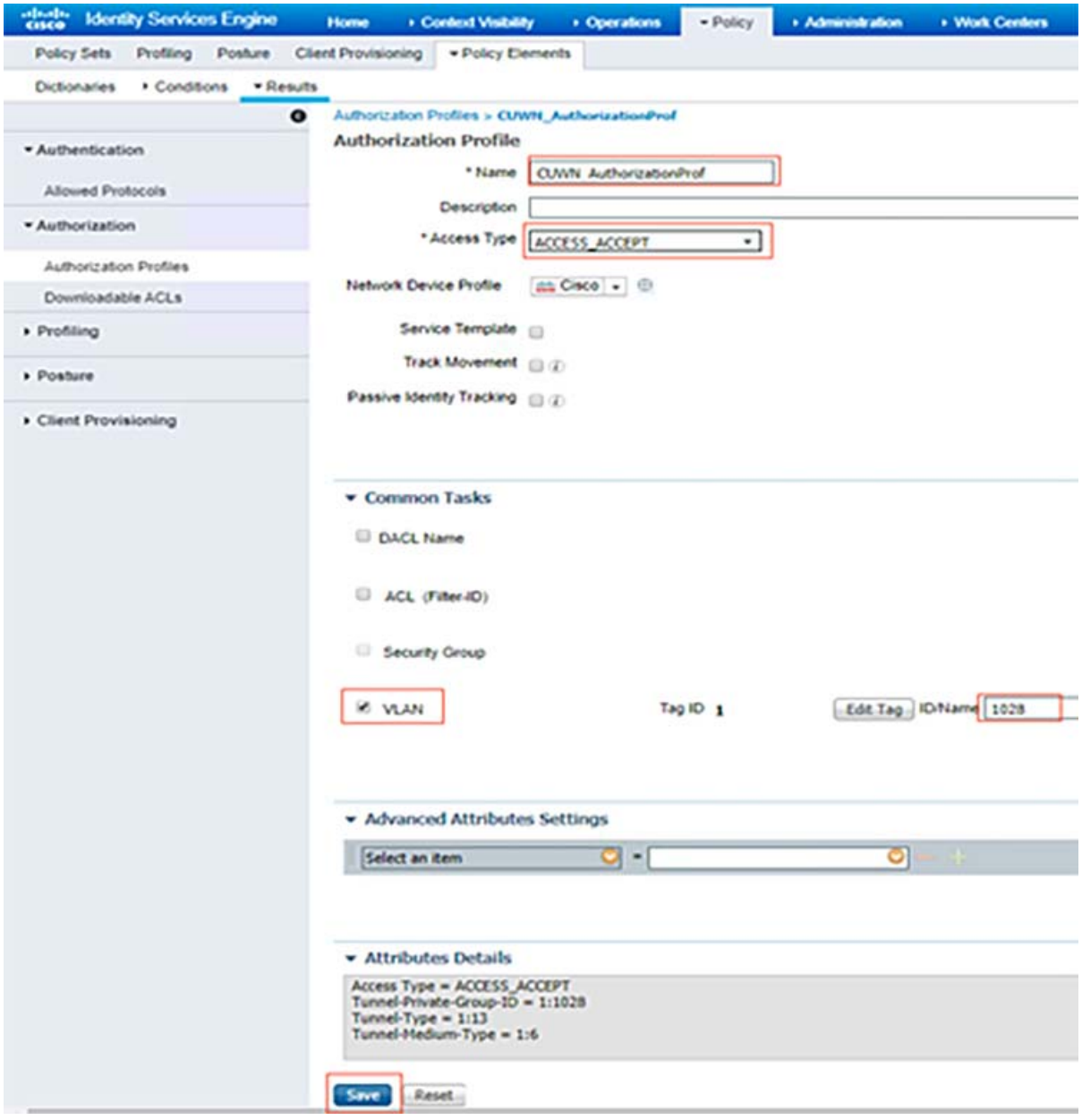
The authorization profile determines if the client has access or not to the network, push Access Control Lists (ACLs), VLAN override or any other parameter. The authorization profile shown in this example sends an access accept for the client and assigns the client to VLAN 1028.

Add a new Authorization Profile.

Navigate to **Policy-> Policy Elements-> Results-> Authorization-> Authorization Profiles** as shown in Figure 125.

Enter the values as shown in the image. Here we can return AAA override attributes like VLAN as example. WLC 9800 accepts tunnel attributes 64,65,81 using VLAN id or Name, and accepts also the usage of the AirSpace-Interface-Name Attribute.

Figure 125 Authorization Profile Configuration on ISE

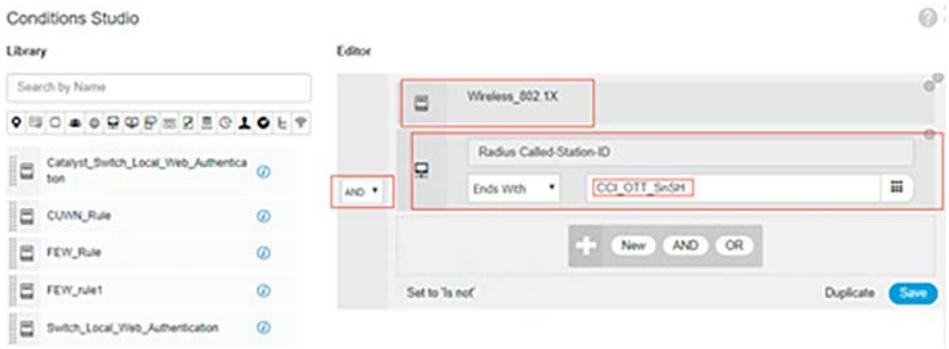


Create Policy Set (Authentication and Authorization rules)

Navigate to **Policy-> Policy Sets** as shown in the image. Click on '+' to create a CUWN_PolicySet

Add the conditions that do the authorization process to fall into this rule. In this example, the authorization process hits this rule if it uses 802.1x Wireless and its called station ID ends with CCI_OTT_SnSH as shown in Figure 126.

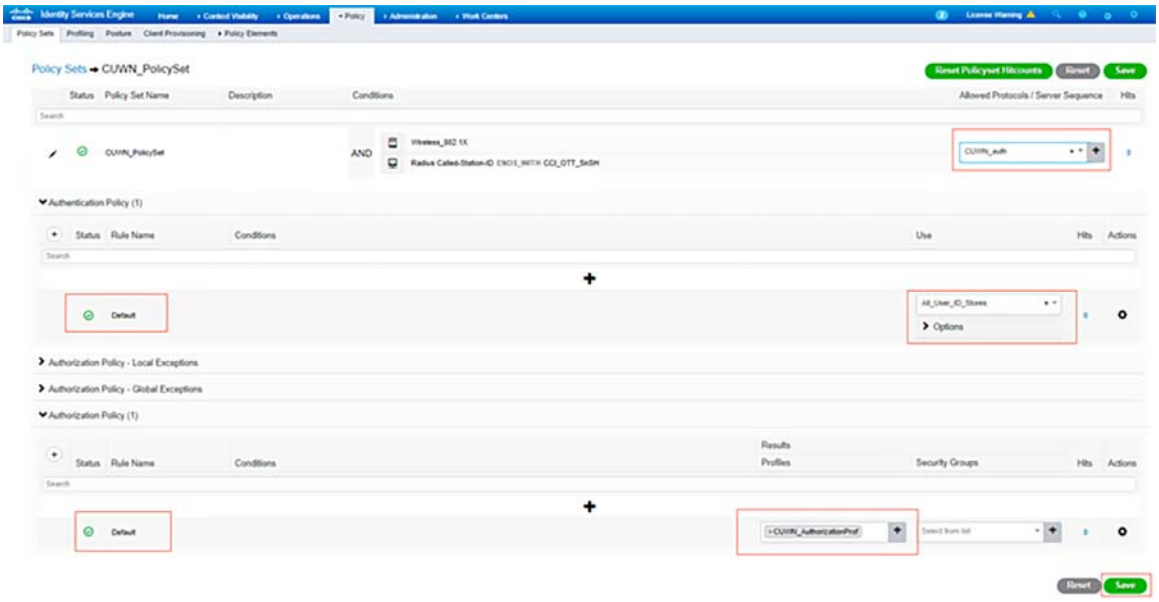
Figure 126 Policy Set Authorization Conditions



To view the Authentication/Authorization rules, we would click on the arrow on the right side to go into that specific policy set:

Under Allowed Protocols field, from the drop-down select the 'CUWN_auth' we had created earlier, for Authentication Policy choose the Default rule with use as 'All_User_ID_Stores' and for Authorization Policy choose the Default rule with 'CUWN_AuthorizationProf' we had created earlier.

Figure 127 Policy Set Configuration in ISE



Click on **Save.**

Implementing SD Access Wireless Network in a PoP

For details about SDA eWLC deployment and SDA AP onboarding, refer to the section "Configuring SD Access Wireless Embedded WLC on C9300 Stack, page 84"

Creating Wireless SSID:

1. On DNA Center, Navigate to **DESIGN-> Network Settings> Wireless**, in the left hierarchy pane, select the **Global** level. In the **Enterprise Wireless** section, click **+ Add**. Create an SSID with the required information as shown in the below image and click **Next** to continue.

2. Enter a Wireless Profile Name, under **Fabric** select **Yes** and choose a Site where SSID broadcasts, and click **Finish** as shown in the below image.

3. Provision the PoP site C9300 switch with eWLC to configure the changes. Make sure the newly created SSID is getting configured.

Repeat the same procedure for creating the other SSIDs.

Micro-Segmentation in SDA Wireless

Even though SDA AP is in local mode, data traffic is not forwarded to WLC over CAPWAP, instead AP encapsulates traffic in VXLAN and forwards it to Fabric Edge switch. So, the micro-segmentation with wireless clients works same as that of the wired clients.

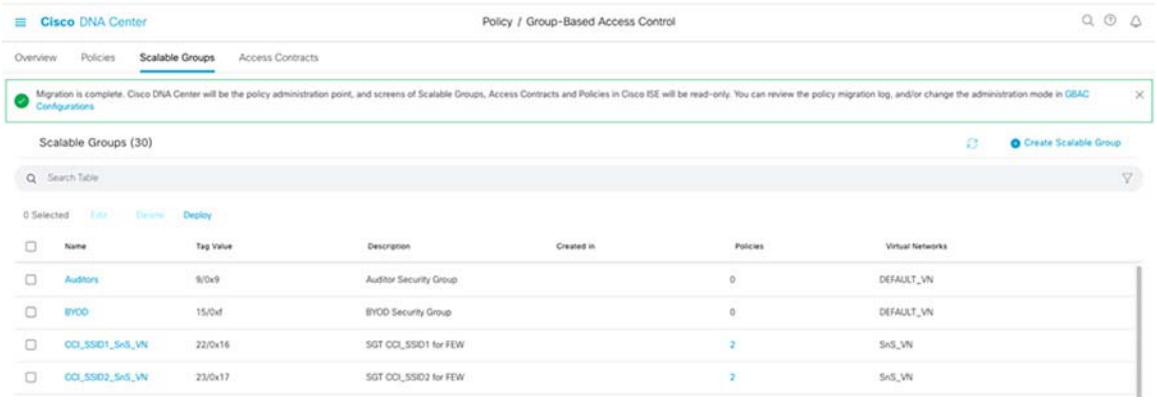
For more details on micro-segmentation using SGTs refer to the following URL:

- https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/sda-fabric-deploy-2019oct.pdf

Creating SGTs:

1. On DNA Center, Navigate to **Policy -> Group-Based Access Control -> Scalable Groups** and create SGTs. In this example, as shown in Figure 128, two SGTs CCI_SSID1_SnS_VN and CCI_SSID2_SnS_VN are created and assigned to the SnS_VN and deployed.

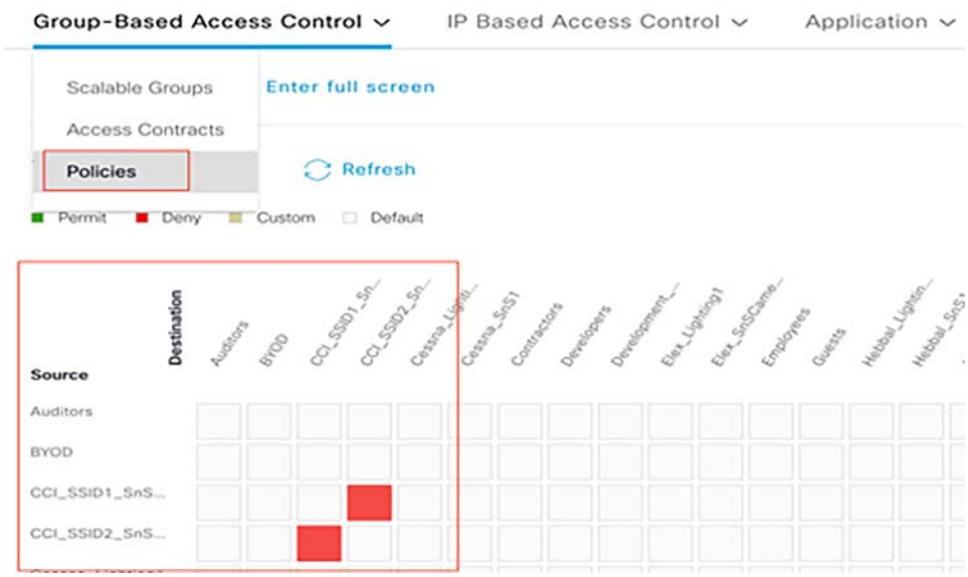
Figure 128 SGT Creation on Cisco DNA Center



Creating Policy (SGACL):

On DNA Center, Navigate to **Policy -> Group-Based Access Control -> Policies** and create policies. In this example as shown in Figure 129, a deny policy is created between CCI_SSID1_SnS_VN and CCI_SSID2_SnS_VN SGTs and deployed.

Figure 129 Policy (SGACL) Creation on Cisco DNA Center

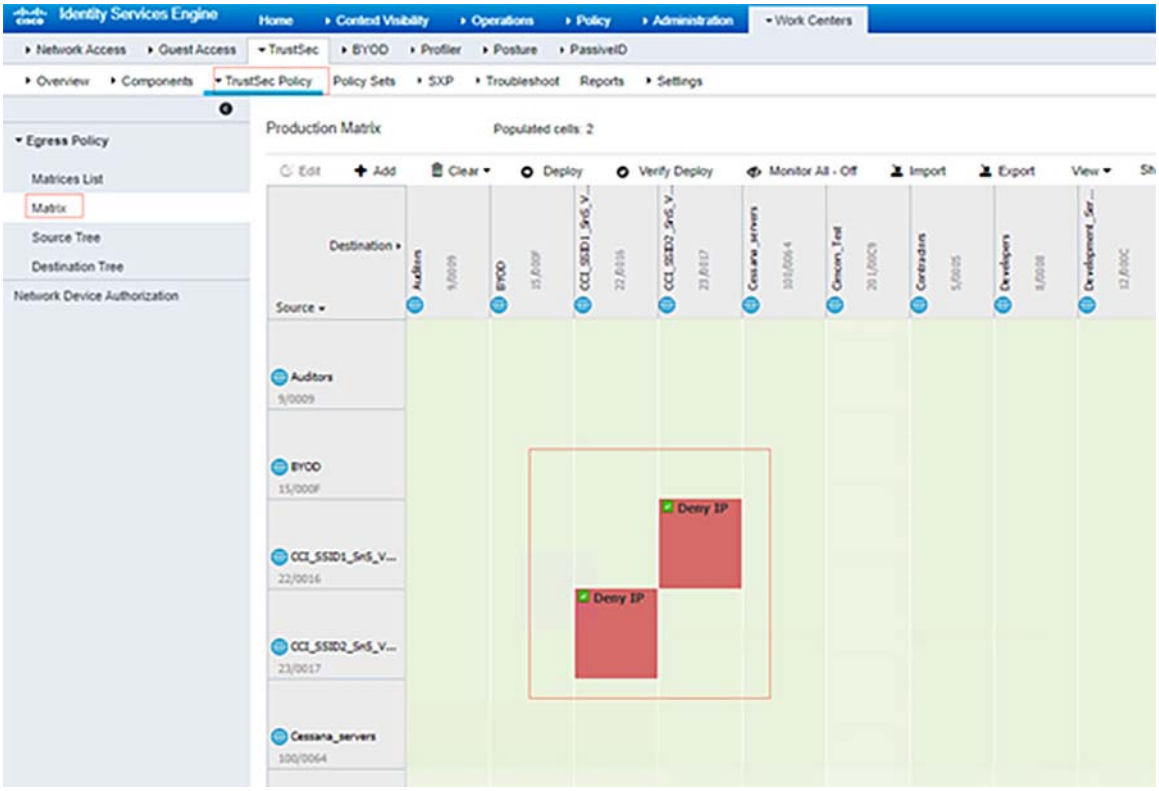


The status changes to DEPLOYED and the policies are available to be applied to SD-Access fabrics Cisco DNA Center creates and are also available in ISE, viewable using the Cisco TrustSec policy matrix.

Verification:

1. On ISE Navigate to **Work Centers-> TrustSec-> TrustSec Policy**, and then on the left side selecting Matrix. Verify that the policy has been created in the ISE TrustSec policy matrix.

Figure 130 SGACL verification on ISE policy Matrix



2. On DNA Center, navigate to **Provision -> Fabric** and choose the Bangalore Fabric. Navigate to MG Road PoP site and under **Host Onboarding** assign the SGTs to the Address Pools, then click **Save and Apply**.

show cts role-based permissions - Shows SGACL configured in ISE and pushed to the edge device

```
C9300-R-Stack#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 22:CCI_SSID1_SnS_VN to group 23:CCI_SSID2_SnS_VN:
Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

When clients with SSIDs,CCI_SSID1 (SGT 22) and CCI_SSID2 (SGT 23) tries to communication each other, on the Fabric Edge we observer packets are getting denied.

show cts role-based counters—Provides information on the exit edge node about SGACL being applied.

Implementation of the Field Area Network

This section covers the implementation FAN on the CCI network for implementing Cisco Resilient Mesh (CR-Mesh) as one of the access networks in the PoP site access rings or a RPoP site. Implementation of the headend network infrastructure for secure communication of CR-Mesh gateway (CGR1240) and nodes data traffic over CCI network to the headend router is discussed in detail in this section.

This section includes the following major topics:

Implementing Headend Network

The headend is a combination of components that helps in authentication, certificate enrollment, provisioning, and management of legitimate FARs and Field devices.

Headend Infrastructure Components

Table 17 lists the headend infrastructure components:

Table 17 Headend Infrastructure Components

Components of the Headend	Location in the Architecture
Certificate Authority (RSA CA)	Data Center
Certificate Authority (ECC CA)	Data Center
Head End Router (HER, In our implementation CSR1000V)	DMZ
DHCP Server (IPv4 and IPv6)	Data Center
Field Network Director (FND)	Shared Services

Hardware, Software Requirement, and License with Versions

Table 18 shows the headend components and operating system requirements:

Table 18 Headend Components: Operating System Requirements

Component Name	Operating System Required	Description
RSA CA Server	Windows 2016 server	Hosted as a VM on ESXi hyper-visor.
ECC CA Server, NPS, AD	Windows 2016 server	All three services can be hosted on the same Windows 2016 server. Hosted as a VM on ESXi hypervisor.
Field Network Director (FND)	RHEL 6.4 and above	RHEL requires subscription license for yum updates.
CPNR Local and Regional	Cent OS	In this implementation, CPNR is deployed from an (VMware) OVA file. Hosted as a VM on ESXi hypervisor.

Table 19 shows the headend components hardware requirements according to scale requirements:

Table 19 Headend Components: Hardware Requirements According to Scale Requirements

Components	Operating System	Hardware Resource Used
RSA CA Server	Windows 2016 server	Memory: 16 GB CPU: 8 Core Hard Disk: 100 GB
ECC CA Server	Windows 2016 server	Memory: 16 GB CPU: 8 Core Hard Disk: 100 GB
FND	Red Hat Enterprise Linux	Memory: 16 GB CPU: 4 Core Hard Disk: 250 GB
CPNR Local	Cent OS	Memory: 4 GB CPU: 1 Core Hard Disk1: 14 GB, Hard Disk2: 10 GB. License is needed only for Regional server. Local server latches onto Regional server for license.
CPNR Regional	Cent OS	Memory: 4 GB CPU: 1 Core Hard Disk1: 14 GB, Hard Disk2: 10 GB. License is required to configure the CPNR Regional User Interface (Cisco Prime Network Registrar software license key).

Table 20 shows the headend components license requirements:

Table 20 Headend Components: License Requirements

Operating System	Components	License Count	Hardware Resource Used
Windows 2016 server	RSA CA server	1	To host Certificate Authority and Active Directory database.
Windows 2016 server	RSA CA server	1	Optional to start with. Mandatory while attempting to integrate CGEs (meters/lights) with FND.
Red Hat Enterprise Linux	FND	1	RHEL License subscription is needed for performing yum updates and installation.

High Level Implementation Sequence of Various Headend Components

Multiple components interact with each other in the headend. Considering the dependency of the components, the following sequence IS followed while implementing the headend. For example, the RSA CA server should be installed and configured first and foremost, followed by implementation of the FND, and so on. **Components 1-4** are mandatory for building the headend infrastructure. **Component 5** is required for securely onboarding endpoints like CGE.

1. Root CA Server
2. Field Network Director (FND)
3. Head End Router (HER)
4. DHCP Server (CPNR)
5. ECC CA Server

Root Certificate Authority (Root CA) Installation

Root CA helps provide the certificate for RSA certificate-based authentication. This component is required by multiple components like the HER, FAR, and FND. RSA CA certificate-based authentication for enhanced security. Interacting components would be authenticating each other in the first place using the RSA CA certificate. Components of the headend that require the RSA CA server are as shown in Table 21:

Table 21 Components that Require the RSA CA Server

Component Name	Enrollment Method
Head End Router (HER)	Authentication and Enrollment happens directly with the RSA CA server. As part of authentication, the HER receives the certificate of the RSA CA server. As part of enrollment, the HER receives its own certificate signed by the RSA CA server.
Field Network Director	Certificate representing FND is created, exported from CA server as FND.pfx. Similarly, the public certificate of the RSA CA server is exported as CA-cert.cer. Both these exported certificates should be securely transmitted to and stored in the keystore of the FND.
Field Area Router	FAR (not part of the Headend infrastructure) also dynamically obtains the RSA certificate via SCEP similar to HER.

For installing/configuring of the RSA Server, refer to the section “Implementing RSA Certificate Authority” on page 35 at the following URL:

- https://salesconnect.cisco.com/-/content-detail/da249429-ec79-49fc-9471-0ec859e83872

Notes:

- If you do not have access to any of these Cisco SalesConnect links, ask your Cisco account team to help provide you with the documentation. However, some of the documents require a signed non-disclosure agreement (NDA) with Cisco.
- In the above Implementation Guide, the installation is given for the Windows 2012 server and the steps are same for the Windows 2016 server.

After installation of RSA CA Server, the following certificates were exported from the RSA CA server:

1. FND.pfx:
   - Contains the properties representing the FND
   - Certificate contains the private key of FND
   - Password Protecting the Exported FND Certificate.
2. IPG-RSA-ROOT-CA.cer:
   - Certificate represents the RSA CA Server
   - Certificate doesn't contain the private key of RSA CA server
   - It is a public certificate and is not protected with any password.

ECC Certificate Authority Installation

The ECC CA server is used to implement the authentication between the NPS Server and the CGE, the NPS Server integrates Certificate Authority with RADIUS and NPS server issues CGE certificates, which are programmed into the CGE for authentication. When CGR receives the authentication request from CGE, it will forward the request to the NPS server for authentication.

Prerequisites to Installing a ECC CA

- Configure the system time and date on the Windows Server 2016 Enterprise machine (to install the ECC CA) to the correct time and date, or enable the Windows Time service to sync time with an authoritative time source.
- For each configuration page mentioned in the following steps, any settings/options that are not mentioned can remain at their default value.
- Each server machine configured with Active Directory Certificate Services (either Root or Subordinate CA (Sub-CA)) can only be configured with one specific Cryptographic Service Provider (CSP). For this installation, the CSP is ECDSA P256#Microsoft Software Key Storage Provider.

  Note: The ECDSA P256 Algorithm is used for authenticating the CGEs.
- In the following procedure to install the ECC CA, it is assumed that you want to install the Active Directory Certificate Services on a server machine that has successfully joined the Active Directory Domain as a member server. The server on which the ADCS is to be enabled needs to be part of an Active Directory Domain (either as a member server or as a domain controller).
- It is recommended to appropriately rename the computer name of the Windows 2016 server to something meaningful according to the role played by the server. While doing so, the server might reload. Once the server comes back up, verify that the computer name has changed.

Time synchronization plays a crucial role while using certificate-based authentication, which provides stronger security compared to pre-shared keys. For installing/configuring of NTP Synchronization of RSA CA Server, refer to section “NTP Synchronization for RSA CA Server,” page 36, at the following URL:

- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

Installing ECC CA Certificate Authority

Creating Active Directory Domain Services, DNS Server, and NPS

1. In Windows 2016, click **Start** and then click **Server Manager**. If Server Manager is not in the menu items, click **Start**, click the **Smart Search** box and type **Server manager**.
2. In the **Select** installation type section, choose the default **Role-based or feature-based installation**, click **Next**, leave default on the **Server Selection** section, and then click **Next** again.
3. In the **Server Roles** section, check **Active Directory Domain Services, DNS Server and Network Policy and Access Services** (in the pop-up window, click **Add Features** after each selection) and then click **Next**.
4. In the **Features** section, leave default values and click **Next**. In the **Active Directory Domain Services** section, leave default values and click **Next**. In the **DNS server** section, leave default values and click **Next**. In the **Network Policy and Access server** section, leave the default values and then click **Next**.
5. In the **Confirm installation services** section, select **Restart the destination server automatically if required**, and then click **Install**. Once the server role installation is completed, the **Installation Results** dialog displays. Check all the relevant parameters.

Configuring Active Directory Domain Services, DNS Server, and NPS

6. On the **Server Manager** page, select **AD DS (Active Directory Domain Services)**, click **More**, and then select **Promote this server to a domain controller**.
7. On the **Deployment Configuration** panel, choose **Add a new forest**, set a Root domain name like **iot.cisco.com**, and then click **Next**. In the **Domain Controller Options** section, set the password and click **Next**. In the **DNS Options** section, leave default value for **Create DNS delegation** and then click **Next**.
8. Under **Additional Options**, set the NETBIOS domain name and click **Next**. In the **Paths** section, leave values as default and then click **Next**.

9. In the **Review Options** section, verify all the desired values and then click **Next**. In the **Prerequisites Check** section, make sure all the prerequisite checks are passed successfully and click **Install**.

Installing AD Certificate Services

1. Open **Server Manager**, click **Add roles and features**, click **Next**, choose the default Role-based or feature-based installation, click **Next**, choose the left default on **Server Selection**, and then click Next.
2. On the **Select Server Roles** page, choose **Active Directory Certificates Services**, in the window click **Add Features**, and then click **Next**.
3. On the **Select Role Services** page, check the following role services, and then click **Next**.
   - **Certification Authority**
   - **Certificate Authority Web Enrollment**
   - **Online Responder** (new Microsoft name for Certificate Revocation List)
4. On **Web Server Role (IIS)** page, click **Next**. On the **Select Role Services** page, click **Next** to accept all the default role services for Web Server (IIS).
5. On the **Confirm Installation Options** page, review all selected configuration settings and (select **Restart the destination server automatically if required**). To accept these options, click **Install** and wait until the setup process complete. Once the server role installation is completed, the **Installation Results** dialog displays.
6. Click **Server Manager**, click **AD CS**, and then click **More**. On the **All Servers Task Details and Notifications** page, select **Configure Active Directory Certificate Services** and then click **Next**.
7. On the **Credentials** page, click **Next**. On the **Select Role Services** page, check the following role services, and then click **Next**.
   - **Certification Authority**
   - **Certificate Authority Web Enrollment**
   - **Online Responder** (new Microsoft name for Certificate Revocation List)
8. On the **CA Type** page, as default, select **Root CA**, and then click **Next**.
9. On the **Set Up Private Key** page, click **Create a new private key**, and then click **Next**.
10. On the **Configure Cryptography for CA** page, select the following CSP, key length, and hash algorithm:
    a. Select **Cryptographic Service Provider (CSP)**:
       - Choose **ECDSA P256#Microsoft Software Key Storage Provider** to create a CA issuing certificates for mutual authentication between CG-Mesh nodes and the Microsoft Network Policy Server RADIUS.

    b. Choose key character length and hash algorithm:
       - Choose **256 bit key length** if the root CA is configured with ECDSA P256#Microsoft Software Key Storage Provider.
       - Select the hash algorithm for signing certificates issued by this CA: Choose **SHA256** for **ECDSA P256#Microsoft Software Key Storage Provider**.
11. On the **CA Name** page, leave all default values and then click **Next**. On the **Set Validity Period** page, specify the number of years or months that the CG-Mesh node certificate is valid. User can choose the Validity Period according to the requirements. In this implementation, as an example, **Validity Period** has been chosen as **5 years**. Click **Next**.

12. On the **Confirm Installation Options** page, review all selected configuration settings. To accept these options, click **Install** and wait until the setup process completes. Once the server role installation is completed, the **Installation Results** dialog displays.

13. Verify that all desired server roles and role services that are shown with Installation succeeded. Click the **Close** option and reboot the server.

Disable Certificate Extensions

14. Open a Command prompt console and type the following commands to disable some certificate extensions:

```
certutil -setreg policy\DisableExtensionList +1.3.6.1.4.1.311.20.2
certutil -setreg policy\DisableExtensionList +1.3.6.1.4.1.311.21.7
certutil -setreg policy\DisableExtensionList +1.3.6.1.5.5.7.1.1
certutil -setreg policy\DisableExtensionList +2.5.29.31
certutil -setreg policy\DisableExtensionList +2.5.29.32
certutil -setreg policy\DisableExtensionList +1.3.6.1.4.1.311.21.10
certutil -setreg policy\DisableExtensionList +2.5.29.14
certutil -setreg policy\DisableExtensionList +2.5.29.35
```

Modify Default Name Curve for Server Key Exchange Message

15. Click **Start**, search for **gpedit.msc** (Local Group Policy Editor), select **Local Computer policy**, select **Computer Configuration**, expand **Administrative Template**, select the drop-down list for **Network**, select **SSL configuration** setting, and then click **ECC Curve Order**.

16. In **ECC Curve Order** page, click **Enabled**, and then add **secp256r1** in **ECC Curve Order**.

Creating and Configuring the Template for CGE

Complete the following steps to create and configure the template for CGE on the NPS:

1. Launch **Certsrv (Certificate Authority Console)**, click **Server Manager**, elect **Tools**, and then in the drop-down list, select **Certification Authority**.

2. In the **Certsrv** window on the **Certificate Authority / Sub-CA Server** (under **Certificate Authority**) running ECC Algorithm, right-click and select **Properties**.

3. In the **Properties** window, select **General** tab, select **View Certificate**, and then click the **Details** tab. Scroll down and check the **Signature algorithm** used is **SHA256ECDSA**. The **Public key** should be **ECC (256 Bits)**.

4. In the **Certification Authority Console**, select **CA (Local)-> Sub CA**. Right-click **Certificate Templates** in the left plane, and then right-click and select **Manage**.

5. Select and duplicate the **Computer** from the **Certificates Templates Console**. In the **Compatibility** tab, select **Windows Server 2016 for Certification Authority and Certificate Recipient**.

6. In the **General** tab, specify the **Template display name** (for example, **CGE_Template**) and that the validity period is **5 years** and the Renewal period is **6 weeks**. Then select the **Publish certificate in Active Directory** check box.

7. On the **Request Handling** tab, choose **Signature** from the **Purpose** drop-down list. Select **Yes** in the **Certificate Templates** warning dialog. To allow certificate private key exports in the **Request Handling** tab, select **Allow private key to be exported**.

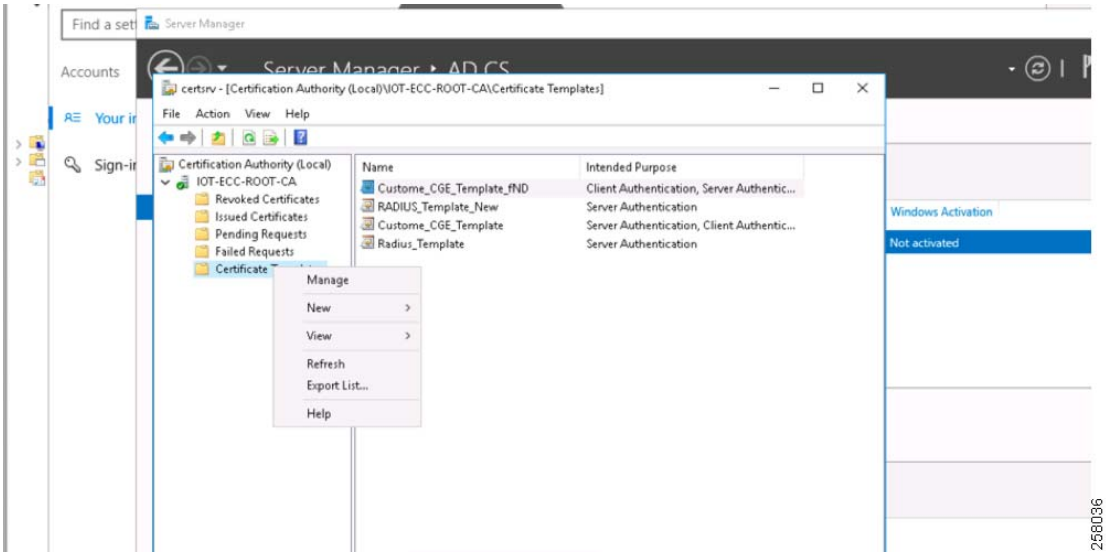
8. On the **Cryptography** tab, choose **Key Storage Provider** for the **Provider Category**, choose **ECDSA_ P256** for the algorithm name. Enter **256** in the **Minimum key size field**. For the **Request** hash, choose **SHA256**.

9. On the **Subject Name** tab, select **Supply** in the request to enter the **Subject Name** and **Common Name**. This can be the EUI64 MAC address string of a CGE Node and is used for additional user authentication against the RADIUS server.

10. On the **Security** tab, for all listed group or user names, ensure that the **Enroll** and **Autoenroll** permissions are selected.

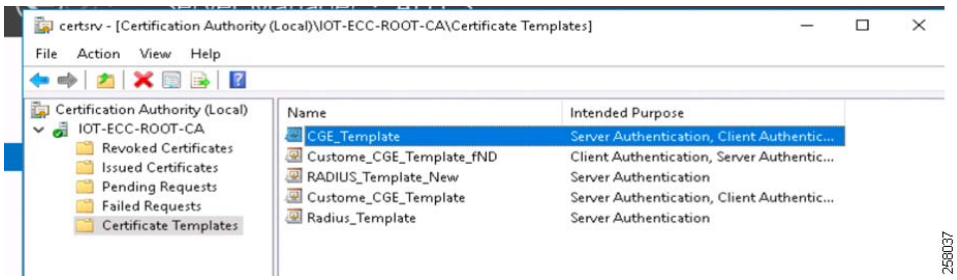
11. Select **Apply** and **OK**, close the **Certificate Template Console**, and then select the **Certificate Template** folder from the **Certification Authority (certsrv)**.

Figure 131 Creation of Certificate Template for CGE



12. Select **New**, select **Certificate Template** to **Issue**, and then select the new certificate template, for example **CGE_Template**, which the user generated earlier. The new certificate template should be listed within the **Certificate Templates** folder of the **Certification Authority Console**.

Figure 132 CGE Template to Issue Certificates



Generating the CGE Certificates

The following steps guide the administrator of the NPS servers to generate a certificate from the CA using the Template that was created above (CGE_Template).

1. Open the **Microsoft Management Console (MMC)** application on the Windows Server 2016 (**Run> mmc**). Be sure that the **Local Computer Certificates Snap-In** is loaded. However, for the first configuration for MMC, the user can click **File** and **Add/Remove Snap-in...**, and in the pop-up window, select and add the **Certificate Authority** in the left pane. Click **OK** and then click **Finish**.

2. Click **File** and **Add/Remove Snap-in**... and will pop the window, select **Certificates** in the left pane, and then click **Add**. Click **OK**, select **My user account**, and then click **Finish**.

3. In the **Add** or **Remove Snap-ins** window, select **Certificates** in the left pane and click **Add**. Click **OK**, select **Computer** account, click **Next**, select **Local Computer**, and then click **Finish**. The items are added in the left pane.

4. In the **Certificates (Local Computer)**, go to the **Personal** drop-down list. Select **Certificates**, right-click and select **All tasks**, select **Request New Certificate**, then click **Next** (**Certificates (Local Computer)-> Personal-> Certificates-> All Tasks-> Request New Certificate**).
5. Select **Active Directory Enrollment Policy** and then click **Next**.
6. Select **CGE_Template** and then click **More information** is required to enroll link below it.
7. In the **Certificate Properties Dialog**, in the **Subject** tab, choose **Common name** from the **Type** drop-down list. After filling in **EUID in Value**, click **Add**, and then click **OK**.
8. Click **Enroll** and then click **Finish** when enroll is completed.

Exporting CGE Certificates

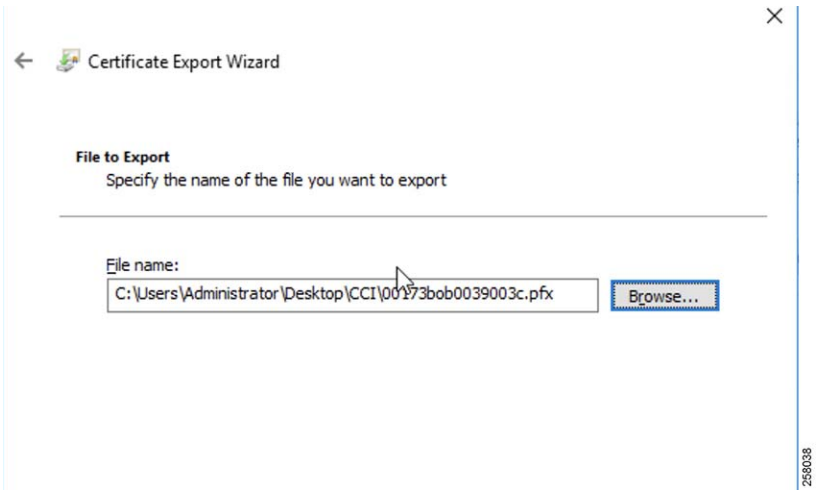
Three certificates need to be exported: CGE certificate with private key, CGE certificate with public key, and ECC CA Server Root Certificate with the public key only:

- CGE Certificate with Public Key will be added as and entry in the Active directory.
- CGE Certificate with Private Key will be programmed into CGE, which is used for authentication purposes.
- ECC CA Root Certificate will be programmed into CGE, which is used for identifying the valid root CA.

Exporting Certificate with Private Key

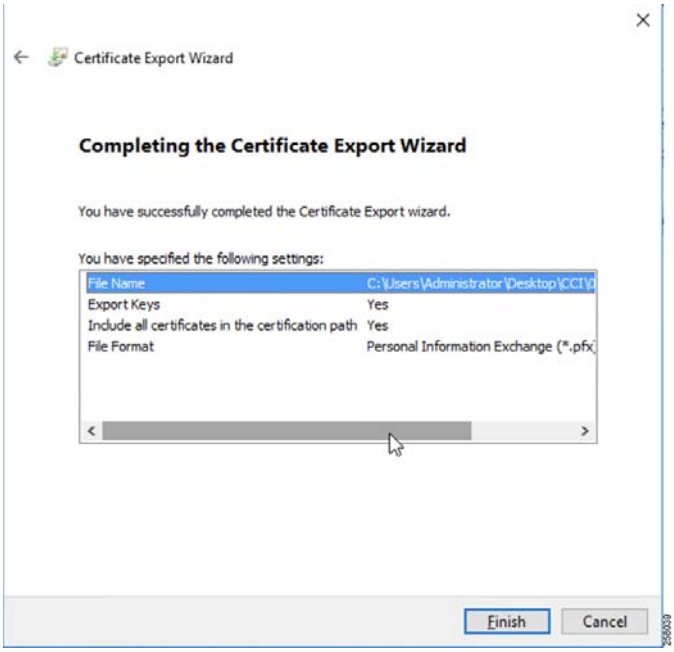
1. Return to the **MMC** application, highlight the newly created certificate (example: 00173b0b0039003c), right-click and select **All Tasks** and then select **Export**.
2. Follow the export wizard to the next screen. Select **Yes, export the private key**.
3. In **Certificate Export Wizard**, select **Include all certificates in the certification path if possible** and select **Next**. This includes the CA certificate.
4. Enter the password for certificate, which will be used in CGE. For default settings, use the password **Cisco123** and select **Next**.
5. Save the .pfx file.

Figure 133 Certificate Export of CGE



6. After exporting, the Certificate Export Wizard looks like what is depicted in Figure 134:

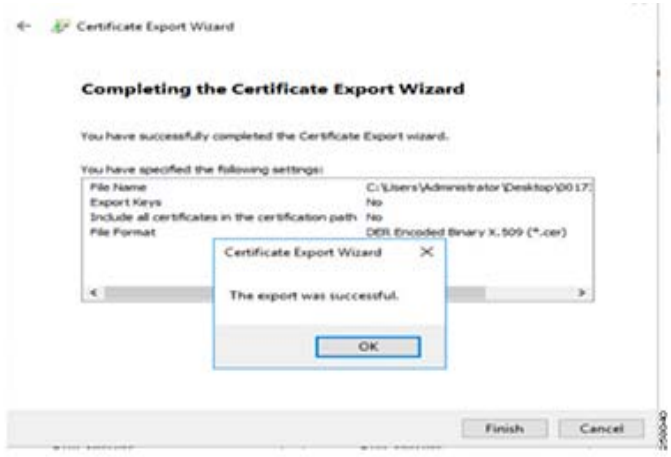
Figure 134 Successful Export of Certificate with Private Key



Exporting Certificate with Public Key

1. Return to the **MMC** application, highlight the newly created certificate (example: 00173b0b0039003c), right-click and select **All Tasks**, and then select **Export**.
2. Follow the export wizard to the next screen. Select **No, do not export the private key**.
3. Select the export file format **DER encoded binary X.509** (.CER). Click **Next** and save it as a .cer file.

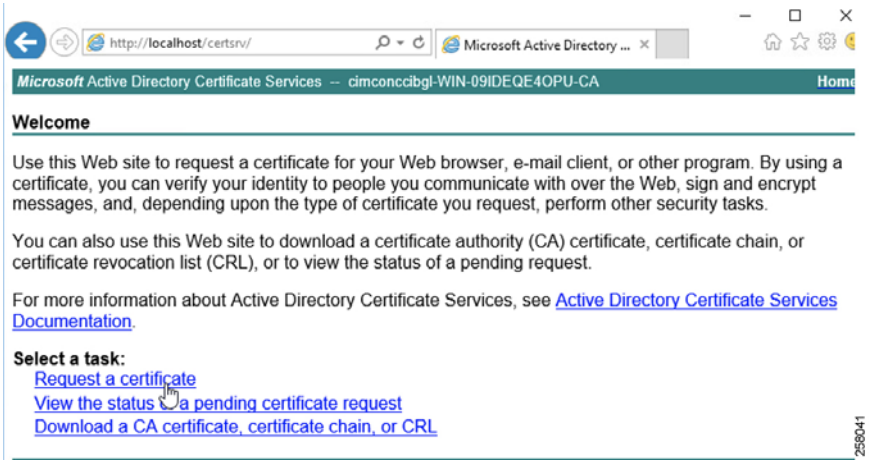
Figure 135 Successful Export of Certificate with Public Key



Exporting CA Server Certificate

1. Open the link on the NPS server and then click the link of **Download a CA certificate, certificate chain, or CRL**.

Figure 136 Exporting CA Certificate on ECC-CA Server



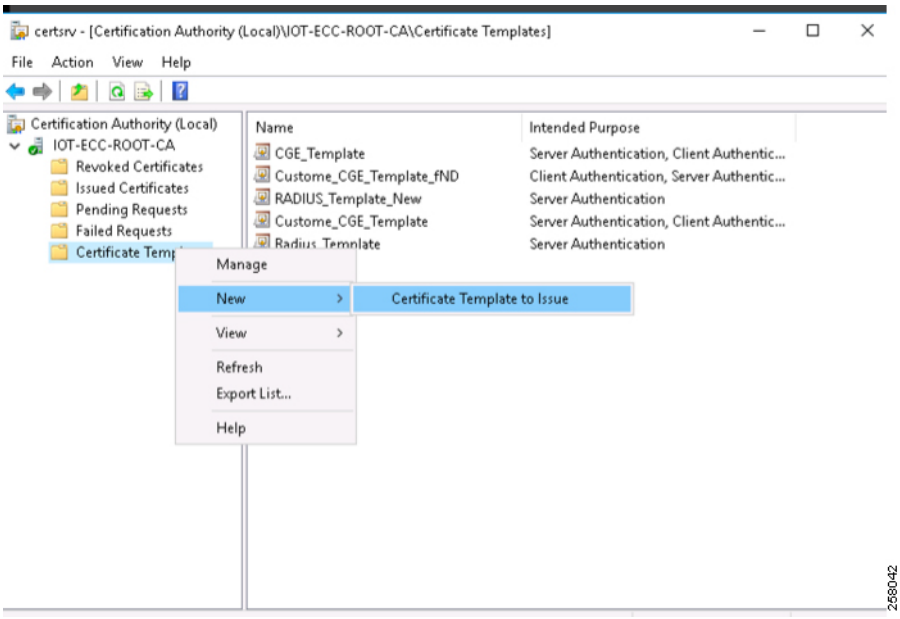
2. Click **Download CA certificate**, and then choose the **DER** format. This is the root certificate for the ECC CA server.

Creating and Configuring the RADIUS Template for CGR on the NPS

1. Launch **Certsrv (Certificate Authority Console)**, click **Server Manager**, select **Tools** and, in the drop-down list, select **Certification Authority**.
2. In **Certsrv** window on the **Certificate Authority / Sub-CA Server** (under **Certificate Authority**) running ECC Algorithm, right-click **Certificate Template**, and then select **Manage**.
3. Select and duplicate the Web Server certificate template from the **Certificates Templates Console.** In the **Compatibility** tab, select the **Windows Server 2016 for Certification Authority and Certificate Recipient**.
4. In the **General** tab, specify the Template display name (for example, **Radius_Template**), choose a validity period of **5 years** and Renewal period of **6 weeks**, and then click the **Publish certificate in Active Directory** check box.
5. On the **Request Handling** tab, choose **Signature** from the **Purpose** drop-down list. Select **Yes** in the **Certificate Templates** warning dialog. To allow certificate private key exports in the Request Handling tab, select **Allow private key to be exported**.
6. On the **Cryptography** tab, choose **Key Storage Provider** for the **Provider Category** and choose **ECDSA_ P256** for the algorithm name. Enter **256** in the **Minimum key size** field. For the **Request hash**, choose **SHA256**.
7. On the **Subject Name** tab, select **Supply** in the request to enter the **Subject Name** and **Common Name**.
8. On the **Security** tab, for all listed group or user names, ensure that the **Enroll** and **Autoenroll** permissions are selected.
9. On the **Extensions** tab, user should ensure that only **Server Authentication** is present. Click **Apply** and then **OK**. Close the **Certificate Template Console**.

   Note: User needs to add the newly created Radius_Template.
10. Select the **Certificate Template** folder from the **Certification Authority (certsrv)**.
11. Select **New**, select **Certificate Template to Issue** and the new certificate template (for example, **Radius_Template**, which the user generated earlier). The new certificate template should be listed within the **Certificate Templates** folder of the **Certification Authority Console**.

Figure 137 Configuring RADIUS Template



12. Restart **Certificate Authority**.

Generating the RADIUS Certificates

Note: In the CCI deployment, we are using two AAA servers: one is Microsoft NPS and the other is Cisco ISE. For CGE authentication, we are relying on Microsoft NPS since the CGE authentication is tightly coupled with Microsoft NPS server as per the current implementation.

The following steps guide the administrator of the NPS servers to generate a certificate from the CA using the template that was created above (**Radius_Template**):

1. Open the **Microsoft Management Console (MMC)** application on Windows Server 2016 (**Run> mmc**) and be sure the **Local Computer Certificates Snap-In** is loaded. However, for the first configuration for MMC, you can click **File and Add/Remove Snap-in**..., select **Certificates** in the left pane, and then click **Add**. Click **OK**, select **Computer** account, click **Next**, select **Local Computer**, and then click **Finish**. The items are added in the left pane.

2. In the **certificates (Local Computer)**, from the **Personal** drop-down list, select **Certificates**, right-click and select **All tasks**, select **Request New Certificate**, click **Next** (**Certificates (Local Computer)-> Personal-> Certificates-> All Tasks-> Request New Certificate**).

3. Select **Active Directory Enrollment Policy** and then click **Next**.

4. Select **Radius_Template** and click the **More information is required to enroll** link below it.

5. In the **Certificate Properties** dialog, in the **Subject** tab, choose **Common name** from the **Type** drop-down list. After filling in the **RADIUS** in **Value**, click **Add**, and then click **OK**.

6. Click **Enroll** and then click **Finish** when Enroll is completed.

Exporting RADIUS Private Certificate

1. Return to the MMC application and highlight the newly created certificate (example: Radius_Template), right-click and select **All Tasks**, and then select **Export**.

2. Follow the export wizard to the next screen. Select **Yes, export the private key**.

3. In the **Certificate Export Wizard**, select Include all certificates in the certification path if possible and then select **Next**. This includes the CA certificate.

4. Enter the password for the certificate that will be used in CGE. For default settings, use the password **Cisco123** and then select **Next**.

5. Save the .pfx file.

Figure 138 Configuring and Creating RADIUS Template

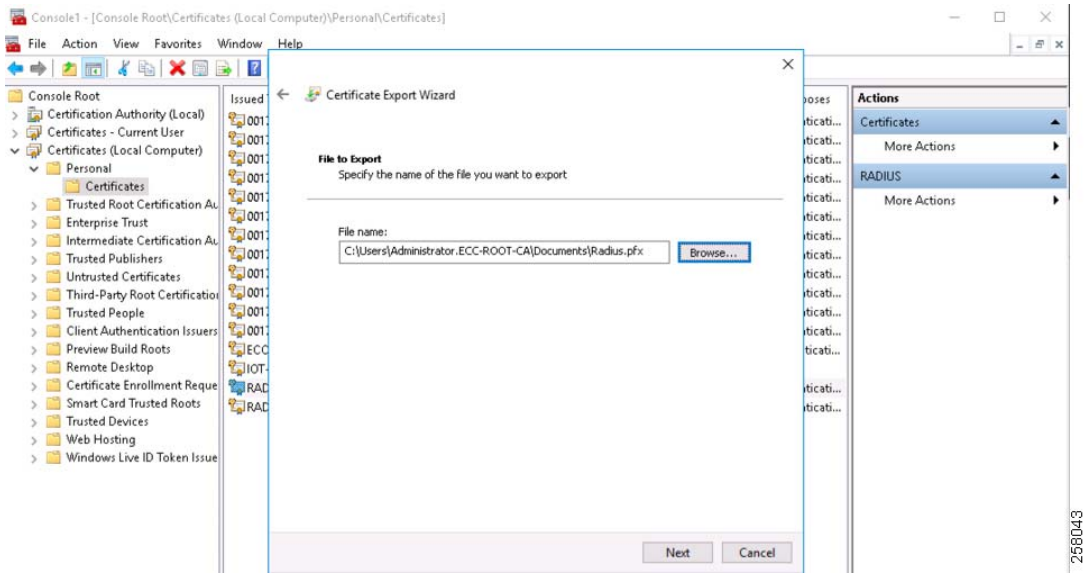
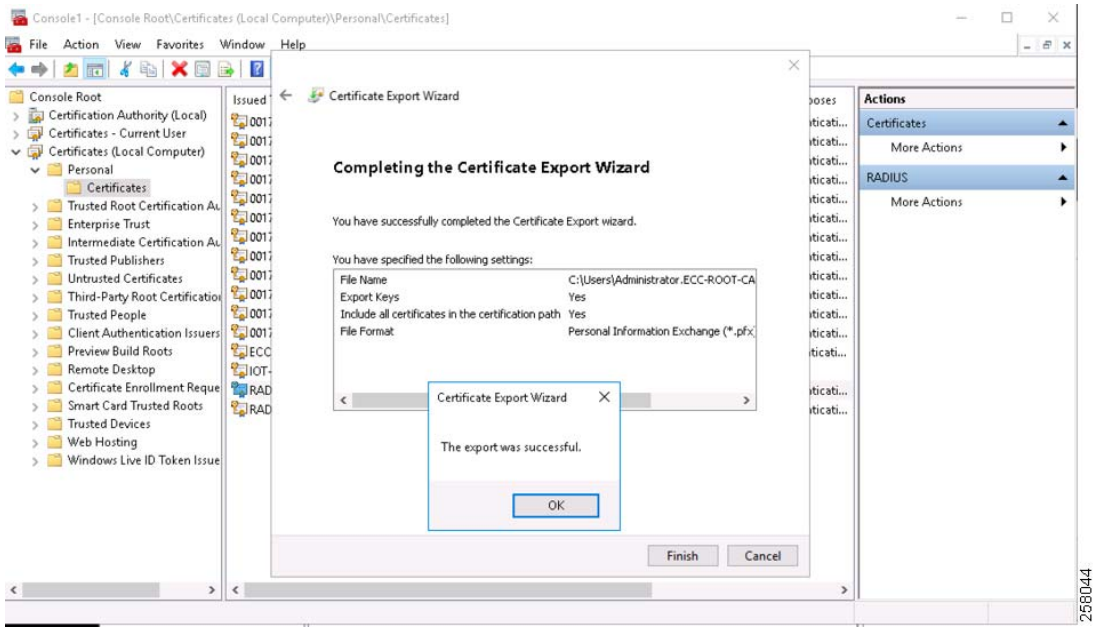


Figure 139 Exporting RADIUS Certificate with Private Key



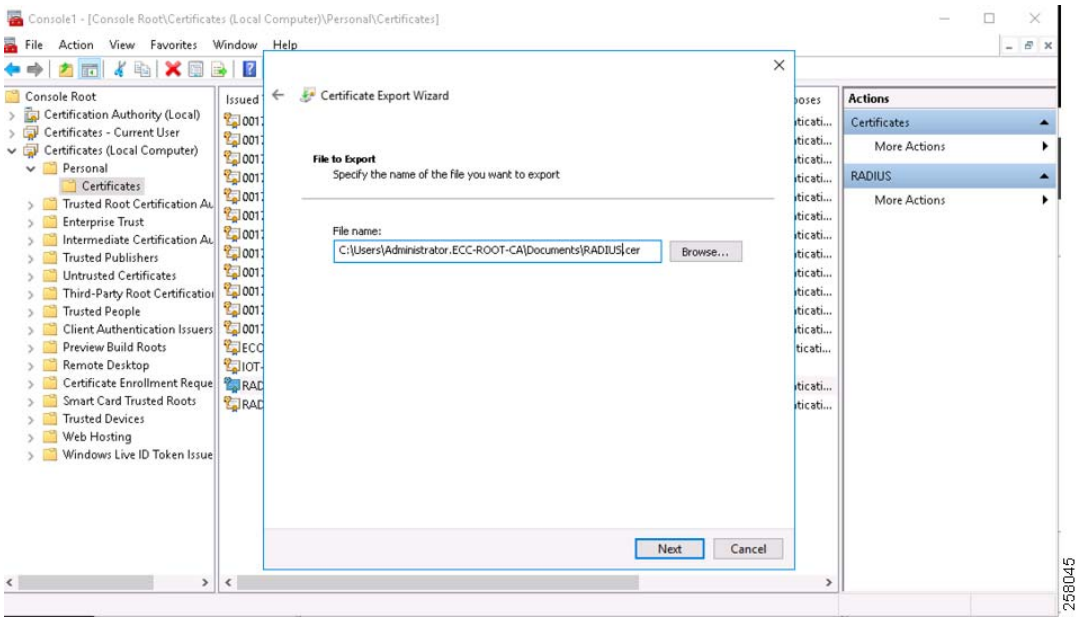
Exporting RADIUS Public Certificate

1. Return to the MMC application and highlight the newly created certificate (example: **Radius_Template**), right-click and select **All Tasks** and then select **Export**.

2. Follow the export wizard to the next screen. Select **No, do not export the private key**.

3. Select export file format **DER encoded binary X.509 (.CER)**. Click **Next** and save it as .cer file.

Figure 140 Exporting RADIUS Certificate with Public Key



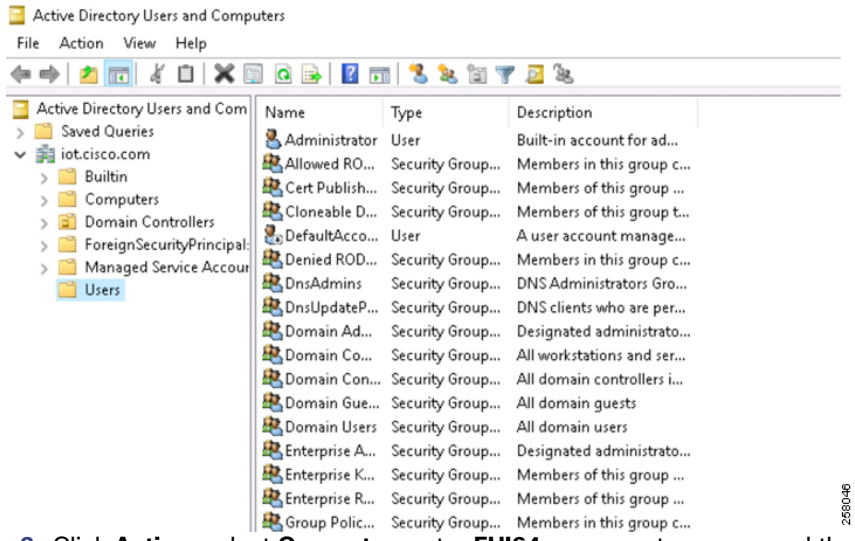
Configuring NPS Server, ADSI for CGE Authentication

CGE Configuration in NPS Server

Adding CGE to Active Directory of NPS

1. From **Start-> Administrative tools**, open **Active Directory Users and Computers**.
2. Select domain **iot.cisco.com** and then click **Computers** (example shown below).

Figure 141 Adding Computer (Node) to Active Directory Users and Computers



3. Click **Action**, select **Computer**, enter **EUI64** as computer name, and then click **OK**.
4. Click **View**, select **Advanced Features**, select the new computer, and then click **Action** and select **Name Mappings**.

5. In **Security Identity Mapping**, click **Add**, and navigate to the new public key cert (**00173b0b0039003c.cer**) above. Verify details and then click **OK**.

Modify the Active Directory Services Interface (ADSI) of CGE

1. Click **Start-> ADSI Edit**. Navigate to the **iot.cisco.com** and its computers.
2. Select the new node you added. Click **Action**, select **Properties**, and then scroll down to **servicePrincipalName**. Click to highlight and edit it.
3. Type in the string HOST/(here it should be **HOST/00173b0b0039003c**) as shown in the example above and click **Add**. Then click **OK**.

Figure 142 Configuring ADSI Parameters

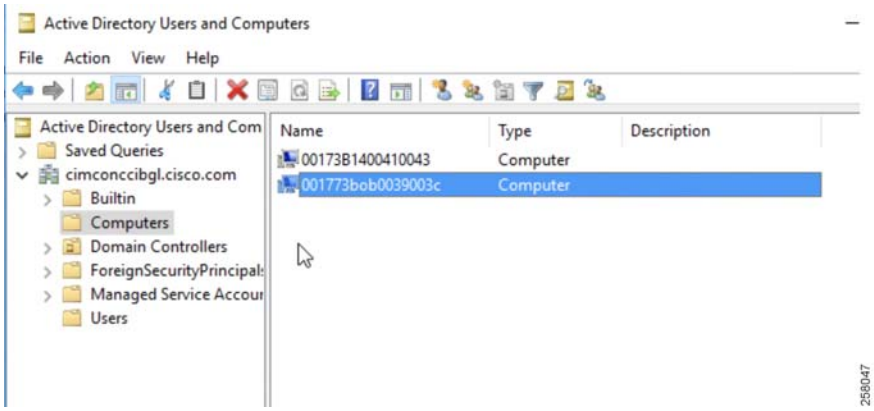
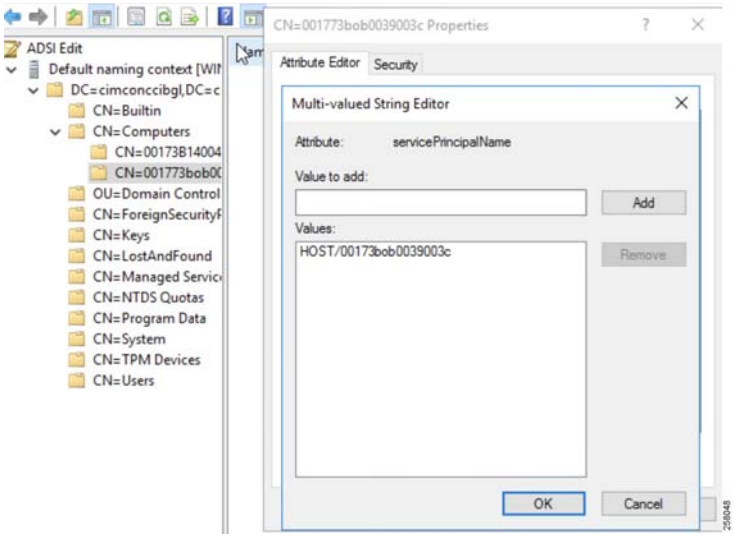


Figure 143 Adding Host EUID to ADSI



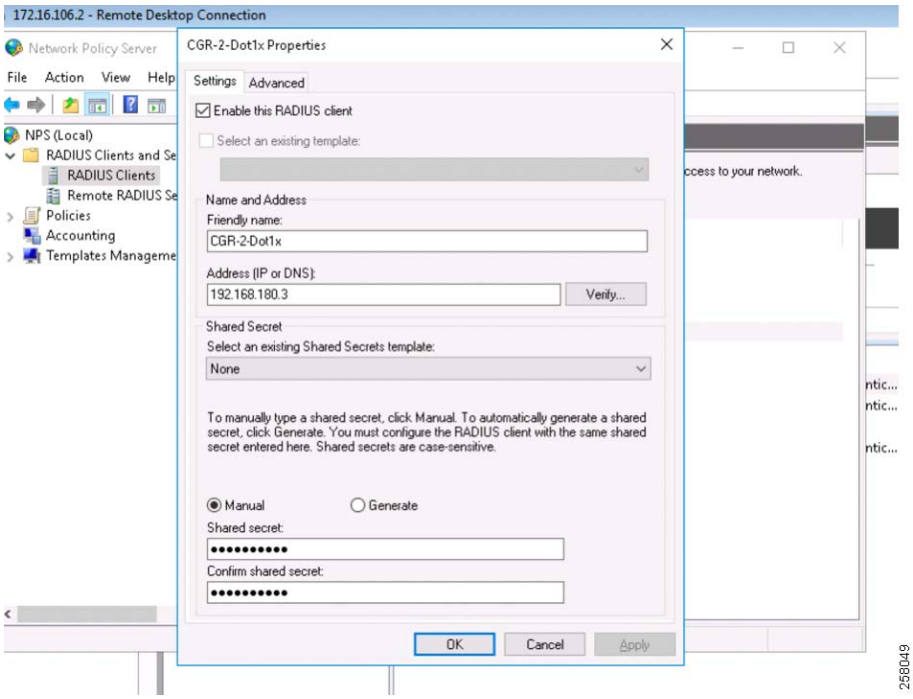
4. Close the ADSI edit window.

Adding CGR to RADIUS Server

1. From **Start**, click **Administrative Tools**, and then select **Network Policy Server**. Right-click the **NPS (Local)** icon and select **Register Server in Active Directory.**
2. Click **RADIUS Clients and Server** and select **RADIUS Clients**.

3. Click **Action** and select **New**. Select **Enable this RADIUS Client**, enter the details of your CGR, and then select **OK**. Note that the password (e.g., **cisco-123**) is the same as the configuration in the CGR and IP address is the IP address of the loopback of the CGR.

Figure 144 Adding CGR to NPS for Authentication



Configuring the Policies on the NPS Server

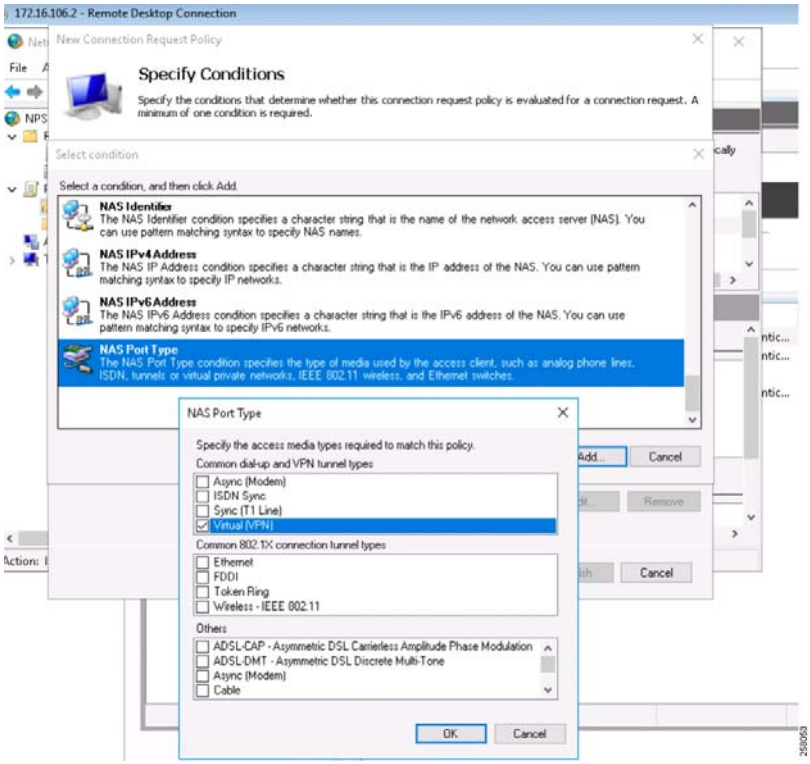
Turn on the Microsoft Network Policy Server (e.g., Windows Server 2016) configuration for the CR-Mesh network. Connection Request Policies and network policies must be configured for the CR-Mesh network.

1. Launch **Network Policy Server**, expand **Policies**, and select **Connection Request Policies**. Add a new **Connection Request Policy** by selecting **Action** and then selecting **New**. In the **Overview** tab:

   a. Enter a policy name (for example, **CRDC CGR Authorization Request**) and then click **Next**.

   b. In the **Specific Conditions** tab, click **Add** and in the pop-up window select **NAS Port Type**. In the next pop-up window, select **Virtual (VPN)** and click **Next**.

Figure 145 Configuring Policy for NPS Server



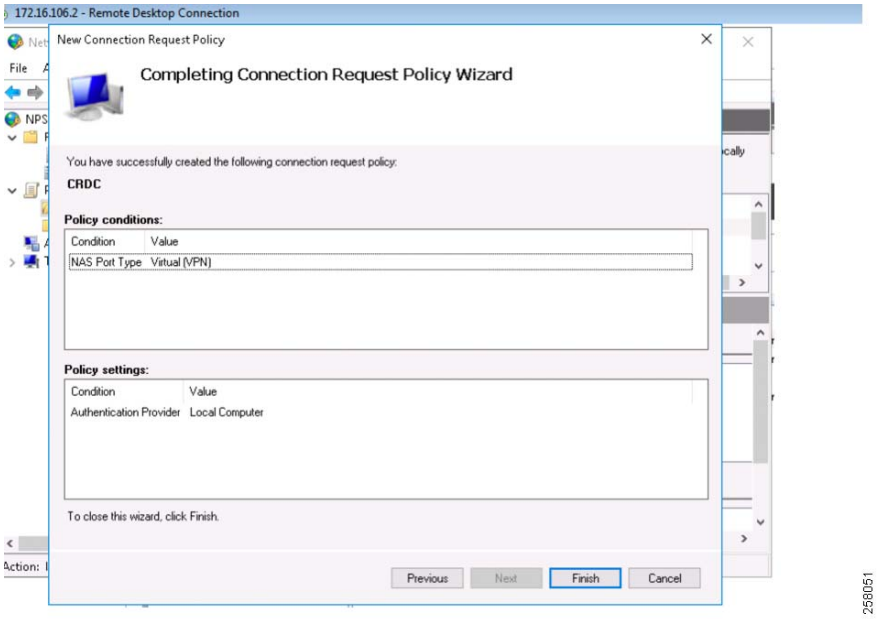
c. In the **Specific Request forwarding** tab, leave the default and click **Next**.

d. In the **Specific Authentication method** tab, leave the default and click **Next**.

e. In the **Configure settings** tab, leave the default and click **Next**.

f. Please review all the parameters in the **Completing Connection Request Policy Wizard** and click **Finish**.

Figure 146 Configuring and Verifying NPS Policy Parameters



2. Launch **Network Policy Server**, expand **Policies** and select **Network Policies**. Add a new Policy by selecting **Action** and then selecting **New**.

   a. In the **New Network Policy** window, enter **Policy** name (e.g., **CGR Authorization Request**) in the tab **Specify Network Policy Name and Connection Type** and then click **Next**.

   b. In the **Specific Conditions** tab, click **Add** and in the pop-up window select **NAS Port Type**. Then in the next pop-up window, select **Virtual (VPN)** and click **Next**.

   c. In the **Specify Access Permission** tab, choose the option **Access granted** and click **Next**.

   d. In the **Configure Authentication Methods** tab, in the right pane, under **EAP Types**, click **Add** and select the **Microsoft: Smart Card or other certificate** option.

   e. Select **Microsoft: Smart Card or other certificate** and click **Edit**. In the pop-up window “Certificate issued to” drop-down, select **RADIUS (RADIUS Server Certificate)** and click **OK**. Do not select the certificate issued to the CA if that certificate is also running on the same machine.

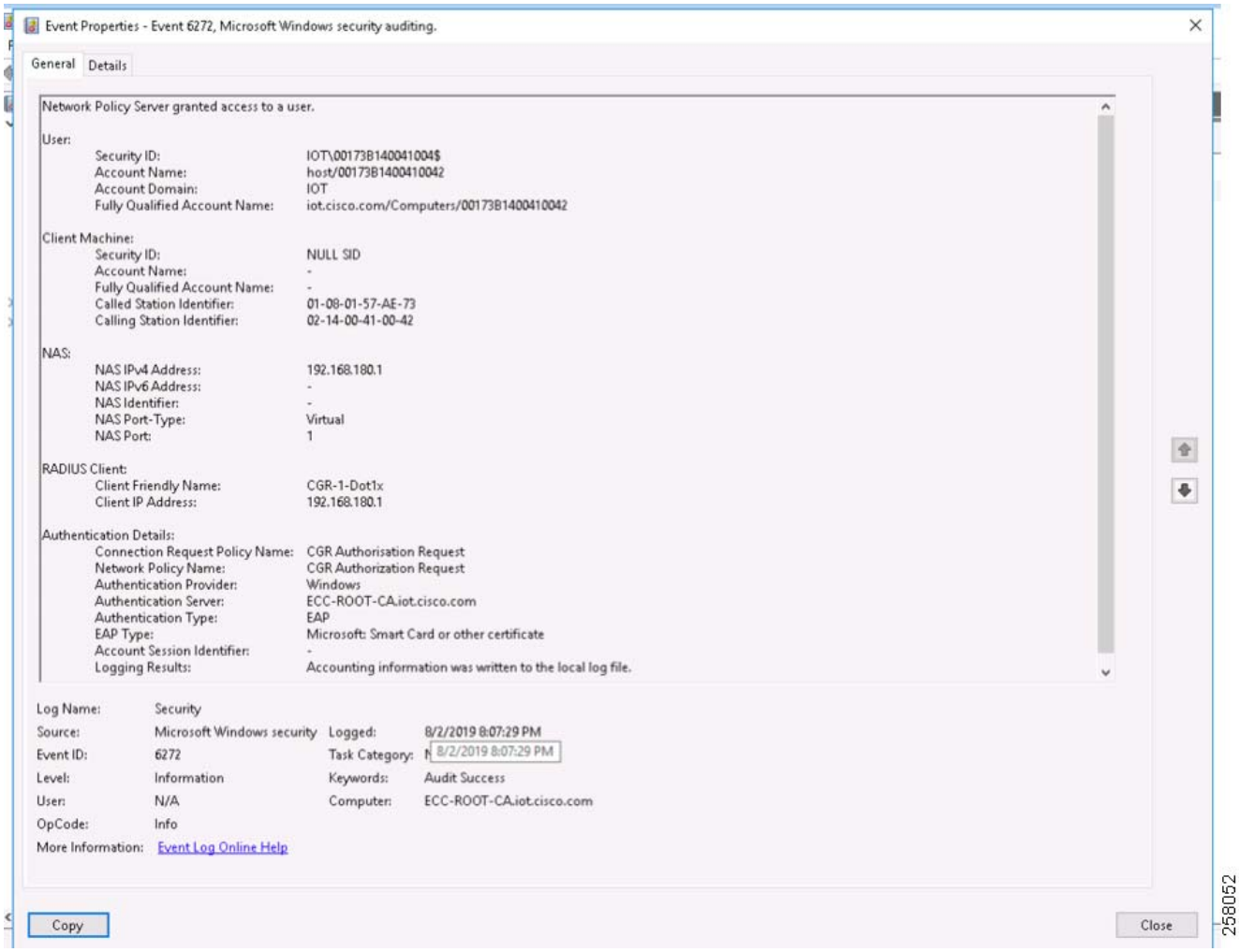
   f. On the **Configure Constraints** tab, leave everything as default and click **Next**.

   g. On the **Configure Settings** tab, specify **Standard RADIUS Attributes** and select **Framed-MTU**. Add the value **700** and then select **OK**. The **Termination-Action** set to default is optional.

   h. Click **Apply** and then **OK** to save all the properties of the Network Policy.

   i. Restart the **Network Policy Server**.

Figure 147 Successful Dot1x Completion Wizard



After installation of ECC CA Server, the following certificates were exported from the ECC CA server:

- **Root Certificate of the ECC CA Server**—This certificate is used to program in CGEs.
- **Private and Public certificate of CGEs**—These certificates are used to program in CGEs for Dot1x authentication.

Implementation of SSM and Generation of CSMP Certificates

The Field Network Director is prerequisite for this section, it is assumed that the FND is installed; if not, please refer to Implementing Field Network Director for CCI, page 44 for installation and configuration of FND.

Software Security Module (SSM) is a low-cost alternative to a Hardware Security Module (HSM). IoT FND uses the CSMP protocol to communicate with CGE endpoints. SSM uses **CiscoJ** to provide cryptographic services such as signing and verifying CSMP messages, and CSMP Keystore management. SSM ensures Federal Information Processing Standards (FIPS) compliance while providing services. The user needs to install SSM on the IoT FND application server or another remote server. SSM remote-machine installations use HTTPS to securely communicate with IoT FND.

This section describes SSM installation and setup, including:

- Installing or Upgrading the SSM Server, page 194

Installing or Upgrading the SSM Server

1. Get the IoT FND configuration details for the SSM. SSM ships with following default credentials:

```
ssm_csmp_keystore password: ciscossm
csmp alias name: ssm_csmp
key password: ciscossm
ssm_web_keystore password: ssmweb

[root@VMNMS demossm]# cd /opt/cgms-ssm/bin/
[root@VMNMS bin]# ./ssm_setup.sh

Software Security Module Server
1. Generate a new keyalias with self-signed certificate for CSMP
2. Generate a new keypair & certificate signing request for CSMP
3. Import a trusted certificate
4. Change CSMP keystore password
5. Print CG-NMS configuration for SSM
6. Change SSM server port
7. Change SSM-Web keystore password
Select available options. Press any other key to exit
Enter your choice :
```

2. Enter **5** at the prompt, and complete the following when prompted:

```
Enter current ssm_csmp_keystore password :ciscossm
Enter alias name : ssm_csmp
Enter key password :ciscossm
security-module=ssm
ssm-host=<Replace with IPv4 address of SSM server>
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

3. To connect to this SSM server, copy/paste the output from the previous step, and complete the following when prompted into the cgms.properties file.

   Note: You must include the IPv4 address of the interface for IoT FND to use to connect to the SSM server.

4. Start the SSM server:

```
[root@VMNMS ~]# service ssm start
Starting Software Security Module Server: [ OK ]
```

Integrating SSM and IoT FND

Note: You must install and start the SSM server before switching to SSM.

To switch from using the Hardware Security Module (HSM) for CSMP-based messaging to using the SSM:

1. Stop IoT FND:

```
service cgms stop
```

2. Run the ssm_setup.sh script on the SSM server.
3. Select Option 3 to print IoT FND SSM configuration.
4. Copy and paste the details into the cgms.properties to connect to that SSM server; an example is shown below.

```
security-module=ssm
ssm-host=127.107.155.85
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

5. Ensure that the SSM is up and running and the user can connect to it.
6. Restart IOT FND.

Generation of CSMP Certificate

New releases of FND change the certificate for the Web every time FND is upgraded. Therefore, the trust entry for web keystore in SSM needs to be updated. Adding the newly generated certificate for Web into the SSM web keystore Keystore location: **/opt/cgms-ssm/conf/ssm_web_keystore**.

1. From the **FND UI Web** Interface, go to **Admin** tab (in the top right corner)-> **SYSTEM MANAGEMENT**. Select **Certificate for Web**. Download the base64 version of Certificate for Web from the FND GUI. The file has been downloaded and saved as certForWeb.txt.
2. Transfer this file to the FND (RHEL OS) through the command line. For example, in the usual case, the file is stored under **/root/certForWeb.txt**.
3. Navigate to the SSM configuration directory **/opt/cgms-ssm/conf/**. View the content of the ssm_web_keystore using the following command:

```
"keytool -list -keystore ssm_web_keystore"

Observe, there might be two aliases minimum:
Alias #1: ssm_web
Alias #2: nms_trusted (this was created on march 30, 2015).
In newer releases of NMS(FND), after every upgrade new self-signed certificate would be generated.
Because of this, the trusted CA configuration in SSM web keystore would be obsolete.
[root@fnd conf]# keytool -list -v -keystore ssm_web_keystore
Enter keystore password: Entered "ssmweb" as password.
Keystore type: JKS , Keystore provider: SUN
Your keystore contains 2 entries

Alias name: ssm_web
Creation date: Jul 15, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=SSM_WEB, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US Issuer: CN=SSM_WEB, OU=CENBU,
O=Cisco, L=San Jose, ST=CA, C=US Serial number: 62e131c
Valid from: Tue Jul 15 18:48:34 EDT 2014 until: Wed Jul 15 18:48:34 EDT 2054
Certificate fingerprints:
MD5: D0:E0:D9:82:7E:99:ED:3A:38:21:A0:2C:AD:5B:BF:13
SHA1: 8B:A1:0B:9C:94:28:C1:1D:5F:43:BF:94:04:90:67:E7:50:2E:04:B0 SHA256:
B8:11:D7:82:0D:2D:B1:40:69:5E:2B:A5:E9:E7:D1:2D:CF:8C:CB:77:08:DB:52: C2:31:DF:AB:78:F1:36:35:7F
Signature algorithm name: SHA1withRSA Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9B 34 BA 3F 57 74 2F A0 32 4B A1 ED DE F7 78 93 .4.?Wt/.2K....x. 0010: D1 E8 5B 18
] ]
*******************************************
*******************************************
Alias name: nms_trusted Creation date: Mar 30, 2015 Entry type: trustedCertEntry
Owner: CN=CG-NMS, OU=IoTSSG, O=Cisco Systems, L=San Jose, ST=CA, C=US
```

```
Issuer: CN=CG-NMS, OU=IoTSSG, O=Cisco Systems, L=San Jose, ST=CA, C=US
Serial number: 1122fead
Valid from: Tue Mar 03 16:58:13 EST 2015 until: Sun Mar 01 16:58:13 EST 2020
Certificate fingerprints:
MD5: 6D:63:B9:8B:3F:C5:E9:6B:2B:DD:77:30:55:9D:C6:E7
SHA1: 5F:3B:84:92:06:22:CE:C4:FA:8B:F0:46:65:4B:CE:74:61:AA:3B:AE SHA256:
1C:59:50:40:92:09:66:D3:67:E9:AE:CA:6D:C8:25:88:FF:A8:26:F7:62:8A:13:E B:0E:EC:57:32:DB:03:94:31
Signature algorithm name: SHA256withRSA Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [ KeyIdentifier [
0000: 7F 21 68 0E 3D 21 24 BB 0010: C0 90 7E 5E
]
]
54 BB A6 6D 28 21 EE 8A .!h.=!$.T..m(!.. ...^
*******************************************
*******************************************
```

4. Updating the current certificate as a new trusted CA certificate in the SSM web keystore. Instead of replacing the existing nms_trusted alias, a new entry could be added to the Trusted CA certificate list. The following command imports the newly downloaded **certForWeb.txt** file into the keystore **ssm_web_keystore** under the alias name of **fnd**, and would be treated as a Trusted CA certificate, from this point onwards.

```
[root@fnd conf]# keytool -import -trustcacerts -keystore /opt/cgms- ssm/conf/ssm_web_keystore -file
/root/certForWeb.txt
Enter keystore password: <- Enter "ssmweb" as password.
Owner: C=US, ST=CA, L=San Jose, O=Cisco Systems, OU=IoT, CN=IoTFND
Issuer: C=US, ST=CA, L=San Jose, O=Cisco Systems, OU=IoT, CN=IoTFND
Serial number: d415544ff8fdca2a
Valid from: Mon Jan 28 08:26:37 EST 2019 until: Thu Jan 27 08:26:37 EST 2022 Certificate
fingerprints:
MD5: 93:55:50:D1:CA:42:88:AD:7A:91:5A:14:EA:68:DE:82
SHA1: 0F:62:18:34:02:A1:B6:B5:67:8D:24:F8:85:11:EF:87:5E:D2:D6:B9 SHA256:
76:41:45:06:BA:97:11:09:81:BD:90:B4:1D:C7:BA:A0:E7:76:B1:B5:3E:D5:48:B4:20:97:E9:F3: A6:B1:A4:01
Signature algorithm name: SHA256withRSA
Version: 1
Trust this certificate? [no]: yes (Certificate was added to keystore)
You have new mail in /var/spool/mail/root
```

5. Observe that the keystore should be having three trusted CA certificates now. Observe the newly added **fnd** alias name as third entry.

```
[root@fnd conf]# keytool -list -keystore ssm_web_keystore Enter keystore password:
***************** WARNING WARNING WARNING ***************** * The integrity of the information
stored in your keystore *
* has NOT been verified! In order to verify its integrity, *
* you must provide your keystore password. * ****************** WARNING WARNING WARNING
*****************
Keystore type: JKS Keystore provider: SUN
Your keystore contains 3 entries
nms_trusted, Mar 30, 2015, trustedCertEntry,
Certificate fingerprint (SHA1): 5F:3B:84:92:06:22:CE:C4:FA:8B:F0:46:65:4B:CE:74:61:AA:3B:AE
ssm_web, Jul 15, 2014, Private-KeyEntry,
Certificate fingerprint (SHA1): 8B:A1:0B:9C:94:28:C1:1D:5F:43:BF:94:04:90:67:E7:50:2E:04:B0 fnd,
Feb 1, 2019, trustedCertEntry,
Certificate fingerprint (SHA1): 0F:62:18:34:02:A1:B6:B5:67:8D:24:F8:85:11:EF:87:5E:D2:D6:B9
[root@fnd conf]#
```

6. Restart the SSM server for the change to take effect. There is no need to restart FND (cgms).

```
[root@fnd conf]# service ssm status ? ssm.service - (null)
Loaded: loaded (/etc/rc.d/init.d/ssm; bad; vendor preset: disabled) Active: active (running) since
Mon 2019-01-28 23:50:56 EST; 3 days ago
Docs: man:systemd-sysv-generator(8)
Process: 29038 ExecStart=/etc/rc.d/init.d/ssm start (code=exited, status=0/SUCCESS)
```

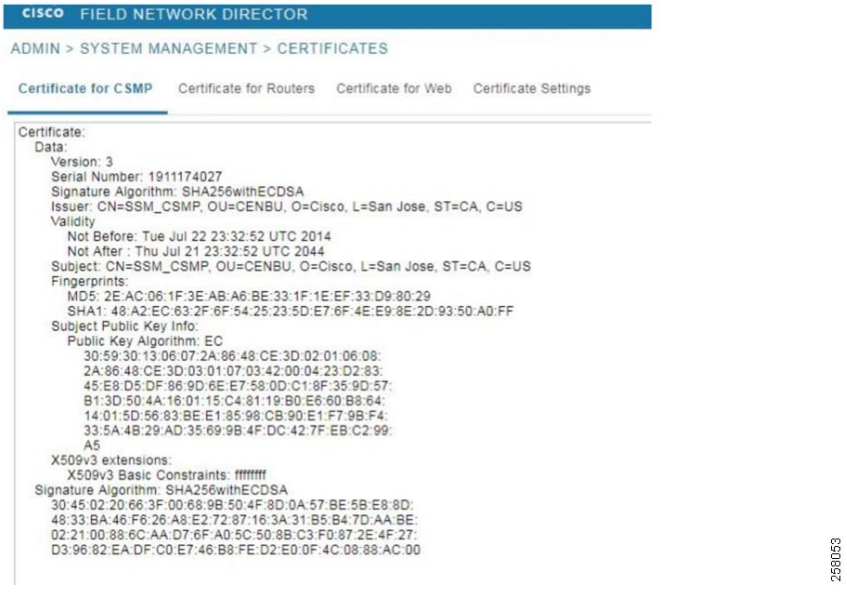
```
CGroup: /system.slice/ssm.service
??29050 java -server -Xms128m -Xmx1g -XX:MaxPermSize=256m -server -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/c...
Jan 28 23:50:55 fnd.ipg.cisco.com systemd[1]: Starting (null)...
Jan 28 23:50:56 fnd.ipg.cisco.com ssm[29038]: Starting Software Security Module Server: [ OK ]
Jan 28 23:50:56 fnd.ipg.cisco.com systemd[1]: Started (null).
[root@fnd conf]# service ssm restart
Restarting ssm (via systemctl): [ OK ]
```

7. Along with two other entries, the fnd entry will be added:

```
Entire output with verbose
[root@fnd conf]# keytool -list -v -keystore ssm_web_keystore Enter keystore password:
***************** WARNING WARNING WARNING ***************** * The integrity of the information
stored in your keystore *
* has NOT been verified! In order to verify its integrity, *
* you must provide your keystore password. * ***************** WARNING WARNING WARNING
*****************
Keystore type: JKS Keystore provider: SUN
Your keystore contains 3 entries (2 other entries were removed)
Alias name: fnd
Creation date: Feb 1, 2019 Entry type: trustedCertEntry
Owner: C=US, ST=CA, L=San Jose, O=Cisco Systems, OU=IoT, CN=IoTFND Issuer: C=US, ST=CA, L=San Jose,
O=Cisco Sys-tems, OU=IoT, CN=IoTFND
Serial number: d415544ff8fdca2a
Valid from: Mon Jan 28 08:26:37 EST 2019 until: Thu Jan 27 08:26:37 EST 2022 Certificate
fingerprints:
MD5: 93:55:50:D1:CA:42:88:AD:7A:91:5A:14:EA:68:DE:82
SHA1: 0F:62:18:34:02:A1:B6:B5:67:8D:24:F8:85:11:EF:87:5E:D2:D6:B9 SHA256:
76:41:45:06:BA:97:11:09:81:BD:90:B4:1D:C7:BA:A0:E7:76:B1:B5:3E:D5:48:B4:20:97:E9:F3: A6:B1:A4:01
Signature algorithm name: SHA256withRSA Version: 1
*******************************************
```

8. FND does not need to be restarted; restarting SSM alone is sufficient. FND now displays the certificate under the certificate for CSMP.

Figure 148 CSMP Certificate in FND after Installing SSM



Implementation of the Headend Router (HER)

The Headend Router (HER) is the converging point for the Headend. HER provides the routing connectivity between the components located in the DMZ versus components located in the data center area.

The HER also provides the routing connectivity between the FARs as well as the Headend components. As the traffic from the FAR is crossing an untrusted WAN, the traffic can be encrypted (optional, but highly recommended) for secure transmission over the WAN. The HER can terminate the secure tunnels from FAR and enable the communication between the FARs and Headend components like the FND, DHCP server, RSA CA server, and ECC CA server.

Note: The HER is located in the DMZ area. The HER provides routing connectivity for the FARs, with Headend components located in both the DMZ and the Data Center, as well as with application servers. Unlike other Headend components that interact between themselves at the application layer, the interaction of the HER is not at the application layer level. These interactions are only at the routing/transport layer. There should be IPv6 reachability between FND, which is present in shared services, and HER.

Prerequisite: IP Address of all the components must be reachable from the HER.

In this implementation, the Cisco CSR 1000v is used as the HER (the user should install two CSRs and should be in HSRP for redundancy). In addition, the majority of components in this implementation synchronize their time with the HER using the NTP protocol.

This section covers the following processes:

1. HER interfaces
2. NTP configurations:
   a. Configure the HER as the NTP primary for other Headend components.
   b. Configure network time source for the HER.
3. Integrating the HER with FND:
   a. Verify that the HER is reachable from the FND.
   b. Import the details of the HER into FND.
   c. Verify the HER/FND communication.
4. Certificate enrollment of the HER:
   a. Verify RSA CA server reachability from the HER.
   b. Receive a copy of the RSA CA server certificate.
   c. Receive the certificate of HER, signed by the RSA CA server.
5. Secure the communication with HER.
6. Selective route advertisement from the HER to the FAR:
   – Route advertisement using IKEv2, post-tunnel establishment with the FAR.

HER Interfaces

The HER has the following types of interfaces:

- DMZ Interface
- Loopback

Role of DMZ Interface

DMZ interfaces are used to receive the communication from the FARs and field devices like CGEs.

HER Configuration for the Field-facing WAN Interface (located in DMZ)

```
*****     CONFIGURATION ON HER for FAR facing interface ***
##Active Router Configuration
interface Gigabit Ethernet xx(interface number)
 description xx
 ip address x.x.x.x 255.255.255.x
 standby version 2
 standby a(Group Number different for different) ip y.y.y.y
 standby a priority 105
 standby a preempt delay min 120

##Standby Router Configuration
interface Gigabit Ethernet xx(interface number)
 description xx
 ip address x.x.x.x 255.255.255.x
 standby version 2
 standby a(Group Number different for different) ip y.y.y.y
 standby a preempt
```

The HER would use this field-facing DMZ interface for communication with the FAR. The interface is also configured with a virtual IP address to facilitate redundancy across multiple HERs.

Note: FAR would initiate the secure tunnel to this virtual IP address (y.y.y.y)

Role of Loopback Interface

Using the field-facing DMZ interface, an overlay tunnel is established between the loopback interface of the HER and the FAR.

The sections NTP Configurations, Integrating HER with FND, and Certificate enrollment of the HER are available at the following URL:

- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

Refer to Implementing HER on page 296 at the above URL.

Secure the Communication with HER

The FlexVPN tunnel is used to secure the tunnel between the HER and the FAR. FlexVPN is a robust, standards-based encryption technology, which uses IKEV2 as a security technology. The tunnel configurations should be mapped to the correct security configurations. After the configurations are complete, the communication between the HER and the FAR is validated. For the communication between the HER and the FAR to be successful, the encryption algorithm, hashing algorithm, and Diffie-Hellman group should match between the HER and the FAR.

HER Virtual-Template Configuration

This configuration shows a virtual template configuration on the hub that allows multiple spoke configurations to be established.

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback180
 ipv6 enable
 tunnel protection ipsec profile FlexVPN_IPsec_Profile_Cert
!
```

HER Security Configuration

The following configurations are important for the FlexVPN tunnel to be established. The IKEV2 proposal lists out the hashing algorithm, encryption algorithms, and Diffie-Hellman group that should be used in establishing the tunnel. This proposal is attached to the policy. In this, the authentication is done using a certificate based. The IKEV2 contains the virtual-template or the tunnel on which the security configurations should be applied. The IKEV2 profile is attached to the IPsec profile and the IPsec profile is attached to the virtual template.

This section covers the IKEv2 configuration required for certificate-based authentication:

The issuer common name used is IOT-RSA-ROOT-CA, which is the common name entered during the subject name configuration of RSA CA server.

```
crypto pki certificate map FlexVPN_Cert_Map 1
issuer-name co cn = iot-rsa-root-ca
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_Cert
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_Cert
 proposal FlexVPN_IKEv2_Proposal_Cert
!
crypto ikev2 profile FlexVPN_IKEv2_Profile_Cert
 match identity remote fqdn CGR1240_ FTX123456B.iot.cisco.com
 #match identity remote fqdn CGR1240_ FTX123457B.iot.cisco.com <<In case of multiple spokes>>
 match certificate FlexVPN_Cert_Map
 identity local fqdn hub-flexVPN
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 dpd 30 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 1
!
```

HER Crypto Configuration-IPSec

This section covers the IPSec configuration required for certificate-based authentication:

```
crypto ipsec security-association replay disable
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_Cert esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile_Cert
 set transform-set FlexVPN_IPsec_Transform_Set_Cert
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile_Cert
 responder-only
!
```

HER Virtual-Template Configuration

The IPv4 and IPv6 addresses configured under the loopback interface are used in the establishment of the tunnels at the HER. Tunnels from multiple field routers can terminate on the same virtual-template interface. A virtual-access would be cloned out of the virtual-template to serve the purpose of tunnel endpoint.

The virtual-template is configurable when no active virtual-access exists or when the virtual-template interface is in shut-down state. Traffic flowing through the virtual-template can be secured with the help of the FlexVPN tunnel.

```
interface Loopback180
 ip address 192.168.180.2 255.255.255.0
```

```
 ipv6 address 2001:DB8:DABA:FACE::2/64
 ipv6 enable
!
!
```

Selective Route Advertisement from HER to FAR

This section covers the route advertisement using IKEv2, instead of using routing protocol.

1. Once the tunnel is established, routes can be advertised over it using IKEv2. Advertising routes using IKEv2 instead of routing protocol has the following benefits:
   - The lowest bandwidth consumption for route exchange.
   - In turn, low cost to maintain the communication between the field element and the Headend.
2. This implementation advertises default route to the tunnel peers by implementing the IPv4 and IPv6 access lists.
3. To be able to advertise specific routes instead of a default route, IPv4 and IPv6 access lists need to be modified by permitting specific prefixes only. Advertising specific prefixes, instead of default route is recommended.
4. In this case, using access lists we are going to advertise specific prefixes of FND, CPNR, ECC CA Server, RSA CA Server (if needed), and use case-based IPv4/IPv6 addresses.

```
!
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit 172.16.103.100
!
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 sequence 50 permit ipv6 2001:DB:12::/64 any
 permit ipv6 2001:DB8:16:107::/64 any
!
!
aaa authorization network FlexVPN_Author_Policy local
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
```

Implementation of the DHCPv6 Server for the IP Addressing of the CGEs

A centralized DHCPv6 server is required to be provisioned in the network to assign IPv6 addresses to CGEs. A DHCP server setup in the shared services network can be configured to enable DHCPv6 service with required scope options. In this implementation, an example configuration to provision a DHCPv6 server leveraging Cisco Prime Network Registrar (CPNR) for CGE IP addressing is discussed.

Note: The main purpose of the DHCPv6 server is to allocate the IPv6 address/prefix dynamically to the field devices (CGEs), not for any Headend components.

Use Case—To allocate IPv6 addresses to CGEs

1. Optionally, an IPv6 prefix can also be delegated along with the IPv6 address (allocated to endpoint).
2. This delegated IPv6 prefix can be used to enable IPv6 address auto-configuration of applications located behind the endpoint.

This section has been implemented using the following flow:

1. Prerequisites

2. CPNR Regional Server Setup
3. CPNR Local Server Setup
4. Integrating CPNR (DHCP) with FND
5. CPNR Configuration of Address Allocation to CGEs

Prerequisite Steps

1. Obtain the CPNR license by mentioning the features needed (like DNS or DHCP).
2. Obtain the CPNR license to suit the scale requirement.
3. Download the latest CPNR X.Y.Z files from www.cisco.com. For example:
   - cpnr_9_1_2_regional.ova
   - cpnr_9_1_2_local.ova
4. Server that hosts the Headend components should be running ESXI as Type-1 hypervisor.
5. Deploy both the regional and local OVAs on the ESXI server:
   a. Ensure both OVAs are successfully deployed as VMs.
   b. Power on both the local and regional VMs.
   c. Open console of both the VMs using the vSphere client and set the root password.
   d. Accept the end user license agreement on both VMs.

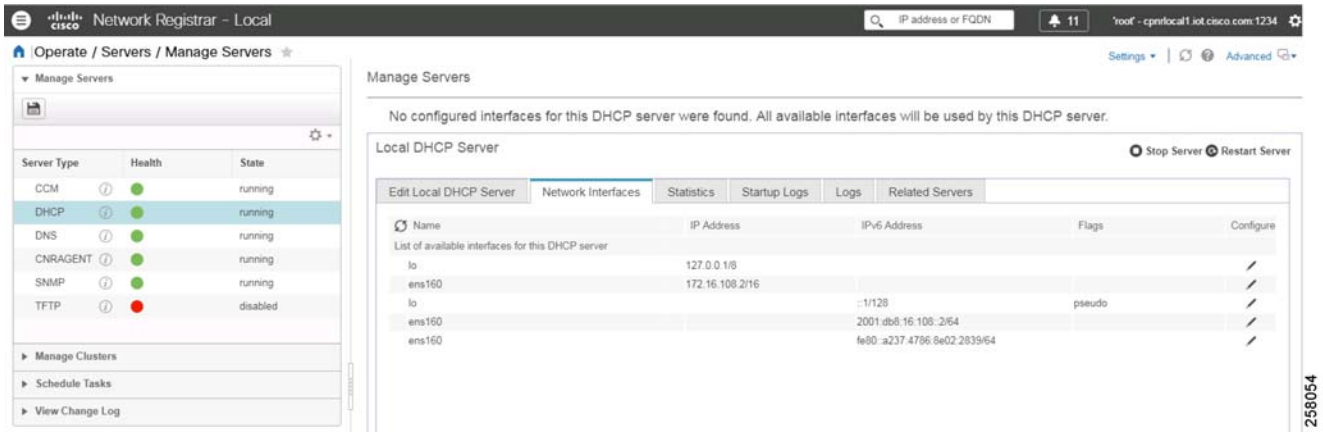
The sections CPNR Regional Server Setup, CPNR Local Server Setup, and Integrating CPNR(DHCP) with FND are available at the following URL (refer to “Implementing DHCP Server”):

- https://salesconnect.cisco.com/#/content-detail/da249429-ec79-49fc-9471-0ec859e83872

CPNR Configuration of Address Allocation to CGEs

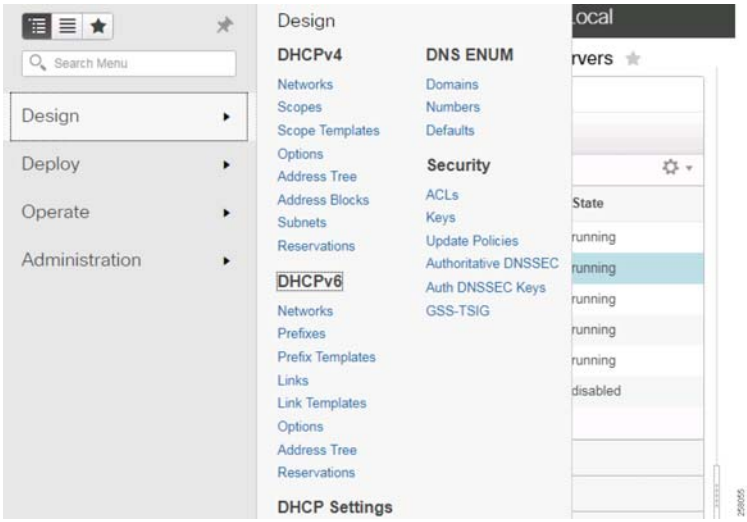
1. Log in to local CPNR (10.x.x.x:8080), click **Settings** (top right), and choose **Advanced**. From **Operate-> Manage servers**, select **Local DHCP server** (on left panel), and select **Network interfaces** (in middle panel). IPv6 address of CPNR is **2001:a:b:c::d**, which is to be used for configuring the FAR relay interface. Therefore, click **Configure** for **2001:a:b:c::d** interface (the last entry in Figure 149 for eth160).

Figure 149 CPNR Ethernet Interface Configuration



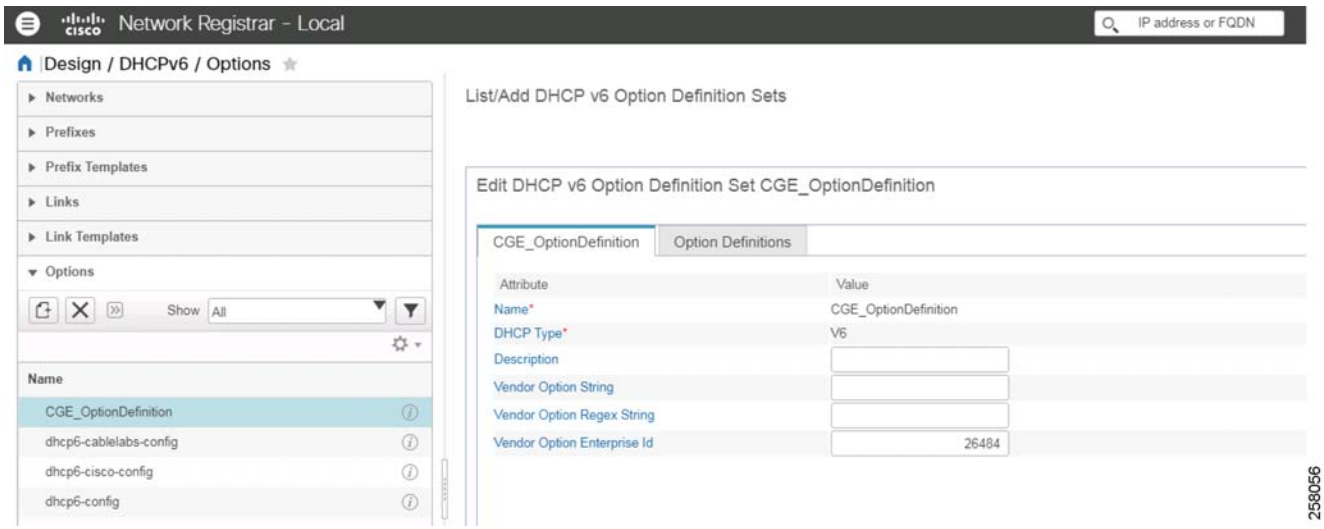
2. From **Design-> DHCPv6**, select **Options**.

Figure 150 CPNR DHCPv6 Options



3. Choose the **Add** Option (+ icon). Under **Options** menu in the left panel, as shown in Figure 151.

Figure 151 DHCPv6 Option Definition Creation

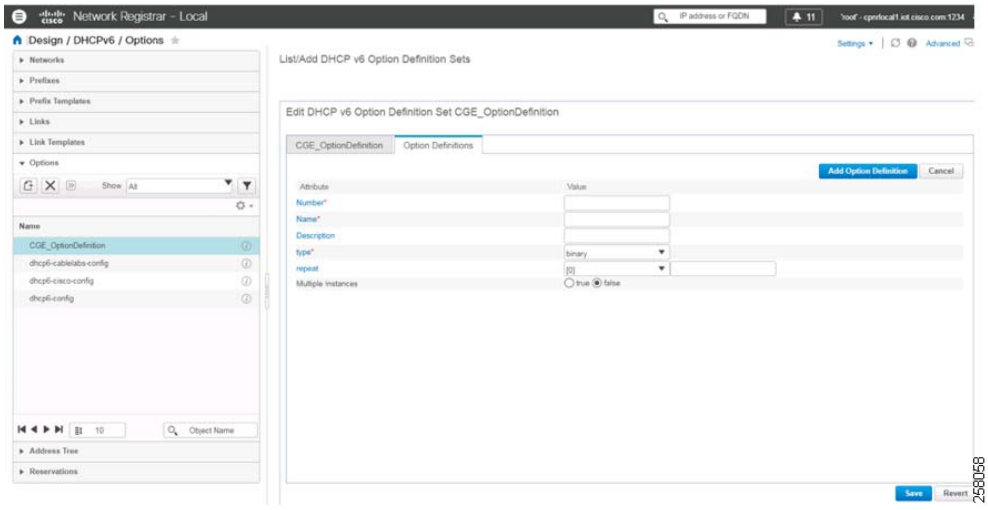


4. In the pop-up window, enter the corresponding values: **Name=CGE_OptionDefinition**, **Type = DHCPv6**, **vendor option enterprise id: 26484**, and then click **Add OptionDefiniteSet**. The option definition set is created.

Figure 152 Setting the Values for Option Definition 258057

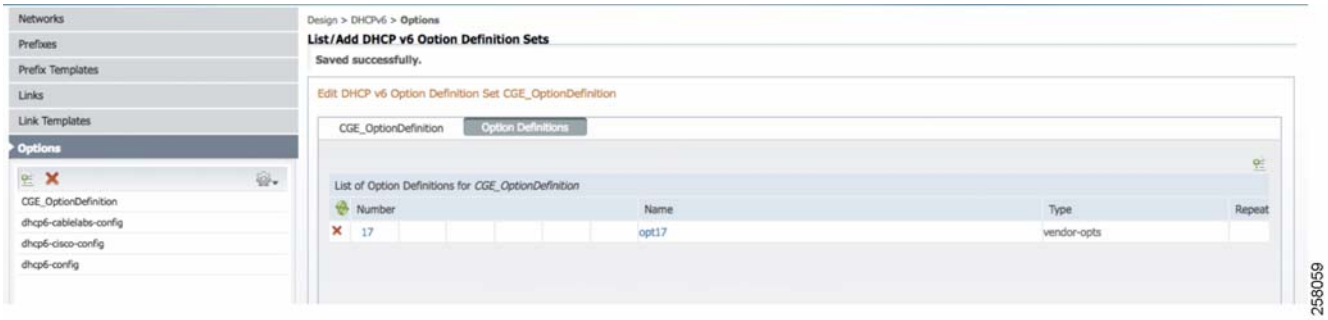
5. On left panel, choose **Options-> CGE_OptionDefinition** and then in the middle panel choose **Option Definitions**. Enter the **Add** icon (+) to enter the corresponding values: **Number: 17**, **Name: opt17**, **Select type: vendor-opts** from the drop-down list, click **Add Option Definition**, and then click **Save**. The user should receive a Saved Successfully" message.

Figure 153 Setting opt-17 Value for Option Definition



6. Click **Option Definitions** and select **opt17** that has just been created.

Figure 154 Successful Creation of opt 17

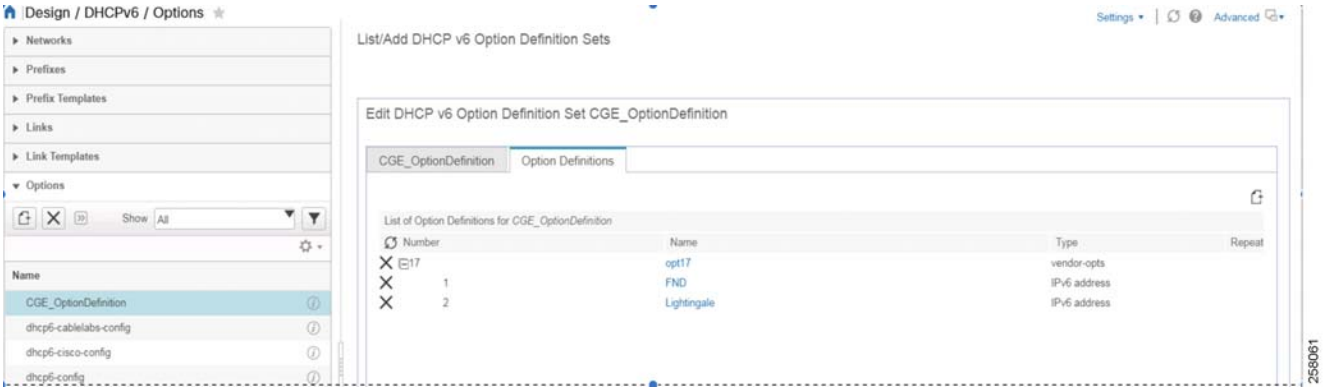


a. Click **Add** sub-option definition for adding NMS IPv6 Address. Enter the following fields in sub-option definition **Number=1**, **Name=NMS**, **type=Ipv6 address** from the drop-down list. Leave repeat field as is. Click **Add Sub-Option definition**. Then click **Save**.

b. Click **opt17** again and then click **Add sub-option definition** again for adding the CE IPv6 Address. Enter the following fields in sub-option definition: **Number=2, Name=Lightingale, type=Ipv6 address** from the drop-down list. Leave repeat field as is. Click **Add Sub-Option definition**. Then click **Save**. After saving both the values, it looks like Figure 155.

Figure 155 Creation of sub-option for opt-17

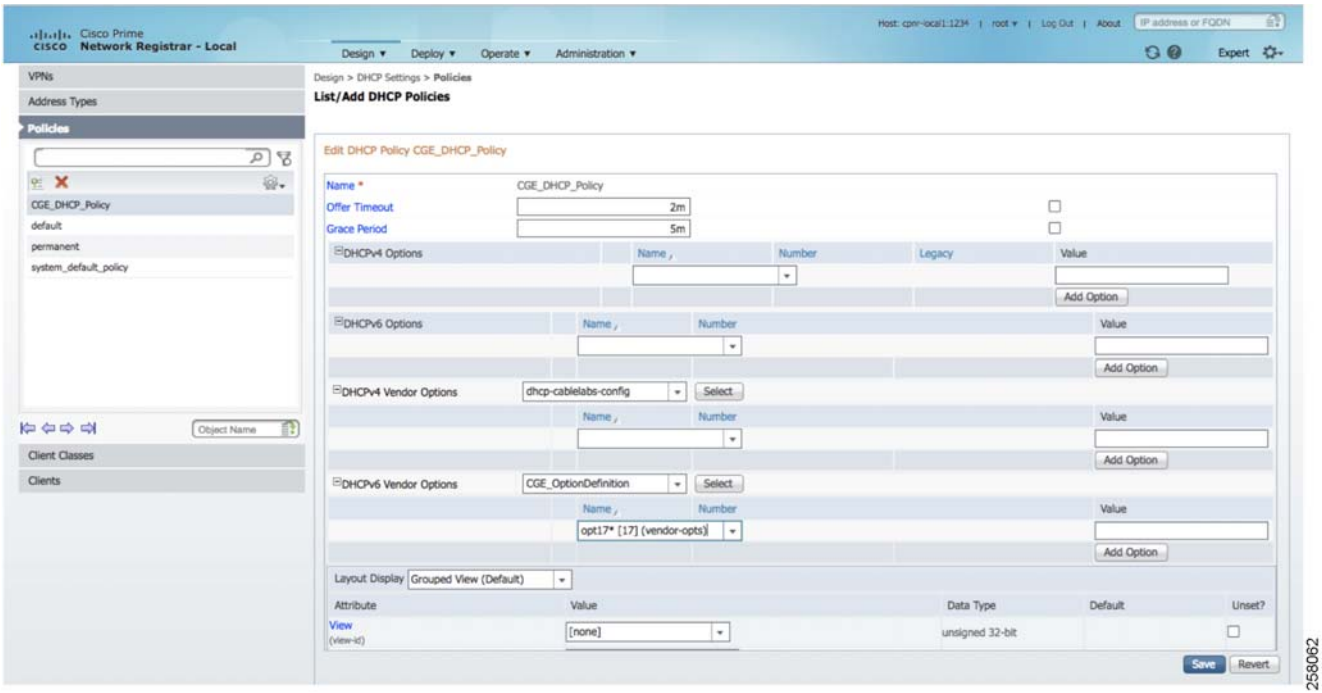
Figure 156 DHCP v6 Definition Set with opt-17 and Sub-options



7. To create a DHCP Policy, from **Design-> DHCP Settings**, select **Policies**. Create **'+'** under **Policies**. In the **Add a DHCP Policy** pop-up menu, from the column **Name: CGE_DHCP_Policy**, select **Add DHCP Policy**.

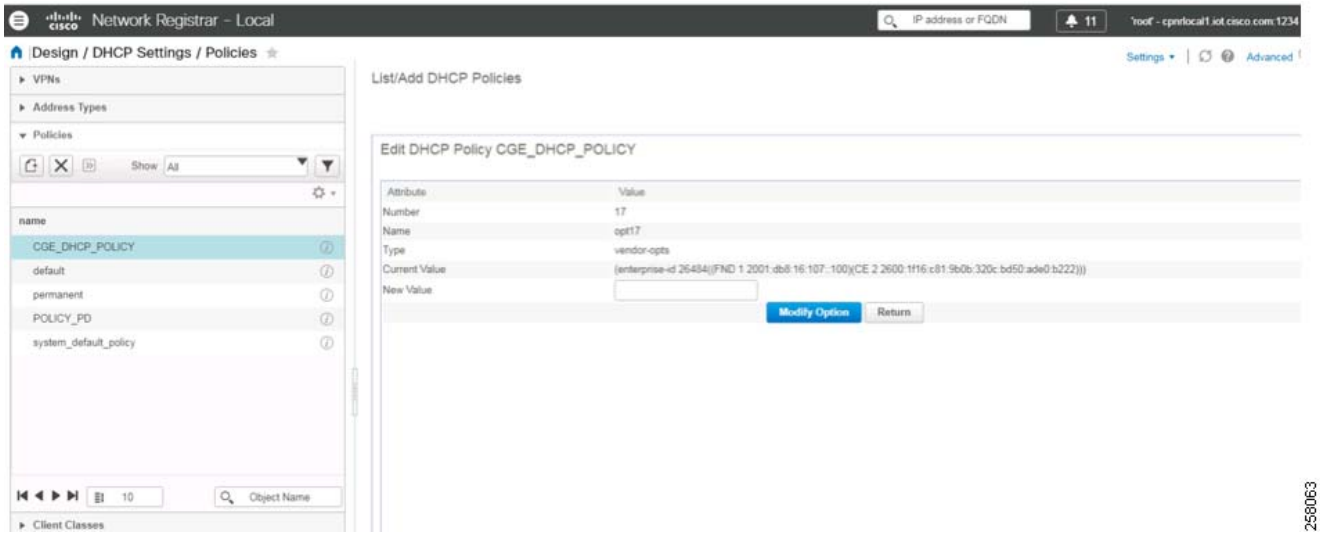
8. Choose **DHCPv6 Vendor Options** as **CGE_OptionDefinition** and **sub-option** as **opt17*[17] (vendor-opts)** and then click **Add Option**.

Figure 157 Configuring a New DHCP Policy



9. Click **opt17** to edit the option 17 settings and gives an option to edit the values. Enter the following values in the **New Value** field by clicking **Modify Values** and then click **Save**. In the **Values** field, enter: **(enterprise-id 26484 ((NMS 1 2001:abc::123) (Lightingale 2 ce-ipv6-address)))**.

Figure 158 Editing/Modifying DHCP Policy



10. Confirm that the **DHCPv6 Settings** on **CGE_DHCP_POLICY** are as shown in Figure 159:

Figure 159 Policy Values for CGE_DHCP_POLICY -1

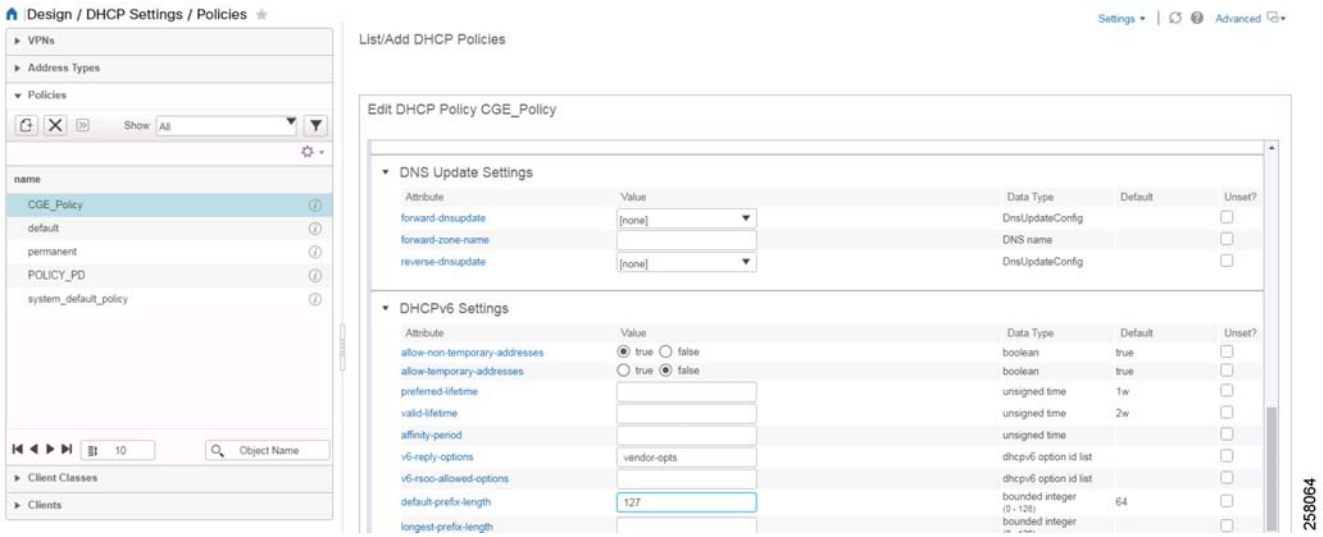
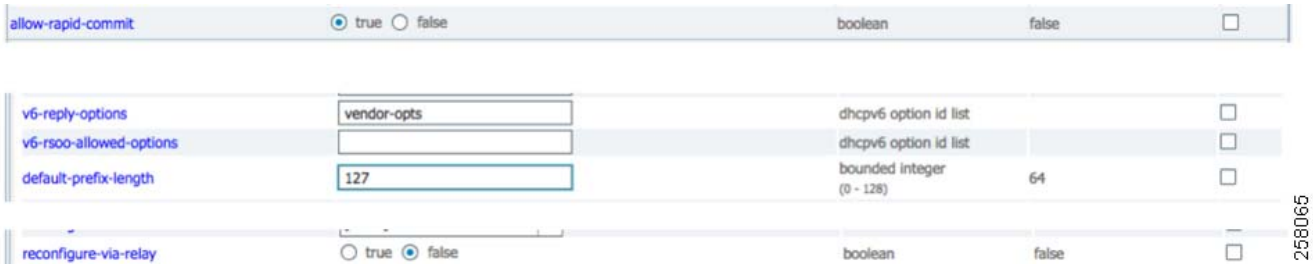


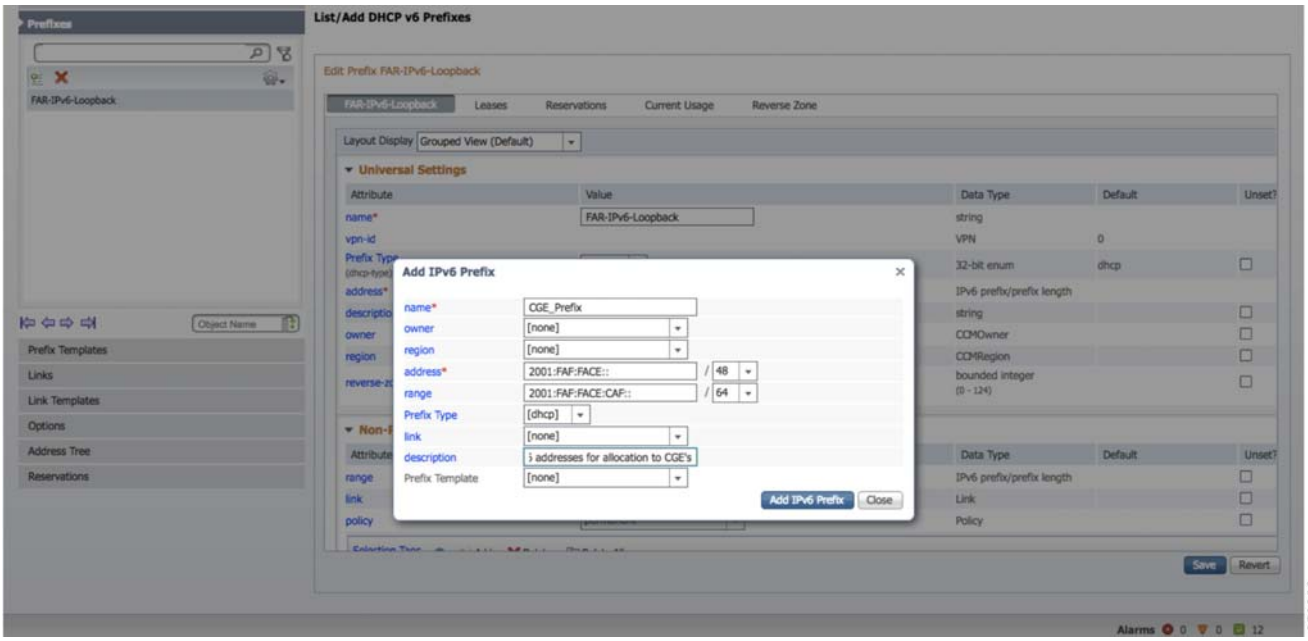
Figure 160 Policy Values for CGE_DHCP_POLICY-2



11. Click **Save** and the message **Saved Successfully** should display after completion.

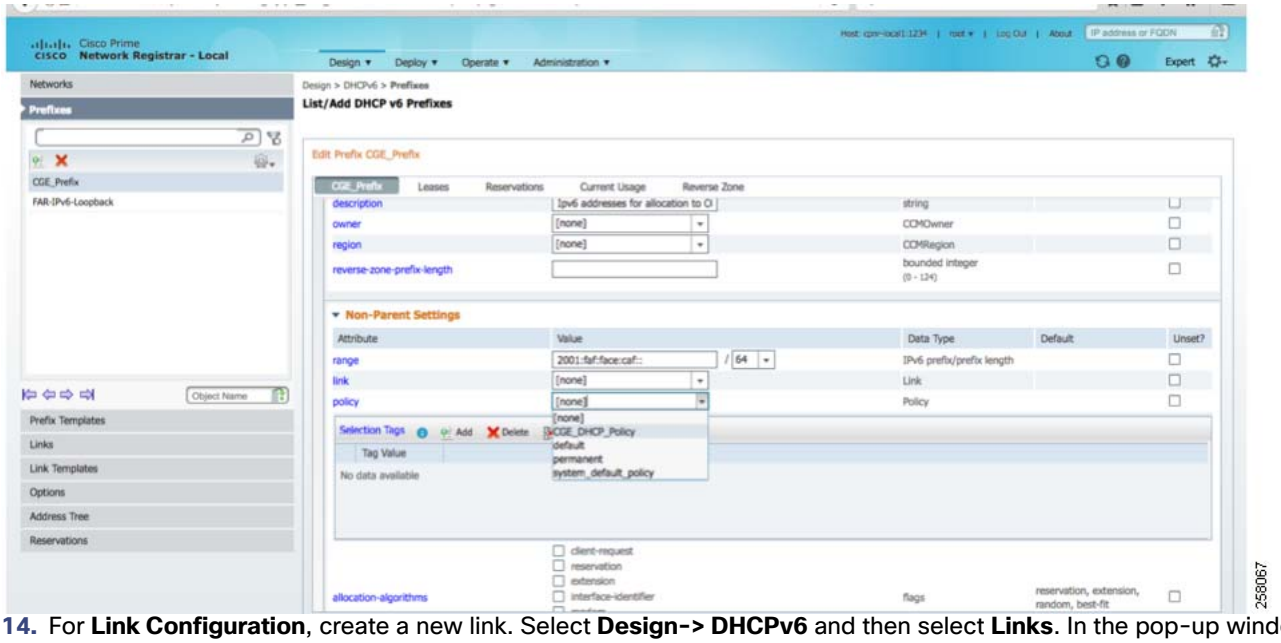
12. Click **Design-> DHCPv6** and select **Prefixes**. In the left panel, under **Prefixes**, create a new prefix by clicking the **'+'** icon. Enter **Name: CGE_Prefix** and address and range as desired and then select **Add IPv6 Prefix**.

Figure 161 Adding IPv6 CGE Prefixes



13. In the **Non-Parents Setting** tab, select **Policy** as **CGE_DHCP_Policy** and **Allocation-algorithms** as **interface-identifier**. Then click **Save**.

Figure 162 Selecting Policies for the Prefixes



14. For **Link Configuration**, create a new link. Select **Design-> DHCPv6** and then select **Links**. In the pop-up window, enter **Name** as **CGE_Link_Details** and the remainder of the values as default. Then select **Add Link**.

15. Under **Select Existing un-associated prefixes for this links**, click **Add**. Select the prefix configured above. Click **Add** in the **Available List** pop-up window.

16. Add prefix for prefix delegation: give address/range, select **dhcp type=prefix-delegation**. Click **Add prefix** and then click **Save**.

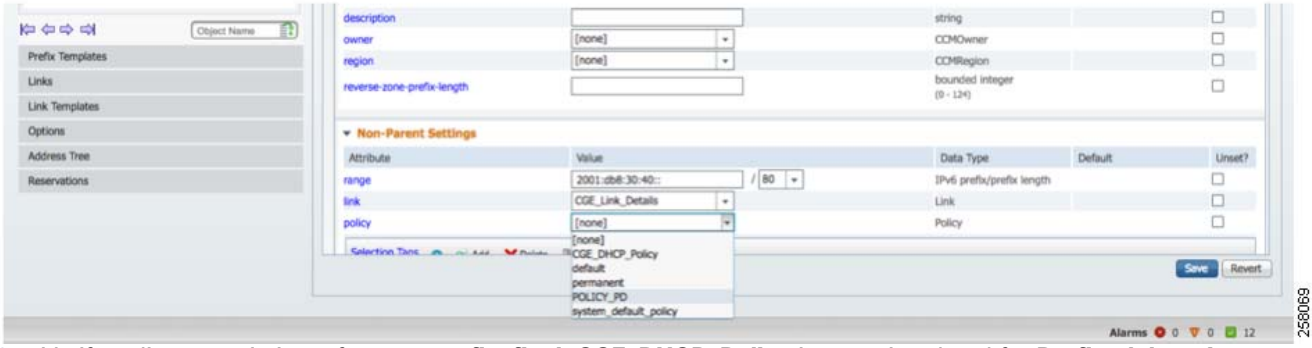
17. The user should now define and create a DHCP policy. From **Design-> DHCP Settings**, select **Policies**.

18. In **POLICY_PD**, select **DHCPv6 settings**. Select the following options:
    - Allow-non-temporary-addresses : **true**
    - Allow-temporary-addresses: **false**
    - preferred-life time: **10h**
    - min-valid-lifetime:**10h**
    - default-prefix-length:**128**
    - allow-rapid-commit: **true**
19. Click **Save**.

Figure 163 Settings for DHCPv6 Settings

20. Click policy defined for prefix delegation (**Design-> DHCPv6** and select **Prefixes**), in our case (**Prefix_Delegation1**), choose the **POLICY_PD** policy under Non-parent settings, and then click **Save**.

Figure 164 Prefixes for POLICY_PD



21. Verify policy associations: for **cge_prefix_final**, **CGE_DHCP_Policy** is associated and for **Prefix_delegation1**, **PD_POLICY** is associated
22. Restart the DHCP server to apply changes. From **Operate Servers-> Servers,** click **Manage Servers**. Then click the DHCP server and in the right corner, select **Restart Server**.

Secure Onboarding of Field Area Router—CGR1240

The Cisco Connected Grid Router (CGR) serves as a horizontal platform for various industrial services. It also provides services for street lighting applications and substation automation using data from intelligent electronic devices (IED). By providing features such as VLAN, VRF-Lite, QoS, the CGR1000 provides true multi-services to IoT industries.

The CGR 1240 Series acts as Field Area Router, which aggregates the traffic from CGEs and routes the traffic to HER via WAN. CGR forms a tunnel with HER to secure the data traffic flowing through it. The two WAN interfaces options are:

- CCI Horizontal Network

- Cellular Network

The CGR 1240 series router provides the network connection between Neighbor Area Network and WAN.

CGR Interface Configuration

CGR has the following types of interfaces:

- Ethernet Interface
- Loopback
- Wireless WPAN interface
- Cellular Interface (Remote POP will covered in Remote PoP with CR-Mesh over Cellular Network Backhaul, page 268.)

Role of Ethernet Interface

CGR, which acts as a Field Area Router, has the Uplink Ethernet Interface connected to the CCI Access Network, which in turn forms a secure tunnel to HER for communication.

Role of Loopback Interface

Using the field-facing interface, an overlay tunnel is established between the loopback interface of FAR and HER.

Role of Wireless WPAN Interface

WPAN interface is used to communicate with CGEs like IR510 and Street Light Controllers.

Pre-Staging a CGR

Pre-staging is the process in which the CGR is pre-configured with Certificates, tunnel-based configurations, CGNA and WSMA profiles, and EEM script-based configurations in the Customer Office Premises. The pre-staging steps are:

1. LAN Configuration
2. SCEP Enrollment of FAR
3. Secure Tunnel Establishment
4. FAR Registration into FND (NMS)
5. Final Configuration Push

LAN Configuration

For SCEP Enrollment, CGR is connected to the CA server for loading certificates. Before certificate enrollment, configure the LAN interface of the CGR to communicate with the CA server.

CGR Configuration for the HER-facing LAN Interface

```
*** FAR CONFIGURATION FACING CA SERVER***
!
interface GigabitEthernet2/2
 ip address a.b.c.d 255.255.255.0
 duplex auto
 speed auto
end
```

Note: The default gateway of the CA server is the CGR interface IP address.

SCEP Enrollment for FAR (CGR)

Simple Certificate Enrollment Protocol (SCEP)

A Cisco-developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly-used method for sending and receiving requests and certificates.

Certificate Enrollment

Certificate enrollment, which is the process of obtaining a certificate from a certification authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA.

Prerequisites for PKI Certificate Enrollment

Before configuring peers for certificate enrollment, you should have the following items:

- Domain Name configuration

```
!
!**Setting Domain Name**
no ip domain lookup
ip domain name iot.cisco.com
!
```

- An authenticated CA

  2016 Windows Server acts as Authority Server (Certificate Server) both in Auto Enrollment and Auto Approval.

- NTP Settings

  Enable NTP on the device so that the PKI services such as Auto Enrollment and certificate rollover may function correctly. (Device should be synchronized with CA server.)

```
!**NTP SERVER Settings (Configure NTP SERVER as HER INTERFACE) **
ntp update-calendar
ntp server x.x.x.x ' IP Address of NTP server.
```

Steps to Enroll CGR with the RSA CA Server

Complete the following steps:

1. Creation of a 2048-bit RSA key-pair named LDevID.
2. Definition of certificate authority details, trusted by the HER/CGR (that is, trustpoint definition):
   a. Enrollment profile (with Enrollment URL defined) to reach the certificate authority for certificate enrollment.
   b. Communication restricted only to the Authentic certificate authority, by performing a fingerprint check.
   c. Communications accepted only from the RSA CA server, which advertised SHA1 fingerprint/thumbprint matches with the configured fingerprint.
   d. The serial number to be part of the certificate.
   e. The IP address is NOT needed to be part of the certificate.
   f. No password is needed during certificate enrollment.
   g. The key pair created above in this section is used.
3. Receiving a copy of the RSA CA server's certificate (with public key).

4. Receiving the certificate of HER signed by RSA CA server:

   a. The signed certificate should contain the above details, which are configured under the trust point definition.

   Note: Ensure that no blank space exists after the password in the Trustpoint configuration.

```
!***********Creating 2048-bit length RSA key-pair, named as 'LDevID'**********
crypto key generate rsa label LDevID modulus 2048
!
!
!***********URL to reach the RSA CA server's SCEP Enrollment service.********
crypto pki profile enrollment LDevID
enrollment url http://rsaca.iot.cisco.com/certsrv/mscep/mscep.dll
!
!
!************Trust point configuration for RSA CA server*************
crypto pki trustpoint LDevID
enrollment retry count 4
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
serial-number none
fqdn none
ip-address none
password
fingerprint 1AC17D88EB11A6F7AADBAenjwkmA94A80C25DA8DCFD ' Fingerprint of RSA CA server
subject-name serialNumber=PID:CGR1240/K9 SN:FTX123456B,CN=CGR1240_FTX123456B
revocation-check none
rsakeypair LDevID 2048
!
!
!*************To Receive a copy of the RSA CA server's certificate (with public key of CA)********
crypto pki authenticate LDevID
!
!
!*************To receive the CGR's certificate signed by the RSA CA server.************
crypto pki enroll LDevID
!
!
!
```

Configuration Commands

```
CGR1240_FTX123456B(config)#crypto pki authenticate LDevID
Certificate has the following attributes:
Fingerprint MD5: 32ED3589 E7F3EE8D 7583B15E 3AEC029B
Fingerprint SHA1: 1AC17D88 EB11A6F7 AADBAA24 A94A80C2 5DA8DCFD
Trustpoint Fingerprint: 1AC17D88 EB11A6F7 AADBAA24 A94A80C2 5DA8DCFD
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
CGR1240_FTX123456B(config)#crypto pki enroll LDevID
%
% Start certificate enrollment ..
% The subject name in the certificate will include: serialNumber=PID:CGR1240/K9
SN:FTX123456B,CN=CGR1240_FTX123456B
% The fully-qualified domain name will not be included in the certificate
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose LDevID' command will show the fingerprint.
CGR1240_FTX123456B(config)#!
May 28 09:00:31.349: CRYPTO_PKI: Certificate Request Fingerprint MD5: 3F0DF40E 268BEB5D 6E91BAA6
4F17F19D
May 28 09:00:31.351: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 5729E78A FB0E1F29 3ABB044A
869C2151 A11BE1D6
May 28 09:00:43.605: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

Verifying the Certificate Enrollment Status of CGR

```
CGR1240_FTX123456B#show crypto pki trustpoints LDevID status
Trustpoint LDevID:
Issuing CA certificate configured:
Subject Name:
cn=IOT-RSA-ROOT-CA,dc=iot,dc=cisco,dc=com
Fingerprint MD5: 32ED3589 E7F3EE8D 7583B15E 3AEC029B
Fingerprint SHA1: 1AC17D88 EB11A6F7 AADBAA24 A94A80C2 5DA8DCFD
Router General Purpose certificate configured:
Subject Name:
cn=CGR1240_FTX123456B,serialNumber=PID:CGR1240/K9 SN:FTX123456B
Fingerprint MD5: E6435DDE A50A0CE1 215D9387 8D911266
Fingerprint SHA1: 1002FB2F 7BC1B1F0 3FB00BCD 8264B7DB 1887AE57
Last enrollment status: Granted
State:
Keys generated ..... Yes (General Purpose, non-exportable)
Issuing CA authenticated ..... Yes   #Received CA Servers Certificate .
Certificate request(s) ..... Yes # Received certificate for HER.
```

Note: The enrollment URL differs according to the type of RSA CA server:

a. For the Windows CA server, the URL path is http://rsaca.iot.cisco.com/certsrv/mscep/mscep.dll.

b. The fingerprint should be extracted from the RSA CA Server's certificate. Subject Name contents will be appearing on certificates.

c. Secure tunnel establishment between HER and FAR.

Secure Tunnel Establishment

CGR Configuration

This section shows the configurations that have to be executed on the Cisco CGR to establish a tunnel with the HER. The security configurations are the same as the HER security configurations. If a mismatch exists between the configurations on the HER or CGR, then the tunnel between them is not established.

```
!
aaa authorization network FlexVPN_Author local
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
!

crypto ikev2 proposal FlexVPN_IKEv2_Proposal_Cert
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_Cert
 proposal FlexVPN_IKEv2_Proposal_Cert
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile_Cert
 match identity remote fqdn CCI-HER-1.iot.cisco.com
 identity local fqdn CGR1240_FTX123456B.iot.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
```

```
 dpd 120 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 client flexvpn FlexVPN_Client
  peer 1 x.x.x.x > IP Address of HER facing CGR
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_Cert esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile_Cer
 set transform-set FlexVPN_IPsec_Transform_Set_Cert
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile_Cert
!

interface Loopback100
 ip address 192.168.200.10 255.255.255.0
 ipv6 address 2001:DB8:BABA:FACE::1/64
!
interface Tunnel100
 description IPsec tunnel CGR-1 to HER-1
 ip unnumbered Loopback100
 ipv6 unnumbered Loopback100
 ipv6 enable
tunnel source GigabitEthernet2/2
 tunnel destination x.x.x.x > IP Address of HER
 tunnel protection ipsec profile FlexVPN_IPsec_Profile_Cer
!
```

Selective Route Advertisement from FAR to HER

FAR advertises routes of IPv6 CGEs to HER by advertising specific prefixes through IKEv2 prefix injection:

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
!
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 permit ipv6 2001:BEED::/64 any
!
```

FAR Registration into FND (NMS)

To monitor CGR using FND, CGR first needs to register with FND. CGR registration steps are shown below:

Note: cg-nms.odm should be the latest; otherwise CGR registration fails.

Verify the Reachability from CGR to FND

The IPv4 reachability of the CGR connecting to FND is reachable.

Add FAR Details in FND

This action needs to be performed in the FND. The list of the FARs that need to go through registration must have an entry added in FND. The following section captures the csv method for adding an entry for the FAR in the FND. Details about one or more FARs can be captured in a csv file and can be imported into the FND in one go.

Contents of FAR.csv

The first row of the csv would have the ordered list of the device properties (comma separated). Each subsequent row will represent a FAR, which is an ordered list of commas separated values corresponding to the ordered list of device properties in the first row.

The following is sample content showing the sample structure of a csv file:

```
Field1,Field2,field3,field4,field5 o Ordered list of device properties
FAR_01,valueA,valueB,valueC,valued o Ordered list of values corresponding to above list
FAR_02,valueW,valueX,valueY,valueZ
```

Note: Do not leave any extra spaces before/after comma while creating the csv file.

```
Eid,deviceType,adminUsername,adminPassword,ip
CGR1240/K9+FTX123456B,cgr1000,cg-nms-administra-tor,ehHIoP1EdepSsY6HMQsOIa8/oZ52+8LVeYX9+gNTkAxKRzF
RFgvdOrJBj0OUge5bA5gXaR6cIB2ehQ23aFqfJ5D3O2wCk6NGV4Ed1UfOClBxFYsZdsrPFK+b+8AncmXc0EndBD3alXQfr131g5
cnlKoR2dhxB60ssT2mi7MnKAgAPGYq+QL+WUJretNLrCcFnWJuvNmRiSlDFALQfv00l1ssxvLVSGpWOMcm9ciAEBhBaFdyWxXep
qWr0noTMMqrKlJzNanE+pN0GhaQFofZOPgFFy2dXp1W/zsxv2TWbgJtbemKYe9fn5OXiErMBGltkhQrod5+ZCtG0UDWSdObvA==
,10.20.100.39
```

Table 22 CGR CSV Details

Parameter Name	Parameter Value	Explanation
eid	CGR1240/K9+FTX123456B	Unique network element identifier for the device
deviceType	cgr1000	Helps identify the type of device. Few examples of device type: ir800, cgr1000
adminUsername	cg-nms-administrator	Username that FND must use to interact with FAR
adminPassword	Encrypted password derived from Generating the Encrypted Password, page 215 is mentioned below.	Password in encrypted form. Unencrypted form of this password would be used by FND to interact with FAR.
Ip	Interface IP of the CGR	IP Address using which FND will try to reach CGR

Generating the Encrypted Password

Log in to the FND via SSH and perform the following steps to get the encrypted password that needs to be populated into the FAR.csv file.

```
[root@fnd conf]# pwd
/opt/cgms/server/cgms/conf
[root@fnd conf]# echo "CgnmsA@123" > /tmp/pwd
[root@fnd conf]#
[root@fnd conf]# /opt/cgms-tools/bin/signature-tool encrypt cgms_keystore /tmp/pwd
Enter alias: cgms
Enter password: Enter the keystore password used to protect FND.
156qay3OnltOPVTmrDhwVZ426ZyewiRG1gmshsem/I0MP+dPGrDNO1Al7FuvyMZrkcLTd3+L9QSyc5SZo1BeS/GZ9T337cf+HVh
F36G0ORerMcg7N5Vh77RH18Fg/SctLRta0gBD4PdcdJeQI0R5UVQpoU3dlPtefCZ4LAOh4gitQJ72avXzygsofG17CPk4ZDdc9c
Q9jrpV2fzpzS/Wyv2ryzIkKVMUYDCr9fLBITPtWUwCuX/bylZHaHvBnsq5ZwTC3uaSTzd2LDXvk+iRtynjLXJRcWdaRqnIGVCDp
0C8l3du3fxHInJ69jjob924tIH3YjZ101D6gt4VxKdtCA==
[root@fnd conf]#
[root@fnd conf]# rm /tmp/pwd
rm: remove regular file '/tmp/pwd'? y
[root@fnd conf]#
```

Note: For security reasons, it is recommended to have unique passwords for each FAR.

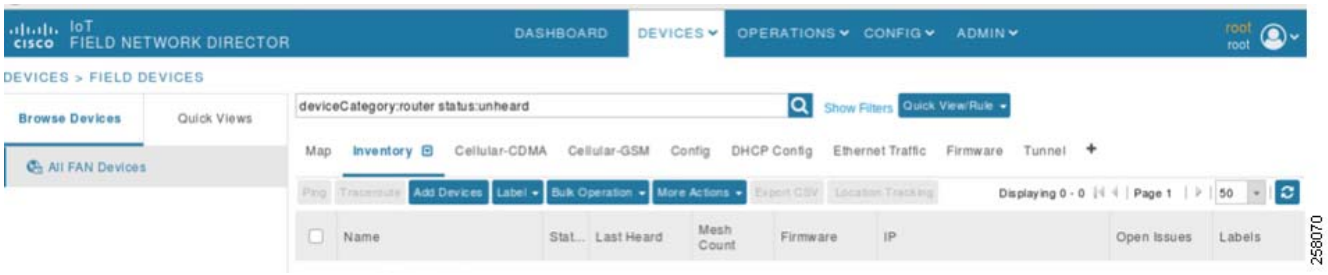
In the above snippet, the password that should be used for accessing the FAR is stored in a temporary file named **/tmp/pwd**. The signature tool is then run to encrypt the password stored in the file **/tmp/pwd** with the key (with alias cgms) stored in the **cgms_keystore**. Finally, remove the password file **/tmp/pwd** for security reasons.

Importing FAR.csv into FND

This section describes the steps for importing the FAR.csv into the FND.

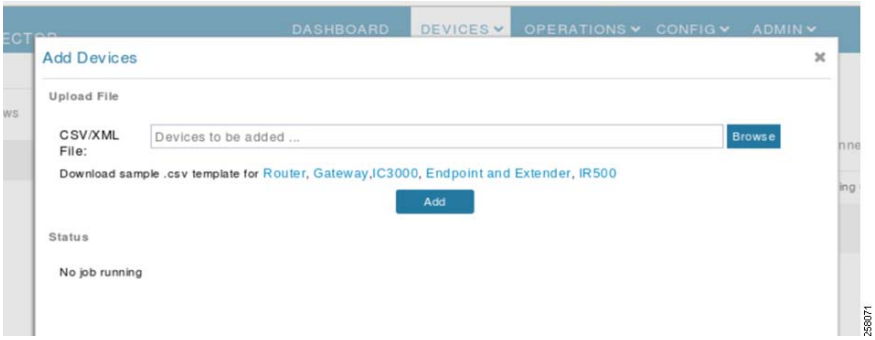
1. From **Devices**, choose **Field Devices**, select **Inventory**, and in the drop-down list, select **Add Devices**.

Figure 165 Importing FAR into FND



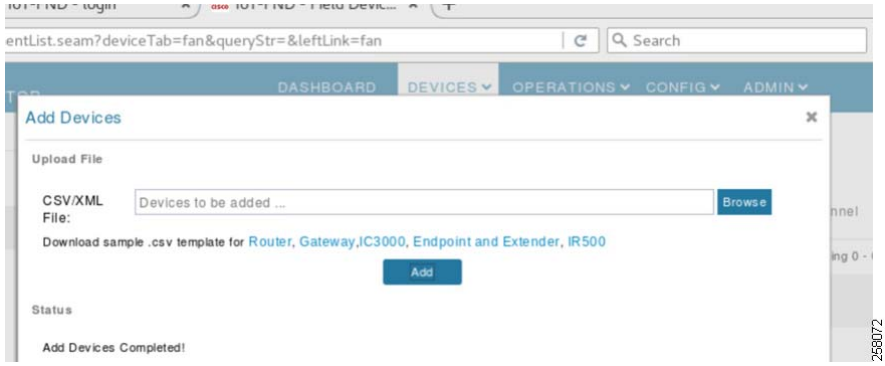
2. Choose the **FAR.csv** file and then click **Add**.

Figure 166 Insert FAR csv into FND



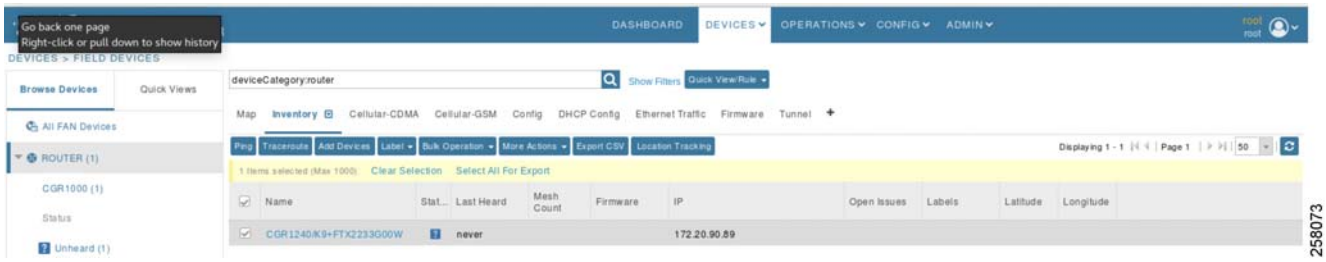
3. The FND performs a validation of the FAR.csv file and successful validation results in importing FAR details into the FND. If any failures exist, click the number under the column **Failure#** corresponding to the latest import attempt; this opens a window that displays the failures encountered.

Figure 167 Successful Addition of CGR into FND



4. After FAR.csv import, the status must be successful before proceeding further. After successful import of the FAR, the device would be in an unheard state. Click the FAR PID to verify device/config properties of the FAR imported into the FND.

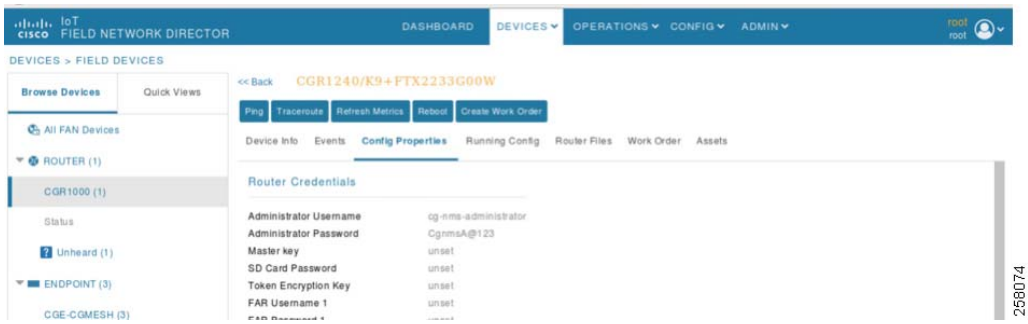
Figure 168 Dashboard Displaying CGR after Upload



Verify FAR Properties at FND

5. After importing the FAR.csv into the FND, navigate to the **Config Properties** section of the corresponding FAR and verify the accuracy of the device parameters.

Figure 169 FND UI Displaying Properties of CGR



Config Provisioning Settings on FND

6. To communicate CGR with FND, user should provide FND URL and the same should match with CGR CGNA configuration.

Figure 170 Configuration of FND Provisional Settings to Communicate with CGR

Final Configuration Push from FND to CGR

In CGR, WPAN configuration along with dot1x, AAA and mesh security will be configured from FND after CGR is successfully registered. This section describes the steps to push the configuration from FND to CGR after registration.

1. From the FND UI, select the **Config** drop-down list in the top panel and then select **Device Configuration**.
2. Select the **Router** option from the left panel and then select the group in which the user needs to apply configuration after CGR registration.
3. Go to the **Edit Configuration Template** tab, remove the default template, and insert the WPAN configuration. For WPAN configuration, please refer to Sample Cisco Resilient Mesh Security Configuration, page 226.
4. Enrollment configuration of CGR.

To enroll CGR into FND, the following configuration for AAA, HTTP, CGNA Profiles, and WSMA needs to be configured into CGR:

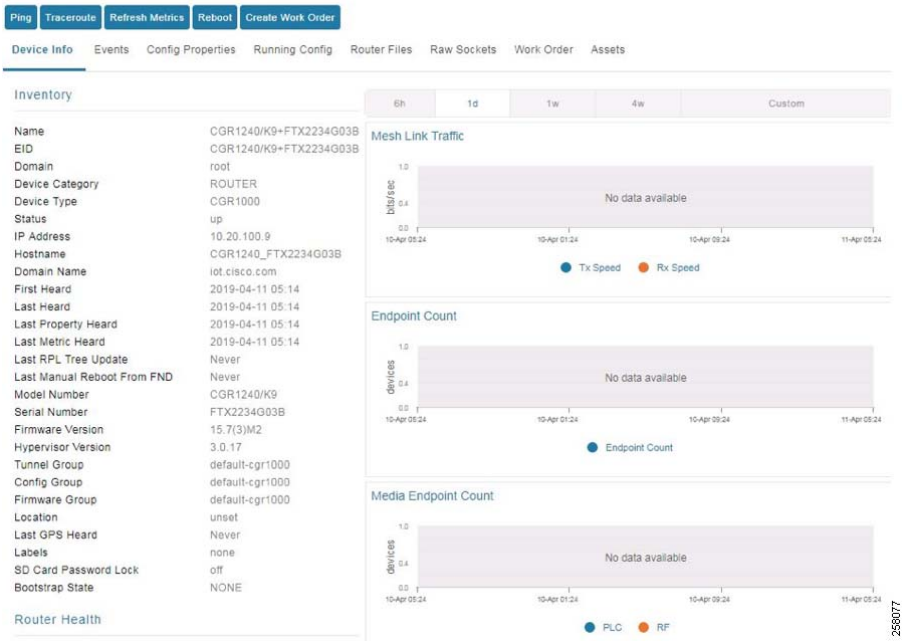
```
!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
username cg-nms-administrator privilege 15 algorithm-type sha256 secret (password)
!
ip host fnd.iot.cisco.com 172.16.107.100
!
mkdir flash:archive
!
!
archive
 path flash:/archive
 maximum 8
!
!
no ip http server
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha dhe-aes-cbc-sha2
ip http secure-client-auth
ip http secure-port 8443
ip http secure-trustpoint LDevID
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface GigabitEthernet2/2
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
dhe-aes-cbc-sha2
!
no iox hdm-enable
iox client enable interface GigabitEthernet2/2
!
wsma agent exec
 profile exec_profile
!
wsma agent config
 profile config_profile
!
!
wsma profile listener exec_profile
 transport https path /wsma/exec
!
wsma profile listener config_profile
 transport https path /wsma/config
!
cgna gzip
!
cgna heart-beat interval 15
cgna heart-beat active
!
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show platform gps location | format flash:/managed/odm/cg-nms.odm
 add-command show platform hypervisor | format flash:/managed/odm/cg-nms.odm
 add-command show sd-card password status | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
```

```
 add-command show iox host list detail | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https:// cci-fnd-oracle.cimconccibgl.cisco.com:9121/cgna/ios/registration
 gzip
 active
!
cgna profile cg-nms-tunnel
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
!
event manager policy no_config_replace.tcl type system authorization bypass
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_Enabled TRUE
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager directory user policy "flash:/eem"
event manager policy tm_ztd_scep.tcl type system authorization bypass
!
end
```

After CGR is on-boarded, the user can see the configuration parameters in FND. In the FND Dashboard, the user is able to see CGR status.

Figure 171 CGR Successful On-boarding

Figure 172 CGR Properties after Successful On-board



Verification on FAR for Successful Registration with FND

The following CGNA profiles can be used to verify on the FAR:

1. Profile Name: **cg-nms-register**:
   a. Observe that the profile is disabled.
   b. With a successful last response.
2. Profile Name: **cg-nms-periodic**:
   a. Observe that the profile is Active, waiting on timer for next action.
   b. With a successful last response.

```
CGR140_FTX13456#show cgna profile-state all
Profile 1:
Profile Name: cg-nms-register
Deactivated at: Thu Aug 15 07:20:35 2019
URL: https://cci-fnd-oracle.cimconccibgl.cisco.com:9121/cgna/ios/registration
Payload content type: xml
Interval: 10 minutes
Transfer count: 85
gzip: activated
Profile command:
    show hosts | format flash:/managed/odm/cg-nms.odm
    show interfaces | format flash:/managed/odm/cg-nms.odm
    show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    show ipv6 interface | format flash:/managed/odm/cg-nms.odm
```

```
    show platform gps location | format flash:/managed/odm/cg-nms.odm
    show platform hypervisor | format flash:/managed/odm/cg-nms.odm
    show sd-card password status | format flash:/managed/odm/cg-nms.odm
    show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
    show iox host list detail | format flash:/managed/odm/cg-nms.odm
    show version | format flash:/managed/odm/cg-nms.odm
State: Profile disabled
Timer stopped at Thu Aug 15 07:20:35 2019
Last successful response at Thu Aug 15 07:20:21 2019
Last failed response at Thu Aug 15 07:10:19 2019

Profile 2:
Profile Name: cg-nms-periodic
Activated at: Thu Aug 15 07:20:31 2019
URL: https://cci-fnd-oracle.cimconccibgl.cisco.com:9121/cgna/ios/metrics
Payload content type: xml
Interval: 60 minutes
Transfer count: 166
gzip: activated
Profile command:
    show version | format flash:/managed/odm/cg-nms.odm
    show environment temperature | format flash:/managed/odm/cg-nms.odm
    show hosts | format flash:/managed/odm/cg-nms.odm
    show interfaces | format flash:/managed/odm/cg-nms.odm
    show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
    show platform hypervisor | format flash:/managed/odm/cg-nms.odm
    show sd-card password status | format flash:/managed/odm/cg-nms.odm
    show platform gps location | format flash:/managed/odm/cg-nms.odm
    show raw-socket tcp sessions | format flash:/managed/odm/cg-nms.odm
    show raw-socket tcp statistics | format flash:/managed/odm/cg-nms.odm
    show iox host list detail | format flash:/managed/odm/cg-nms.odm
    show cellular 3/1 all | format flash:/managed/odm/cg-nms.odm
State: Wait for timer for next action
Timer started at Thu Aug 22 05:22:37 2019
Next update will be sent in 3 minutes 19 seconds
Last successful response at Thu Aug 22 05:22:39 2019
Last failed response not found
```

Upgrade of CGR from FND

Management of CGRs like device maintenance, monitoring, and operations can be performed by FND. In this section, we will see CGR being upgraded using FND. The CGR upgrade has the following steps:

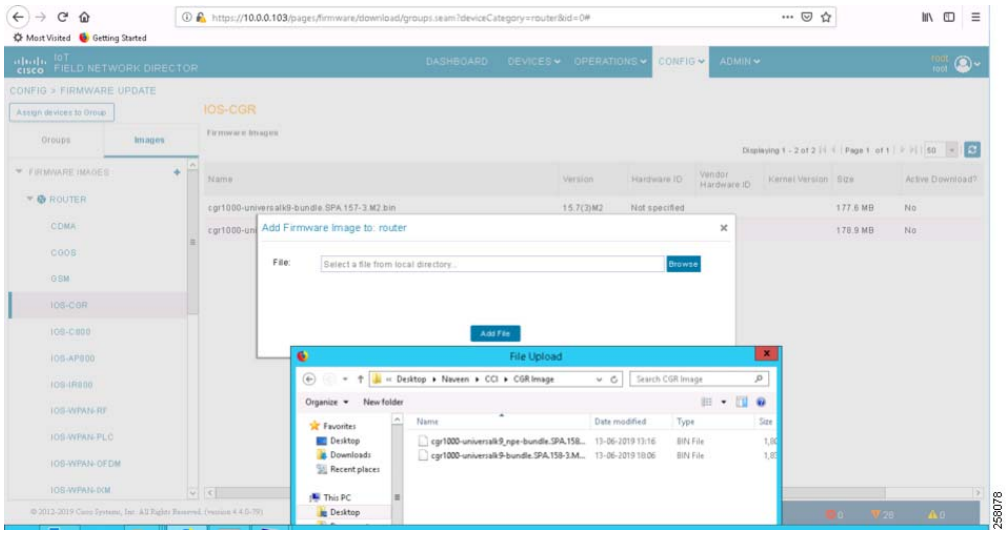
a. Image loaded into FND Firmware Images.

b. Upload the image into CGR.

c. Install Image and reload the Device.

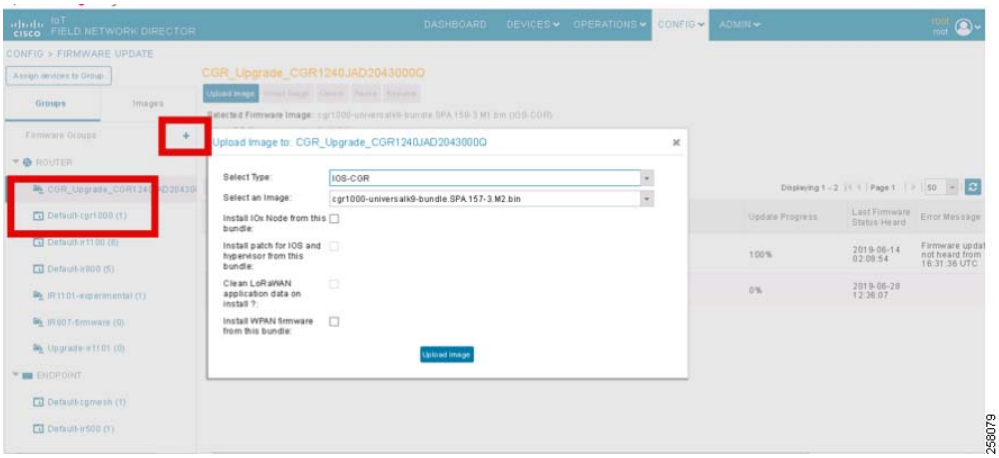
1. Go to **FND UI** and on the top right, select the **CONFIG** drop-down list and then select **Firmware Update**.
2. Go to **Images**, select **IOS-CGR**, select **+**. In the pop-up window, select **CGR image** and then select **Add File**.

Figure 173 CGR Image Upload into FND



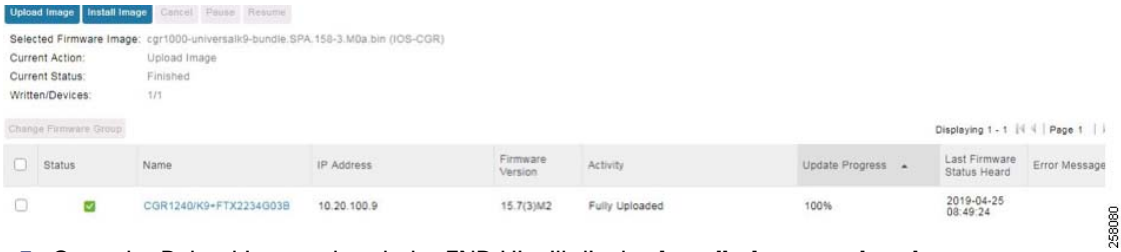
3. After uploading the image in **Firmware Images**, select **Groups** where you can create groups by selecting **Assign devices to group**. Select the group and then select upload image; it will upload the image to CGR group members.

Figure 174 Creation of Groups and Upload of Image into Device



4. Once upload is completed, click **Install Image** to install the image on the router. It will take some time to install the latest image on the router.

Figure 175 Completion of Image Upload in FND



5. Once the Reload is completed, the FND UI will display **Installation completed**.

Figure 176 Image Upgrade Completion

Dot1x Authenticator Configuration on FAR for CGE

The CGE communication module performs secure 802.1x network join through neighboring CG-Endpoints or FAR, validating authentication to the AAA RADIUS server in the data center. CGR serves as the authenticator and communicates with a standard AAA server using RADIUS. CGE uses a stateless EAP proxy that forwards EAP messages between the CGR and a joining interface because the joining interface might be multiple mesh hops away from the CGR. The MTU setting on the AAA server must be set to 800 bytes or lower, because IEEE802.1x implementation in CGEs limits the MTU to 800 bytes. RADIUS servers can use auth-port 1812 and acct-port 1813.

```
aaa new-model
!
!
aaa group server radius nps-group
 server name nps-radius
!
aaa authentication login default local
aaa authentication dot1x default group nps-group
<...snip...>
dot1x system-auth-control
!
<...snip...>
!
!
radius server nps-radius
address ipv4 <IP address> auth-port 1812 acct-port 1813
key <RADIUS key>
!
```

Implementing CR-Mesh Access Network

Cisco supports Radio Frequency (RF) mesh communication technology in the CGE space for the last mile connectivity. A Cisco CGE needs to implement RF protocol stacks and needs to be appropriately configured to be able to join and communicate with a Neighborhood Area Network (NAN) rooted at a Cisco's Connected Grid Router (CGR) 1000 series.

A CGE connected to a NAN/CG mesh (RF) must be capable of end-to-end Layer 3 communication using IPv6. When a CGE attempts to join a CR-Mesh network, it must authenticate itself to the network, obtain link layer security credentials, join the RPL routing domain, obtain an IPv6 address along with options and prefix delegation if required, register itself to network management services (FND) using CoAP Simple Management Protocol (CSMP), and communicate with required application servers (LightingGale Application) to deliver grid functionalities.

As we know, the CGR 1000 series acts as a Field Area Router (FAR). Each FAR advertises a unique Personal Area Network (PAN), which is recognized by a combination of a SSID and PAN ID. CGEs are programmed to join a PAN with a given SSID. CGEs can migrate between PANs based on a set of metrics for the PAN (very rarely) and for fault tolerance.

CR-Mesh is embedded in CGEs using IP Layer 3 mesh networking technology that performs end-to-end IPv6 networking functions on the communication module. CGEs support an IEEE 802.15.4e/g interface and standards-based IPv6 communication stack, including security and network management.

CR-Mesh supports a frequency-hopping radio link, network discovery, link-layer network access control, network-layer auto configuration, IPv6 routing and forwarding, firmware upgrade, and power outage notification. The CGR runs the IPv6 Routing Protocol over Low Power and Lossy Networks, also known as RPL. The IPv6 Layer-3 RPL protocol is used to build the mesh network.

The installation of WPAN with CGR1240 can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/modules/wpan_cgmesh/b_wpan_cgmesh_IOS_cfg.html

Note: The CGR1000 router must be running Cisco IOS Release 15.8(3)M0a (cgr1000-universalk9-bundle.SPA.158-3.M0a.bin) or greater to support the CGM WPAN-OFDM Module. Cisco WPAN version must be 5.7.27.

Configuring Cisco Resilient Mesh and the WPAN Module

This section of the document covers only the WPAN configuration of Cisco CGR WPAN module. Before deployment in the field, pre-staging configurations are done on CGE. The pre-staging configurations are provided by the operator and the CGE provider configures the same on the CGE device during the manufacturing process.

The pre-staging configurations include CGE certificate with private key, CSMP certificate, ECC CA Root Certificate, and XML config file. Apart from several other configurations, the XML config includes SSID and Phy mode.

All configurations and management of CGR WPAN are done by IoT FND using Cisco IOS commands (Release 15.4(2)CG and greater).

At the CGR 1000, configure the WPAN Module interface as follows:

```
cgr1000_wpanmodule# config terminal
cgr1000_wpanmodule(config)# interface wpan   <slot |port >
cgr1000_wpanmodule(config-if)#
```

Note: If an user is inserted in slot 5, it will be 5/1 (slot numbers are visible inside CGR.

Enabling Dot1x, Mesh-security, and DHCPv6

User must enable the dot1x (802.1X), mesh-security, and DHCPv6 features to configure the WPAN interface. To enable these features, use the following command:

```
cgr1000_wpanmodule(config)# dot1x system-auth-control
This command should be enable in Global configuration mode.
```

For dot1x, the WPAN interface configuration requires:

```
cgr1000_wpanmodule(config)# interface wpan   <slot |port >
cgr1000_wpanmodule(config-if)# dot1x pae authenticator
```

Naming Your PAN

To configure the name of your IEEE 802.15.4 Personal Area Network Identifier (PAN ID), use the following WPAN command:

```
cgr1000_wpanmodule(config-if)# ieee154 panid 2400
Pan ID value can vary from 0 to 65535
```

Naming the SSID

The Service Set Identifier (SSID) should be consistent across the CGR WPAN interface and CGE's.

To configure the name of the SSID, use the SSID command ieee154 ssid <ssid_name >, for example:

```
cgr1000_wpanmodule(config)# interface wpan   5/1
cgr1000_wpanmodule(config-if)#ieee154 ssid myWPANssid
  SSID string can be a word up to max size of 32.
```

Configuring Transmit Power

The txpower in the configuration specifies the txpower setting in the physical hardware (chip). However, the radio signal out of the hardware chip must travel through the amplifier, front end, antenna, etc. that causes the output power of the chip to be less than the actual electro-magnetic signal that is emitted into the air. Values range from 2 (high) to the default value of -34 dBm (low-Lab Testing).

To configure the transmit power for outdoor usage, specify a higher transmit power, such as:

```
cgr1000_wpanmodule(config-if )# ieee154 txpower 30
The value can be vary from -64 to 64 and the default is -34.
```

Naming the Notch

A notch is a list of disabled channels from the 902-to-928 MHz range. If no notch exists at all, then all channels are enabled. if there is a notch [x, y], then channels between x and y are disabled:

```
cgr1000_wpanmodule(config-if)#ieee154 notch 10-15, 30-35
```

Configuring Phy-mode

CLI interface commands defines CGR phy-mode. In our case, we are using only PHY-mode 98:

```
cgr1000_wpanmodule(config-if)# ieee154 phy-mode
 98: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400     kHz
```

Setting the Minimum Version Increment

To set the minimum time between RPL version increments, use the *version-incr-time* command:

```
cgr1000_wpanmodule(config-if)# rpl version-incr-time
```

Setting the DODAG Lifetime Duration

To set the Destination-Oriented Directed Acyclic Graph (DODAG) lifetime duration, use the *DAG lifetime* command. Each node uses the lifetime duration parameter to drive its own operation (such as Destination Advertisement Object or DAO transmission interval). Also, the CGR uses this lifetime value as the timeout duration for each RPL routing entry:

```
cgr1000_wpanmodule(config-if)# rpl dag-lifetime 60
Enter a value between 15 and 255 seconds. Default is 120.
```

Configuring the DODAG Information Object Parameter

To configure the DODAG Information Object (DIO) parameter per the RPL IETF specification, use the *rpl dio-min* command:

```
cgr1000_wpanmodule(config-if)# rpl dio-dbl 5
```

To set the DIO double parameter as per the RPL IETF specification, use the *dio-dbl* command. DIO double is a doubling factor parameter used by the RPL protocol:

```
cgr1000_wpanmodule(config-if)# rpl dio-min 16
```

Configuring IPv6

To determine the available IPv6 functions, query the ipv6 commands. To enable IPv6 on an interface, use:

```
cgr1000_wpanmodule(config-if)# ipv6 enable
cgr1000_wpanmodule(config-if)# ipv6 address 2001:BEED::1/64
```

Configuring IPv6 DHCP Relay

IPv6 addresses lease for end nodes will be managed by CPNR (centralized DHCP Server). To configure the IPv6 DHCP relay, use the ipv6 dhcp relay command:

```
cgr1000_wpanmodule(config-if)# ipv6 dhcp relay destination 001:DB8:16:108::100
```

Configuring the Power Outage Server

User can configure the power outage server with the outage server command. We recommend an IPv6 address or IPv6 resolvable FQDN of a server. In most cases, the outage server is your IoT FND server:

```
cgr1000_wpanmodule(config-if)# outage server 2001:DB8:16:110::100
```

Configuring Cisco Resilient Mesh Security

CGEs use the IEEE 802.1X protocol, known as Extensible Authentication Protocol over LAN (EAPOL), for authentication.

Configuring Mesh Key

To set the mesh key, use the *mesh-security set mesh-key* command in privileged mode:

```
cgr1000_wpanmodule # mesh-security set mesh-key interface wpan 5/1 key 1234567891234567 < --# Your
secret key.
cgr1000_wpanmodule (config-if)# mesh-security mesh-key lifetime 60
```

Note: Mesh-security config and keys do not appear in the CGR configuration as shown by *show running-config* or *show startup-config*.

Sample Cisco Resilient Mesh Security Configuration

The following example shows what is required for CGR WPAN, dot1x and mesh-security:

```
!
aaa new-model
!
mesh-security set mesh-key interface wpan 5/1 key 1234567891234567!
! Creation of Radius server group ios-aaa
aaa group server radius ios-aaa
 server name PHE_AAA_NPS
!
!
aaa authentication login default local
aaa authentication dot1x default group iok-aaa
<...snip...>
dot1x system-auth-control
!
<...snip...>
!
interface Wpan5/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 load-interval 30
 ieee154 beacon-async min-interval 20 max-interval 120 suppression-coefficient 0
 ieee154 panid 2400
 ieee154 ssid ccilightnode
 ieee154 txpower 11
 outage-server 2001:DB8:16:110::100<< Outage server is FND.
 rpl dag-lifetime 60
 rpl dio-dbl 5
 rpl dio-min 16
 rpl version-incr-time 120
 authentication host-mode multi-auth
 authentication port-control auto
```

```
 ipv6 address 2001:BEED::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:db8:16:108::1 << IPv6 address of CPNR
 dot1x pae authenticator
mesh-security mesh-key lifetime 259200
end
!
!Radius server details
! The IP address mentioned below is the IP address of NPS server(In our case !the NPS server is
same as ECC server)
!Radius key must be same for NPS server and below
radius server PHE_AAA_NPS
 address ipv4 172.17.100.11 auth-port 1812 acct-port 1813
 key <<Radius Key>>
!
```

Onboarding CGE in FND

FND-CGE Addition

This action needs to be performed in the FND. The following section captures the csv method for adding an entry for the CGE in the FND. Just like CGR, the same kind of CSV needs to be uploaded in FND to on-board CGEs.

The following is sample content showing the sample structure of a csv file:

```
Field1,Field2,field3,field4,field5 o Ordered list of device properties
FAR_01,valueA,valueB,valueC,valued o Ordered list of values corresponding to above list
FAR_02,valueW,valueX,valueY,valueZ
```

Note: Do not leave any extra spaces before/after comma while creating the csv file.

```
eid,deviceType,function
00173B14004A003F,cgmesh,meter
```

Table 23 CG-Mesh Node CSV Details

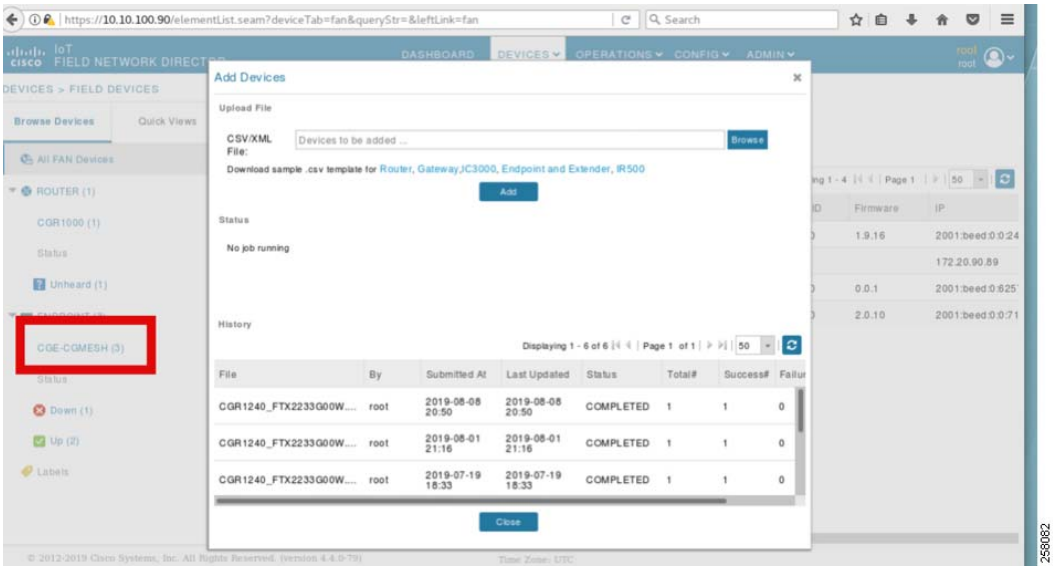
Parameter Name	Parameter Value	Explanation
eid	00173B14004A003F	Unique network element identifier for the device
deviceType	cgmesh	Helps identify the type of device. Few examples of device type: ir800, cgr1000, cgmesh
function	meter	Function of the Endpoint Node

Importing CR-Mesh.csv into FND

This section describes the steps for importing the CR-Mesh.csv into the FND:

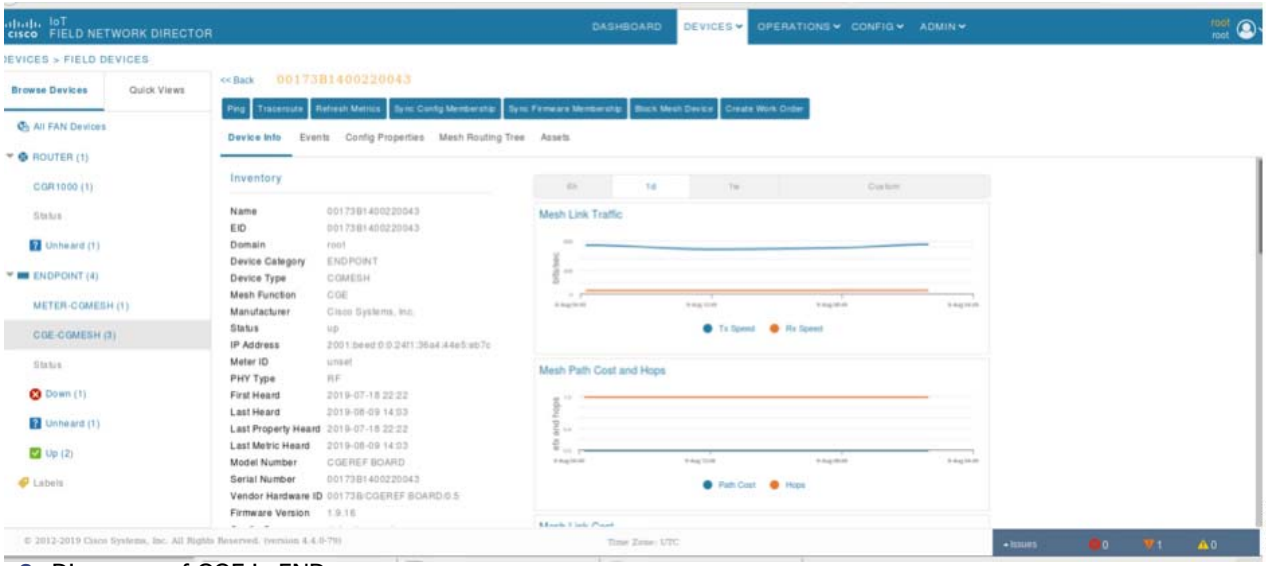
1. Open **FND UI**, click the **Devices** drop-down list, select **Field Devices**, select the **Inventory** tab, click the **Add Devices** tab, select **CR-Mesh csv** and then click **Add**, which will import the CGEs into FND.

Figure 177 Importing CGE into FND

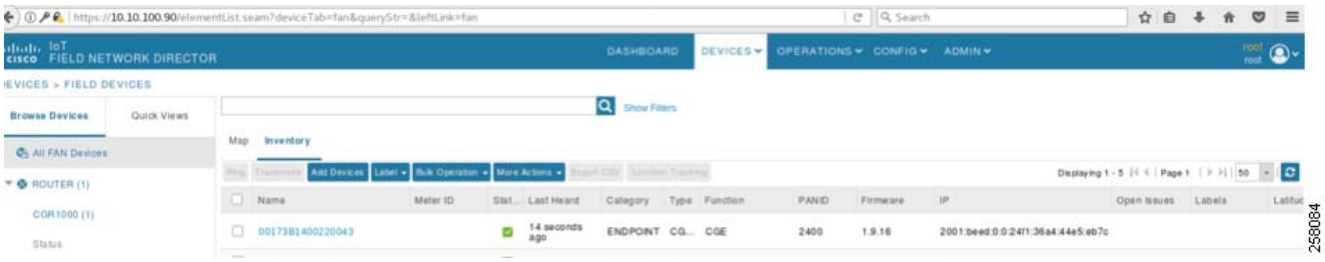


2. After uploading the csv of the devices, once the RPL tree is formed in CGR, devices will show up in FND. The user can monitor the status in FND. Please check the reachability from FND to CGE and vice versa if the CGE doesn't come up.

Figure 178 CGE Properties



3. Discovery of CGE in FND



4. The user can verify the reachability by using *traceroute* and *ping* commands from FND UI. (**Devices-> Click Device(00173B14002200)-> Ping/Traceroute**).

Figure 179 Ping from FND to CGE

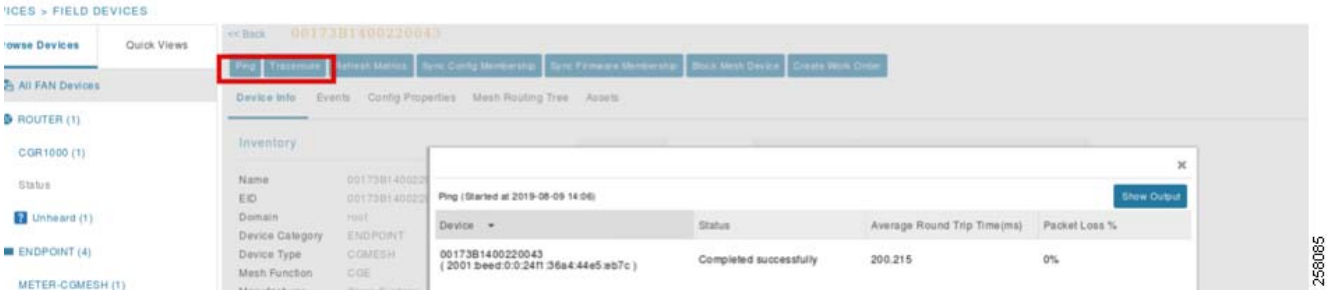
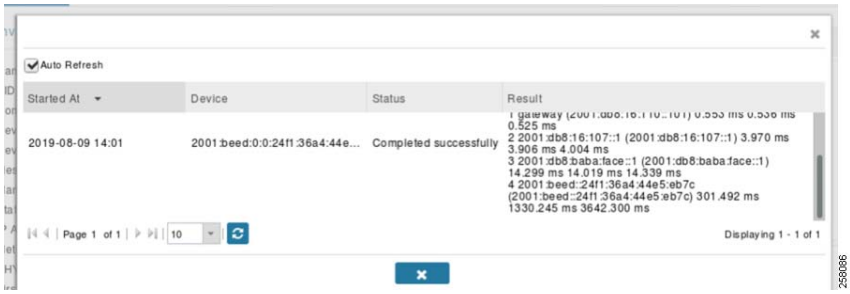


Figure 180 Traceroute from FND to CGE



Use Case: CGE Application Firmware Upgrade Using FND

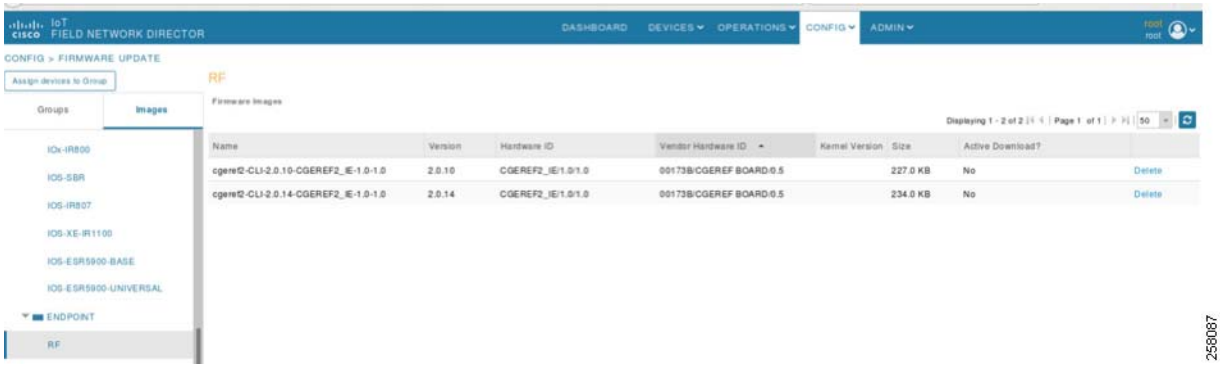
Application Firmware of CGE can be upgraded from the FND. The Application Firmware Image has to be obtained from third party vendors. The steps for performing the upgrade are the following:

1. Upload Image into the Firmware repository.
2. Load Application Firmware Image into CGE.
3. Schedule an upgrade and verify upgrade.

   Note: Make sure the Application Firmware Image is compatible with the WPAN version; otherwise, the user will lose connection to CGE.

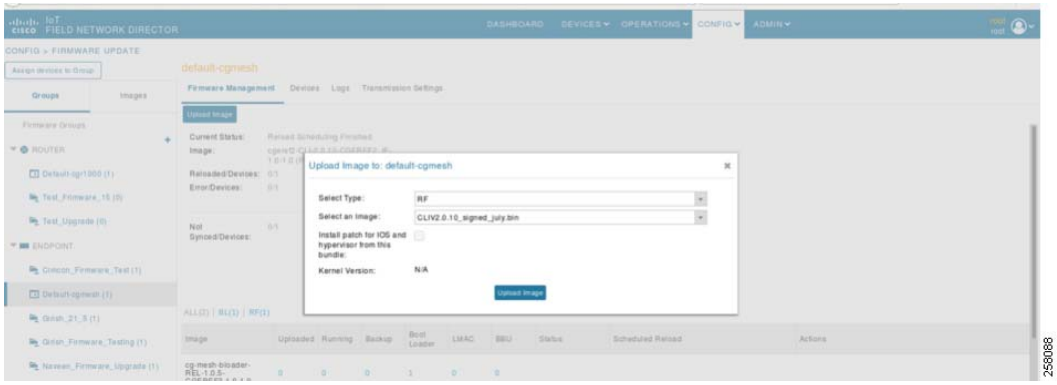
4. Go to **FND UI,** select **Config** drop-down list, and select **Firmware Update**. Select **Images**, select **RF** and click '**+**' icon to upload the Firmware image. Then click **Add File**.

Figure 181 Application Firmware Images of CGEs in FND



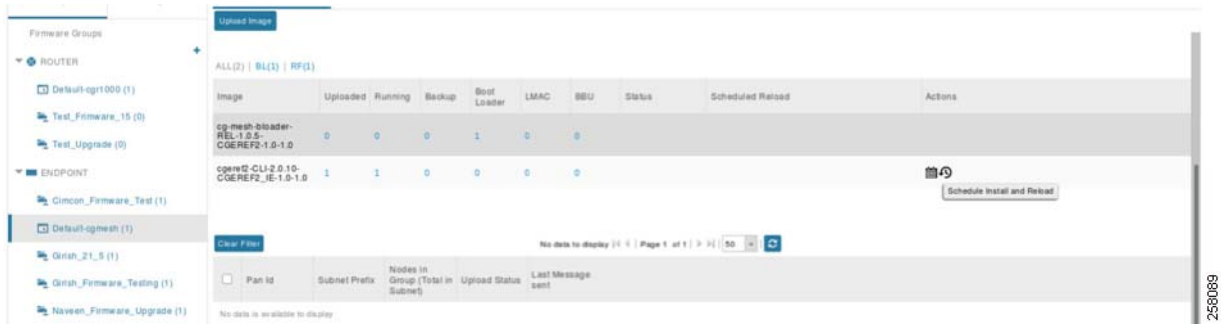
5. Go to **Groups**, select the Group the user wants to upgrade. From **Firmware Management** and **Select Upload Image**, after the pop-up window, select **select-type** as **RF**, and then select the image to upload.

Figure 182 Upload of Application Firmware Image to CGEs



6. After the firmware image is uploaded into the device, schedule an upgrade by clicking **Schedule** as shown in Figure 183:

Figure 183 Scheduling an Upgrade in FND



7. Set the **Install and Reload** time and then CGE will automatically install and reload. After upgrade, when the node comes up, check the node version to be sure that it is in the latest version.

Figure 184 Image Upgrade Successful

Configuring the CGR with WPAN-OFDM Module

CGRs can also be installed with a CGM-WPAN-OFDM module provide a low cost, low power solution to CCI. The CGM-WPAN-OFDM module is designed to operate within an RF900 wireless network to provide control over Cisco Resilient Mesh Endpoints (CR-Mesh) with serial (RS232/RS485), USB (LS/FS), or Fast Ethernet (10/100) ports.

Table 24 WPAN Module Models Used in CCI

Model	Description
CGM-WPAN-FSK-NA	Connected Grid Module—IEEE 802.15.4e/g WPAN 900 MHz.
CGM-WPAN-OFDM-FCC	WPAN RF 900 Plug-in module for CGR 1000 routers. Provides access to 900 MHz mesh networks.

Table 25 LED Indicators of the CGM WPAN-OFDM-FCC WPAN Module

LED Name	Definition	State
RSSI	Measure of power present in the received radio signal.	Yellow (Off) / Green (Off): RSSI less than -105 dBm
		Yellow (On) / Green (Off): RSSI is -105 to -95 dBm
		Yellow (Off) / Green (Slow Blink): RSSI is -95 to -75 dBm
		Yellow (Off) / Green (Fast Blink): RSSI is -75 to -60 dBm
		Yellow (Off) / Green (Solid On): RSSI greater than -60 dBm
WPAN	WPAN traffic activity detect.	Yellow (Off) / Green (Off): WPAN port is disabled.
		Yellow (On) / Green (Off): Searching for network.
		Yellow (Off) / Green (Slow Blink): WPAN port is up.
		Yellow (Off) / Green (Fast Blink): Route is available and DHCPv6 configuration is starting.
		Yellow (Off) / Green (On): Global IPv6 address is available.
SYS	Indicates module status.	Green (Blinking): Broadcast slot time complete

		Yellow (Blinking): Bootload in process
		Yellow (Solid): Software update mode in process

Table 26 shows the CLI interface commands for the CGM WPAN-OFDM Module. In CCI Scenario we have used phy-mode as 98.

Table 26 Summary of CLI Interface Commands for the CGM WPAN-OFDM Module

Command	Definition
ieee154 phy-mode <98 |144 |146 |147 |149 |150 |192 >	Defines the IEEE154 phy-mode. Possible options noted below, default value is 149.
	98: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz
	144: Rate=50 kb/s; Modulation=OFDM; Option=2; MCS=0; Channel Spacing=800 kHz
	146: Rate=200 kb/s; Modulation=OFDM; Option=2; MCS=2; Channel Spacing=800 kHz
	147: Rate=400 kb/s; Modulation=OFDM; Option=2; MCS=3; Channel Spacing=800 kHz
	149: Rate=800 kb/s; Modulation=OFDM; Option=2; MCS=5; Channel Spacing=800 kHz
	150: Rate=1200 kb/s; Modulation=OFDM; Option=2; MCS=6; Channel Spacing=800 kHz

Note:

- The minimum supported firmware version for OFDM WPAN is 5.7.27.
- CGR1000 router must be running Cisco IOS Release 15.7(3)M1 (cgr1000-universalk9-bundle.SPA.157-3.M1.bin) or greater to support the CGM WPAN-OFDM Module.

Sample configuration:

```
interface Wpan4/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 load-interval 30
 ieee154 phy-mode 98
 ieee154 beacon-async min-interval 20 max-interval 120 suppression-coefficient 0
 ieee154 panid 2400
 ieee154 ssid demo_cci
 ieee154 txpower 11
 outage-server 2001:F8:1:110::100
 rpl dag-lifetime 60
 rpl dio-dbl 5
 rpl dio-min 16
 rpl version-incr-time 120
 authentication host-mode multi-auth
 authentication port-control auto
 ipv6 address 2020:BEED::1/64
 ipv6 enable
 ipv6 dhcp server man-dhcpd6 rapid-commit
 dot1x pae authenticator
end
```

Verification commands:

```
CGR1240_FTX123456W#show wpan 4/1 config
Module Type:    RF-WPAN (IEEE 802.15.4e/g RF OFDM)
ssid:           demo_cci
panid:          2400
phy_mode:       98
band-id:        4
transmit power: 11
channel:        254
dwell:          window 20000 max-dwell 400
fec:            ON
beacon async:   min-interval 20 max-interval 120 suppression-coefficient 0
security mode:  1
test mode:      0 (test firmware only)
admin_status:   up
rpl prefix:             2020:BEED::1/64
rpl route-poisoning:    off
rpl dodag-lifetime:     60
rpl dio-dbl:            5
rpl dio-min:            16
rpl version-incr-time: 120
detach bridge:          no
bootloader mode:        no
mcast-agent:            FF38:40:2020:BEED:1 61624 1153
firmware version:       6.0.0
slave mode:             no
wisun mode:             no
ieee154 beacon ver incr time: 60 seconds

CGR1240_ FTX123456W #show wpan 4/1 hardware version
firmware version: 6.1(6.1.27), cg-mesh-bridge, origin/master-6.1, f084af2, May 31 2019
```

Implementing Remote Point-of-Presence (RPoP) Sites

This section covers the implementation of Remote Point-of-Presence (RPoP) sites in CCI network, as discussed in the *CCI Solution Design Guide*. Example Remote PoP sites with LoRaWAN or a CR-Mesh access networks configuration over wireless (cellular) backhaul network that are validated in this CVD are discussed in this section.

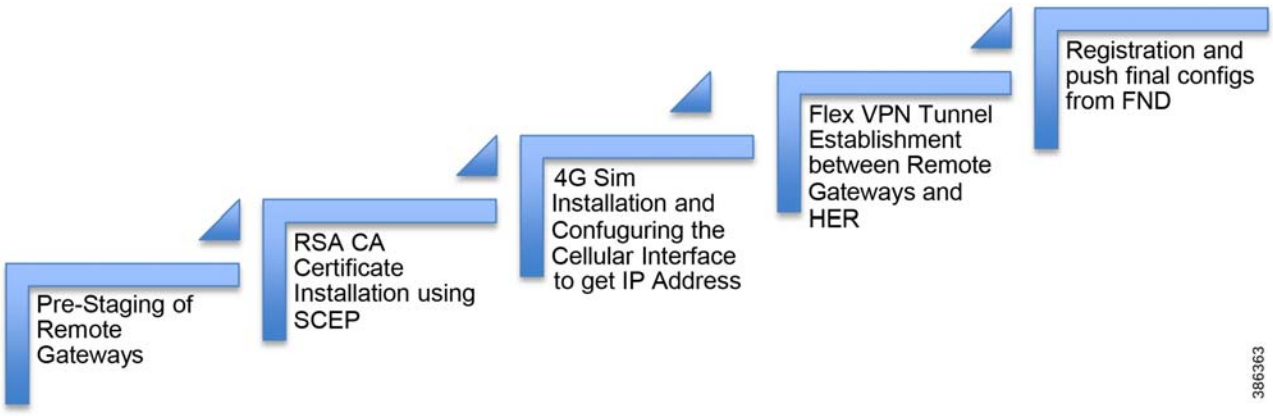
This chapter includes the following major topics:

Implementing RPoP IR1101 with Cellular Backhaul to CCI Headend

This section covers Cisco IR1101 as Remote PoP gateway implementation in CCI. It discusses different services that RPoP offers with the capabilities of IR1101 and how the CCI multiservice network with macro-segmentation is extended to RPoP endpoints/assets via the CCI headend (HE) network in the DMZ.

CCI provides network macro-segmentation using SD-Access using the concept of Virtual Networks (VNs), the same VNs are extended to RPoP Gateways via Flexvpn and each service to be isolated from the other for network security which hence offers isolated and secured multiservice deployments at the RPoP gateways.

Figure 185 RPoP IR1101 Implementation Flow



Pre-staging of IR1101 Gateway

Pre-staging is the process in which the IR1101s are preconfigured with Certificates, tunnel-based configurations, CGNA and WSMA profiles, and EEM script-based configurations. Pre-staging will be done in facility by connecting IR1101 to the LAN. Once pre-staging is done, the remote Gateways will be shipped to the deployment locations. The pre-staging steps are:

1. LAN Configuration
2. SCEP Enrollment of IR1101

3. 4G Sim Installation and Configuration
4. FlexVPN Tunnel Establishment
5. IR1101 Registration into FND (NMS) and Management

LAN Configuration

For SCEP Enrollment, IR1101 is connected to the CA server for loading certificates. Before certificate enrollment, configure the LAN interface of the IR1101 to communicate with the CA server. Connect the FastEthernet port of IR1101 to any of the CCI Access trusted switch which has reachability to the CA server.

Create an SVI and configure VLAN and assign IP address via DHCP:

```
interface Vlan1022
 ip address dhcp
```

Configure IR1101 interface :

```
interface FastEthernet0/0/1
 switchport mode access
 switchport access vlan 1022
```

SCEP Enrollment of IR1101

Prerequisites for PKI Certificate Enrollment

Before configuring peers for certificate enrollment, you should have the following items:

- Domain Name configuration

  ```
  ip domain name cimconccibgl.cisco.com
  ip host rsaca.cimconccibgl.cisco.com <CA_Server_IP>
  ip host cci-fnd-oracle.cimconccibgl.cisco.com <FND_IP>
  ```

- An authenticated CA

  2016 Windows Server acts as Authority Server (Certificate Server) both in Auto Enrollment and Auto Approval.

- NTP Settings

  Enable NTP on the device so that the PKI services such as Auto Enrollment and certificate rollover may function correctly. (Device should be synchronized with CA server.)

  ```
  ntp server x.x.x.x ' IP Address of NTP server.
  ```

Steps to Enroll IR1101 with the RSA CA Server

The following steps need to be performed:

1. Creation of a 2048-bit RSA key-pair named LDevID.
2. Definition of certificate authority details, trusted by the HER/IR1101 (that is, trust point definition):
   a. Enrollment profile (with Enrollment URL defined) to reach the certificate authority for certificate enrollment.
   b. Communication restricted only to the Authentic certificate authority, by performing a fingerprint check.

c. Communications accepted only from the RSA CA server, whose advertised SHA1 fingerprint/thumbprint matches with the configured fingerprint.

d. The serial number to be part of the certificate.

e. The IP address is NOT needed to be part of the certificate.

f. No password is needed during certificate enrollment.

g. The key pair created above in this section is used.

3. Receiving a copy of the RSA CA server's certificate (with public key).

4. Receiving the certificate of HER signed by RSA CA server:

   a. The signed certificate should contain the above details, which are configured under the trust point definition.

Note: Ensure that no blank space exists after the password in the Trustpoint configuration.

```
      ***********Creating 2048-bit length RSA key-pair, named as 'LDevID'**********
crypto key generate rsa label LDevID modulus 2048
!***********URL to reach the RSA CA server's SCEP Enrollment service.********
crypto pki profile enrollment LDevID
enrolment url http://rsaca.cimconccibgl.cisco.com/certsrv/mscep/mscep.dll
************Trust point configuration for RSA CA server*************
crypto pki trustpoint LDevID
enrollment retry count 4
enrollment retry period 2
enrollment mode ra
enrollment profile LDevID
serial-number none
fqdn none
ip-address none
password
fingerprint 9F069AEA02B6E0B438C6E545169E76846020D5EF
subject-name serialNumber=PID: IR1101-K9 SN:FCW23100HS2,CN=
IR1101-K9_FCW23100HS2.cimconccibgl.cisco.com
revocation-check none
rsakeypair LDevID 2048

!
!*************To Receive a copy of the RSA CA server's certificate (with public key of CA)********
crypto pki authenticate LDevID
!
!
!*************To receive the CGR's certificate signed by the RSA CA server.************ crypto pki
enroll LDevID
!
!
```

Verifying the Certificate Enrollment Status of IR1101:

```
IR1101#show crypto pki trustpoints LDevID
Trustpoint LDevID:
    Subject Name:
    cn=cci-rsa-ca
    dc=cimconccibgl
    dc=cisco
    dc=com
          Serial Number (hex): 7166F8B04EBE41BD4F91E3C852B16310
    Certificate configured.
    SCEP URL: http://rsaca.cimconccibgl.cisco.com:80/certsrv/mscep/mscep.dll
```

```
IR1101#show crypto pki certificates LDevID
Certificate
  Status: Available
  Certificate Serial Number (hex): 650000003728F294829EFAA473000000000037
  Certificate Usage: General Purpose
  Issuer:
    cn=cci-rsa-ca
    dc=cimconccibgl
    dc=cisco
    dc=com
  Subject:
    Name: IR1101-K9_FCW23100HS2
    Serial Number: PID: IR1101-K9 SN:FCW23100HS2
    cn=IR1101-K9_FCW23100HS2
    serialNumber=PID: IR1101-K9 SN:FCW23100HS2
  CRL Distribution Points:

ldap:///CN=cci-rsa-ca,CN=WIN-HJOAMVKC7AA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration
,DC=cimconccibgl,DC=cisco,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Validity Date:
    start date: 04:57:57 UTC Jun 9 2020
    end   date: 05:07:57 UTC Jun 9 2022
  Associated Trustpoints: LDevID

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 7166F8B04EBE41BD4F91E3C852B16310
  Certificate Usage: Signature
  Issuer:
    cn=cci-rsa-ca
    dc=cimconccibgl
    dc=cisco
    dc=com
  Subject:
    cn=cci-rsa-ca
    dc=cimconccibgl
    dc=cisco
    dc=com
  Validity Date:
    start date: 17:33:51 UTC May 30 2019
    end   date: 17:43:50 UTC May 30 2024
  Associated Trustpoints: LDevID
```

Note: The enrollment URL differs according to the type of RSA CA server.

4G SIM Installation and Configuration

Refer to the following to install SIM on IR1101:
https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_010.html

- IR1101 SIM installation (requires a pluggable LTE module installed on the gateway)

IR1101 Cellular Interface Example Configuration:

```
interface Cellular0/1/0
 description Cellular Connection to HER Public IP
 mtu 1430
 ip address negotiated
 ip nat outside
 ip tcp adjust-mss 1460
 dialer in-band
 dialer idle-timeout 0
```

```
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
end

ip route 0.0.0.0 0.0.0.0 Cellular0/1/0

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
```

FlexVPN Tunnel Establishment

This section covers the configurations that have to be executed on the Cisco IR1101 in order to establish a FlexVPN tunnel with the HER. The security configurations should match with that of the HER security configurations ito form the FlexVPN tunnel.

```
aaa new-model
aaa authorization exec default local
aaa authorization network FlexVPN_Author local

!
crypto ikev2 authorization policy FlexVPN_Author_Policy
route set interface
route set access-list FlexVPN_Client_Default_IPv4_Route
route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route

!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_Cert
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_Cert
proposal FlexVPN_IKEv2_Proposal_Cert
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile_Cert
match identity remote fqdn CCI-HER-1
identity local fqdn spoke-18-flexVPN
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint LDevID
dpd 120 3 periodic
aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 fragmentation
crypto ikev2 client flexvpn FlexVPN_Client
    peer 1 <HER_Public_IP> !!!!! IP Address of HER facing IR1101 Gateway
 client connect Tunnel100
!
!
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha-hmac
mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile_Cer
set transform-set FlexVPN_IPsec_Transform_Set
set pfs group14
set ikev2-profile FlexVPN_IKEv2_Profile_Cert
```

```
!
!

interface Loopback25
description loopback IP for tunnel
ip address 192.168.200.25 255.255.255.0
ipv6 address 2001:DB8:BABA:FACE::25/64
ipv6 enable
!
interface Tunnel100
description IPsec tunnel to HER
ip unnumbered Loopback25
ipv6 unnumbered Loopback25
tunnel source Cellular0/1/0
tunnel destination dynamic
tunnel protection ipsec profile FlexVPN_IPsec_Profile_Cer
!
```

Selective Route Advertisement from IR1101 to HER:

IR1101 routes to HER selected by advertising specific prefixes through IKEv2 prefix injection as shown below:

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy route set interface
route set access-list FlexVPN_Client_Default_IPv4_Route route set access-list ipv6
FlexVPN_Client_Default_IPv6_Route
!
!
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit 10.22.22.11
 permit 10.254.254.11
!
```

IR1101 Registration into FND and Management

For IR1101 registration with FND and management, refer to FAR Registration into FND (NMS), page 214.

RPoP Macro-Segmentation Implementation

In CCI SDA deployment, Virtual Networks (VN) provide the isolation of networks by segmenting the overall network into multiple logically separate networks as needed. In RPoP deployments the CCI SDA VNs are extended to the RPoP Gateways (IR1101s).

Stretching the SDA VNs to the RPoP gateways involves two steps:

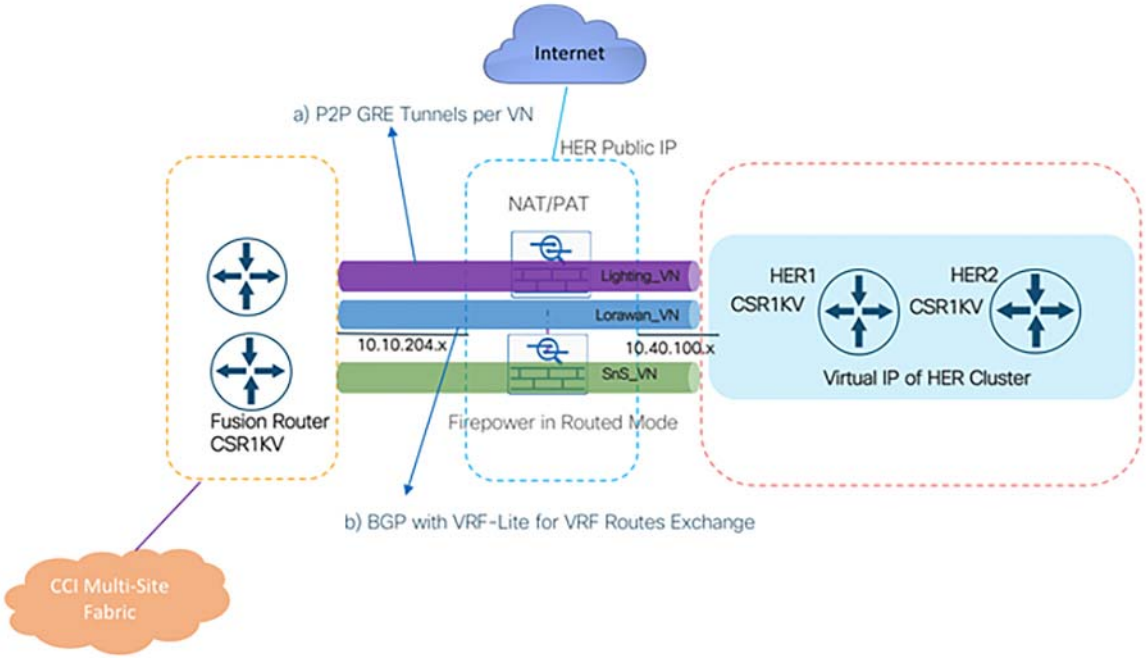
1. Extending the SDA Multi-VRF routes to HER from FR
2. Multi-VRF routes extension from HER to RPoP Gateway

Extending the SDA Multi-VRF Routes to HER from FR

As Fusion router is aware of all the prefixes available inside each VRF, because of through route peering from the Borders of different PoP sites, therefore the intended VRFs can be extended to the RPoP Gateway by VRF-Lite using BGP.

In CCI, Firepower is positioned between the Fusion Router and the HER and it is deployed in Routed mode. To use VRF-Lite between Fusion Router and HER to exchange Multi-VRF route prefixes, FR and HER should be in the same network. To overcome this Point to Point (P2P) Generic Routing Encapsulation (GRE) tunnelling mechanism is used. The configuration steps are shown.

Figure 186 VN/VRF Extension from Fusion Router to HER



Step 1: Configuring VRF definitions:

Configure the VRF definitions on the HER for the VRFs/VNs which we intended to stretch to the RPoP. Each VRF is assigned a Route Distinguisher.

```
!
vrf definition Lighting_VN
 rd 1:4100
!
vrf definition SnS_VN
 rd 1:4099
 !
```

Note: VRF-lite configuration does not need the route-target.

Step 2: GRE Interfaces reachability:

GRE source and destination interfaces reachability can be achieved by advertising via static or undelay routing, in our case EIGRP.

Fusion Route Configuration	HER Configuration
`router eigrp 2000`	`router eigrp 2000`
`network 10.11.11.0 0.0.0.255`	`network 10.11.11.0 0.0.0.255`

Step 3: Configuring GRE Tunnels for Each VN/VRF:

The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. Configuring a GRE tunnel involves creating a tunnel interface, which is a logical interface. Below is the example configuration on FR and HER for two of the VRFs.

Fusion Route Configuration	HER Configuration
interface loopback11 description Tunnel11 source IP ip address 10.11.11.11 255.255.255.255 no shut exit interface Tunnel11 **description Tunnel for Lighting_VN** vrf forwarding Lighting_VN ip address 10.255.255.1 255.255.255.252 tunnel source loopback11 tunnel destination 10.11.11.12 tunnel mode gre ip	interface loopback11 description Tunnel1 source IP ip address 10.11.11.12 255.255.255.255 no shut exit interface Tunnel11 **description Tunnel for Lighting_VN** vrf forwarding Lighting_VN ip address 10.255.255.2 255.255.255.252 tunnel source loopback11 tunnel destination 10.11.11.11 tunnel mode gre ip
interface loopback14 description Tunnel14 source IP ip address 10.11.11.17 255.255.255.255 no shut exit interface Tunnel14 **description Tunnel for SnS_VN** vrf forwarding SnS_VN ip address 10.255.255.13 255.255.255.252 tunnel source loopback14 tunnel destination 10.11.11.18 tunnel mode gre ip	interface loopback14 description Tunnel14 source IP ip address 10.11.11.18 255.255.255.255 no shut exit interface Tunnel14 **description Tunnel for SnS_VN** vrf forwarding SnS_VN ip address 10.255.255.14 255.255.255.252 tunnel source loopback14 tunnel destination 10.11.11.17 tunnel mode gre ip

Verification:

```
CCI-HER-1#show ip interface tunnel 11
Tunnel11 is up, line protocol is up
  Internet address is 10.255.255.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1476 bytes
 <snip>
 IP Null turbo vector
  VPN Routing/Forwarding "Lighting_VN"
  <snip>

CCI-HER-1#sh tunnel interface tunnel11
Tunnel11
   Mode:GRE/IP, Destination 10.11.11.11, Source Loopback11
   IP transport: output interface GigabitEthernet1 next hop 10.40.100.1
   Application ID 1: unspecified
   OCE: IP tunnel decap
   Provider: interface Tu11, prot 47
     Performs protocol check [47]
     Protocol Handler: GRE: opt 0x0
       ptype: ipv4 [ipv4 dispatcher: from if Tu11]
       ptype: ipv6 [ipv6 dispatcher: punt]
       ptype: mpls [mpls dispatcher: drop]
       ptype: otv [mpls dispatcher: drop]
       ptype: generic [mpls dispatcher: drop]
   Tunnel Subblocks:
      src-track:
         Tunnel11 source tracking subblock associated with Loopback11
          Set of tunnels with source Loopback11, 1 member (includes iterators), on interface <OK>
   Linestate - current up
   Internal linestate - current up, evaluated up
   Tunnel Source Flags: Local
   Transport IPv4 Header DF bit cleared
```

Step 4: VRF-Lite with BGP Configuration:

eBGP is configured on FR and HER by peering with GRE tunnel interfaces. IPv4 address families are used to specify the VRFs and redistribute the connected interfaces into BGP.

Fusion Route Configuration	HER Configuration

router bgp 65540
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf Lighting_VN
redistribute connected
  redistribute static
  neighbor 10.255.255.2 remote-as 65550
  neighbor 10.255.255.2 update-source
Tunnel11
  neighbor 10.255.255.2 activate
 exit-address-family
 	
 address-family ipv4 vrf SnS_VN
redistribute connected
  redistribute static
  neighbor 10.255.255.14 remote-as 65550
  neighbor 10.255.255.14 update-source
Tunnel14
  neighbor 10.255.255.14 activate
 exit-address-family
	router bgp 65550
	 bgp log-neighbor-changes
	 !
	 address-family ipv4 vrf Lighting_VN
	redistribute connected
	  redistribute static
	  neighbor 10.255.255.1 remote-as 65540
	  neighbor 10.255.255.1 update-source
	Tunnel11
	  neighbor 10.255.255.1 activate
	 exit-address-family
	
	 address-family ipv4 vrf SnS_VN
	redistribute connected
	  redistribute static
	  neighbor 10.255.255.13 remote-as 65540
	  neighbor 10.255.255.13 update-source
	Tunnel14
	  neighbor 10.255.255.13 activate
	 exit-address-family

Verification:

Check the routing table to confirm the HER learned the routes advertised from the corresponding VRF on FR.

```
CCI-HER-1#sh ip route vrf Lighting_VN

Routing Table: Lighting_VN
<snip>
Gateway of last resort is 10.255.255.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 10.255.255.1, 03:33:24
      10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
B        10.10.100.0/24 [20/0] via 10.255.255.1, 03:33:24
B        10.40.100.0/24 [20/0] via 10.255.255.1, 03:33:24
C        10.255.255.0/30 is directly connected, Tunnel11
L        10.255.255.2/32 is directly connected, Tunnel11
      172.17.0.0/24 is subnetted, 1 subnets
B        172.17.70.0 [20/0] via 10.255.255.1, 03:33:24
      172.20.0.0/24 is subnetted, 3 subnets
B        172.20.80.0 [20/0] via 10.255.255.1, 03:33:24
B        172.20.90.0 [20/0] via 10.255.255.1, 03:33:24
B        172.20.100.0 [20/0] via 10.255.255.1, 03:33:24
      172.22.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        172.22.70.0/24 [20/0] via 10.255.255.1, 03:33:24
B        172.22.80.1/32 [20/0] via 10.255.255.1, 03:33:24
B        172.22.100.2/32 [20/0] via 10.255.255.1, 03:33:24
      192.168.70.0/30 is subnetted, 1 subnets
B        192.168.70.4 [20/0] via 10.255.255.1, 03:33:24
B     192.168.200.0/24 [20/0] via 10.255.255.1, 03:33:24
```

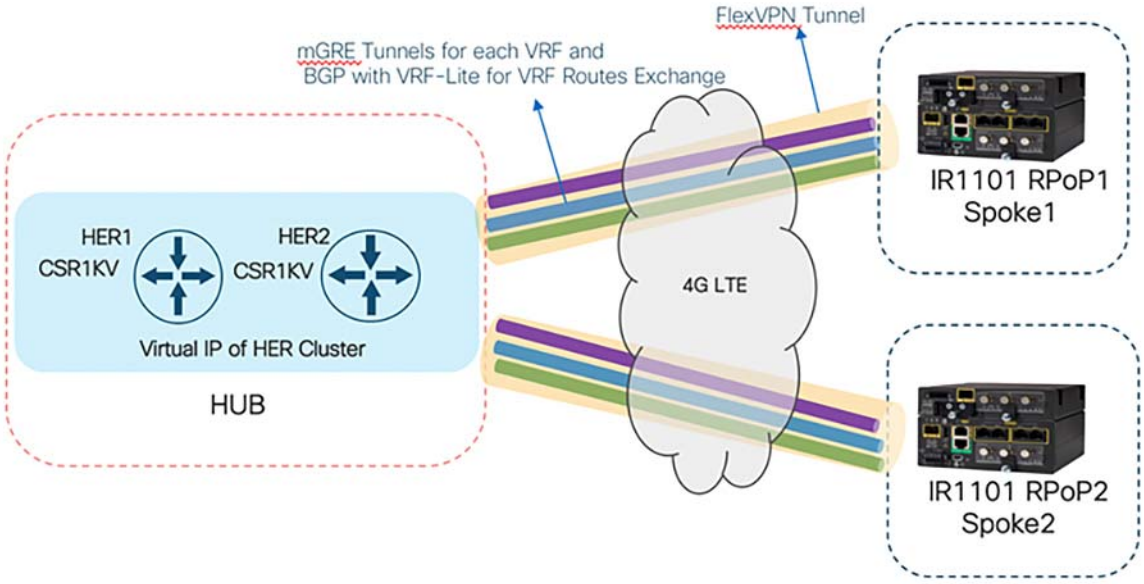
Multi-VRF Routes Extension from HER to RPoP Gateway

Prerequisites:

- Flexvpn tunnel has been established between the HER and the RPoP Gateway (IR1101).
- RPoP Intended VRF/VN routes are exchanged between the Fusion Router (FR) and the HER.

The following steps describe the Multi-VRFs extended from HER to multiple RPOPs using a secured FlexVPN transport.

Figure 187 Macro-Segmentation VRF Exchange to IR1101 RPoP Gateways



Step 1: Configuring VRF definitions:

Configure the required VRF definitions on the RPoP (IR1101) Gateways. Each VRF is assigned a Route Distinguisher.

```
!
vrf definition Lighting_VN
 rd 1:4100
!
vrf definition SnS_VN
 rd 1:4099
 !
```

Note: VRF-lite configuration does not need the route-target.

Step 2: mGRE Interfaces reachability:

Using IKEV2 Prefix injection, advertise mGRE Tunnel source loopbacks using FlexVPN access-list. An example configuration on HER and IR1101 Spoke is shown below.

HER (Hub) Configuration	RPoP Gateway (IR1101) Configuration
ip access-list standard FlexVPN_Client_Default_IPv4_Route permit 10.254.254.1 permit 10.254.254.4 permit 10.22.22.0 0.0.0.255	ip access-list standard FlexVPN_Client_Default_IPv4_Route permit 10.22.22.11 permit 10.254.254.11 permit 10.22.22.14 permit 10.254.254.14

Step 3: Configuring mGRE overlay Tunnels for each VN/VRF on FlexVPN:

As there is one HER (Hub) and there are multiple RPoP(IR11010) Spokes, to accomplish this Multipoint GRE (mGRE) is used. Multipoint GRE(mGRE) allows us to have multiple destinations from HER(Hub) and helps to form an overlay network.

Since Next Hop Resolution Protocol (NHRP) uses this server and clients model, below are the roles assigned to the Hub and the Spokes:

- HER (Hub) will be the NHRP server.
- IR1101 RPoPs (Spokes) will be NHRP clients.
- NHRP clients (spokes) register themselves with the NHRP server and report their public IP address.
- The NHRP server (Hub) keeps track of all public IP addresses in its cache.
- New spokes can be added without requiring any configuration changes on the hub devices.
- The overlay logical mGRE network is part of a single IP subnet and many distinct point-to-point subnets are not required for each GRE spoke tunnel.

In our case, one mGRE tunnel is created for each VN/VRF. NHRP is enabled on the mGRE interface using the ip nhrp network-id command. The value specified must match the one configured on the spoke devices.

Each tunnel interface is mapped to the respective VRF using the vrf forwarding command, which is the key starting point in building the overlay logical network. An example configuration on HER and the IR1101 is shown below.

HER (Hub) Configuration	RPoP Gateway (IR1101) Configuration
interface loopback21 description Tunnel21 source IP ip address 10.22.22.11 255.255.255.255 no shut exit interface Tunnel21 description Tunnel for **Lighting_VN** vrf forwarding Lighting_VN ip address 10.254.254.11 255.255.255.0 ip nhrp map 10.254.254.1 10.22.22.1 ip nhrp network-id 1 ip nhrp holdtime 600 ip nhrp nhs 10.254.254.1 ip nhrp registration timeout 30 tunnel source loopback21 tunnel mode gre multipoint	interface loopback21 description Tunnel21 source IP ip address 10.22.22.21 255.255.255.255 no shut exit interface Tunnel21 description Tunnel for **Lighting_VN** vrf forwarding Lighting_VN ip address 10.254.254.21 255.255.255.0 ip nhrp map 10.254.254.1 10.22.22.1 ip nhrp network-id 1 ip nhrp holdtime 600 ip nhrp nhs 10.254.254.1 ip nhrp registration timeout 30 tunnel source loopback21 tunnel mode gre multipoint

MTU Considerations:

The use of GRE tunnels to create overlay logical networks can eventually cause MTU issues because of the increased size of the IP packets. The goal is to avoid IP fragmentation whenever possible and to avoid all related issues. For more information, see:

- http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml

Step 4: VRF-Lite with BGP Configuration:

Routing for overlay traffic between the HER and the spokes is done by VRF-Lite using iBGP by peering the mGRE tunnel interfaces. IPv4 address families are used to specify the VRFs and redistribute the connected interfaces into BGP.

HER (Hub) Configuration	RPoP Gateway (IR1101) Configuration

router bgp 65550
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf Lighting_VN
  redistribute connected
  redistribute static
  neighbor 10.254.254.1 remote-as 65550
  neighbor 10.254.254.1 update-source
Tunnel21
  neighbor 10p.254.254.1 activate
 exit-address-family
 	
 address-family ipv4 vrf SnS_VN
  redistribute connected
  redistribute static
  neighbor 10.254.254.4 remote-as 65550
  neighbor 10.254.254.4 update-source
Tunnel24
  neighbor 10.254.254.4 activate
 exit-address-family
	router bgp 65550
	 bgp log-neighbor-changes
	 !
	 address-family ipv4 vrf Lighting_VN
	  redistribute connected
	  redistribute static
	  neighbor 10.254.254.1 remote-as 65550
	  neighbor 10.254.254.1 update-source
	Tunnel21
	  neighbor 10.254.254.1 activate
	 exit-address-family
	
	 address-family ipv4 vrf SnS_VN
	  redistribute connected
	  redistribute static
	  neighbor 10.254.254.4 remote-as 65550
	  neighbor 10.254.254.4 update-source
	Tunnel24
	  neighbor 10.254.254.4 activate
	 exit-address-family

Verification:

Check the routing table on IR1101 Spoke to confirm the Spokes learned the routes advertised from the corresponding VRF on HER.

```
IR1101#sh ip route vrf SnS_VN

Routing Table: SnS_VN
<snip>
Gateway of last resort is 10.254.254.4 to network 0.0.0.0

B*    0.0.0.0/0 [200/0] via 10.254.254.4, 1d06h
      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
B        10.10.100.0/24 [200/0] via 10.254.254.4, 1d06h
B        10.40.100.0/24 [200/0] via 10.254.254.4, 1d06h
C        10.254.254.12/30 is directly connected, Tunnel24
L        10.254.254.14/32 is directly connected, Tunnel24
B        10.255.255.12/30 [200/0] via 10.254.254.4, 1d06h
B     172.5.0.0/16 [200/0] via 10.254.254.4, 1d06h
B     172.6.0.0/16 [200/0] via 10.254.254.4, 1d06h
B     172.7.0.0/16 [200/0] via 10.254.254.4, 1d06h
      172.9.0.0/24 is subnetted, 3 subnets
B        172.9.80.0 [200/0] via 10.254.254.4, 1d06h
B        172.9.90.0 [200/0] via 10.254.254.4, 1d06h
B        172.9.100.0 [200/0] via 10.254.254.4, 1d06h
      172.10.0.0/24 is subnetted, 3 subnets
B        172.10.80.0 [200/0] via 10.254.254.4, 1d06h
B        172.10.90.0 [200/0] via 10.254.254.4, 1d06h
B        172.10.100.0 [200/0] via 10.254.254.4, 1d06h
      172.15.0.0/24 is subnetted, 1 subnets
B        172.15.70.0 [200/0] via 10.254.254.4, 1d06h
      172.16.0.0/24 is subnetted, 1 subnets
```

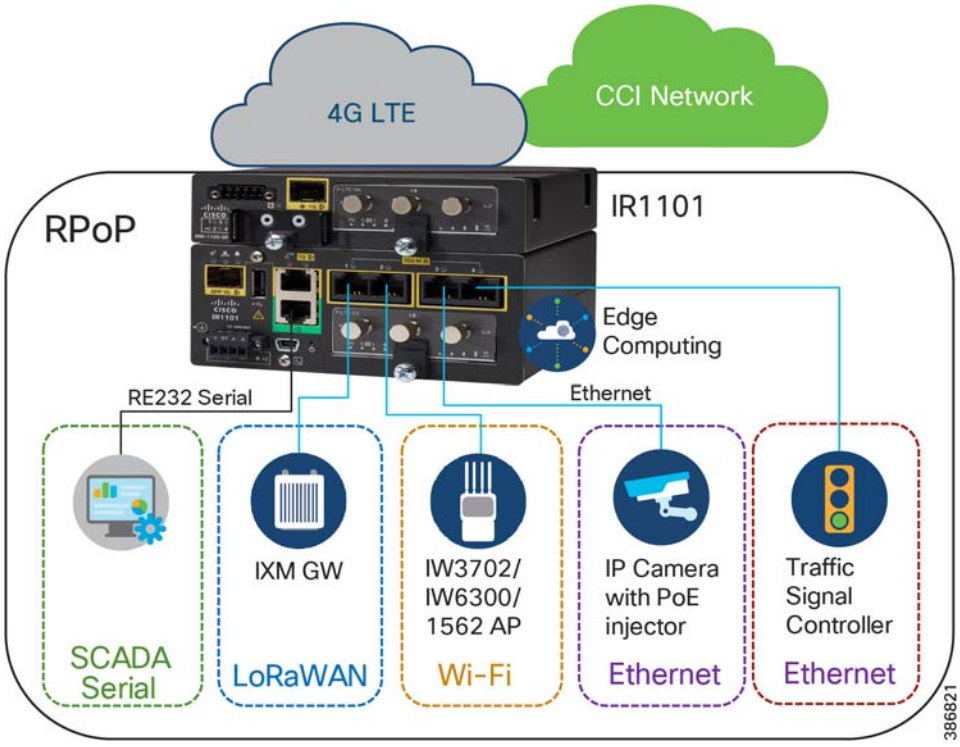
```
B        172.16.70.0 [200/0] via 10.254.254.4, 1d06h
      192.168.70.0/30 is subnetted, 1 subnets
B        192.168.70.8 [200/0] via 10.254.254.4, 1d06h
B     192.168.200.0/24 [200/0] via 10.254.254.4, 1d06h
```

RPoP Multi-Service Implementation

IR1101 supports LAN ports and a RS232 Serial port which helps connect various CCI vertical endpoints. As the macro-segmentation using mGRE tunnels with VRF-Lite is discussed in the above section, the multiple endpoints corresponding to different vertical services can be onboarded by creating an SVI with an IP Pool for a VN Service.

Because the CCI DHCP infrastructure is deployed in a centralized location in the network, the first Layer 3 hop devices need to be able to relay the initial broadcast DHCP request received from the RPoP client to the remotely located DHCP server. This is supported via the ip helper-address command. With the help of helper address, dynamic IP address can be fetched from CCI DHCP server, which is in Shared Services.

Figure 188 Multi-Service Onboarding on IR1101



Host Onboarding on IR1101

Example Configuration for SVI for Lighting_VN:

```
Vlan 125

interface Vlan125
 vrf forwarding Lighting_VN
 ip address 172.10.25.1 255.255.255.0
 ip helper-address 10.10.100.20
end
```

Any Access Host can be connected to the port using the Access Configuration:

Example Configuration for Port Configuration for Access Hosts:

```
interface FastEthernet0/0/1
 switchport access vlan 125
 switchport mode access
 spanning-tree portfast
end
```

Example Configuration for Port Configuration for FlexConnect AP:

```
interface FastEthernet0/0/2
 switchport trunk native vlan 125
 switchport trunk allowed vlan 125,225,325,425
 switchport mode trunk
 spanning-tree portfast
end
```

Shared Services Reachability

To enable the reachability of the RPoP clients which are part of the overlay VRF network to the Shared Services which are in Global routing table, perform the following configuration on Fusion Router and the HER.

On Fusion Router:

Using Route-map, do the route-leaking of the VRFs to talk to the Shared Services network.

```
vrf definition Lighting_VN
 rd 1:4100
 address-family ipv4
  export ipv4 unicast map Lighting-VN-TO-GLOBAL

route-map Lighting-VN-TO-GLOBAL permit 10
 match ip address prefix-list CESSNA_Lighting_VN_ROUTES

ip prefix-list CESSNA_Lighting_VN_ROUTES seq 52 permit 10.254.254.0/30
ip prefix-list CESSNA_Lighting_VN_ROUTES seq 48 permit 10.255.255.0/30
ip prefix-list CESSNA_Lighting_VN_ROUTES seq 53 permit 172.10.25.0/24
```

On HER:

Add static route to take the GRE tunnel to reach the Fusion Router.

```
ip route vrf Lighting_VN 10.10.100.0 255.255.255.0 10.255.255.1
```

AAA at RPoP:

IR1101 RPoP Gateway can act as an authentication, authorization, and accounting (AAA) client through which AAA service requests are sent to Cisco ISE, which is located in CCI shared services.

To add IR1101 as a network device refer to Add a Network Device in ISE at:

- https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_secure_wired_access.html?bookSearch=true#task_5A6DE8F287AF43AB964DC5C10DAAC86F

Configure the AAA and RADIUS configurations on the IR1101s. An example configuration is shown below.

```
radius server dnac-radius_10.10.100.55
 address ipv4 10.10.100.55 auth-port 1812 acct-port 1813
 timeout 4
 retransmit 3
 pac key Cisco@123
```

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3


aaa new-model
aaa group server radius dnac-client-radius-group
 server name dnac-radius_10.10.100.55
 ip radius source-interface Loopback39
aaa group server radius dnac-network-radius-group
 server name dnac-radius_10.10.100.55
 ip radius source-interface Loopback39
aaa authentication login default local
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication login VTY_authen group dnac-network-radius-group local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec default local
aaa authorization exec VTY_author group dnac-network-radius-group local if-authenticated
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group dnac-client-radius-group
aaa accounting exec default start-stop group dnac-network-radius-group
aaa server radius dynamic-author
 client 10.10.100.55 server-key 0 Cisco@123
aaa session-id common

dot1x system-auth-control

aaa server radius dynamic-author
 client 10.10.100.55 server-key 0 Cisco@123
```

Secure connectivity for the wired endpoints or hosts connecting to RPoP Gateway can be implemented using 802.1X authentication mechanism for the endpoints supporting 802.1X protocols. For the endpoints that do not support 802.1X protocol, MAC Authentication Bypass (MAB) can be implemented to authenticate and authorize the endpoints or hosts connecting to RPoP overlay network.

For implementation of 802.1X and MAB for the wired clients like IP Camera, refer to Endpoints Security Using 802.1X and MAC Authentication Bypass, page 366.

Example Configuration on the Port to which IP Camera is Connected:

```
interface FastEthernet0/0/3
 switchport access vlan 425
 switchport mode access
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 service-policy type control subscriber Dot1xOrMAB
end
```

Internet Connectivity at RPoP

To provide internet access for the RPoP clients directly from IR1101 Cellular LTE connectivity, follow the steps below.

Step 1: As the RPoP clients are part of VRF network, route-leaking is required between the VRF table and the Global routing table. The example below shows the route-leaking configuration between the VRF and global routing table using the prefix-list and route-maps.

```
route-map Lighting-VN-TO-GLOBAL permit 10
 match ip address prefix-list Lighting_VN_ROUTES
ip prefix-list Lighting_VN_ROUTES seq 1 permit 172.10.25.0/24
ip prefix-list Lighting_VN_ROUTES seq 2 permit 10.254.254.0/24
vrf definition Lighting_VN
 rd 1:4100
 address-family ipv4
 export ipv4 unicast map Lighting-VN-TO-GLOBAL
```

Step 2: Create Access-list for allowed NAT source prefixes, Apply the access-list to the dialer.

```
ip access-list standard 1
  permit 172.10.25.0 0.0.0.255

dialer-list 1 protocol ip list 1
```

Step 3: Configure an IP NAT side rule for VRF with allowed list.

```
ip nat inside source list 1 interface Cellular0/1/0 vrf Lighting_VN overload
```

Step 4: Apply IP NAT inside on SVI and NAT outside on cellular interface.

```
interface Vlan125
 description SVI for Lighting VRF
 vrf forwarding Lighting_VN
 ip address 172.10.25.1 255.255.255.0
 ip helper-address 10.10.100.20
 ip nat inside
end

interface Cellular0/1/0
 description Cellular Connection to Firewall Public IP
 mtu 1430
 ip address negotiated
 ip nat outside
 ip tcp adjust-mss 1460
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
end
```

Verification:

```
IR1101-Spoke25#ping vrf Lighting_VN 8.8.8.8 so vlan125
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 172.10.25.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/36/48 ms
```

Application Hosting on RPoP IR1101

Cisco IOx allows you to execute IoT applications in the fog with secure connectivity with Cisco IOS software and get powerful services for rapid, reliable integration with IoT sensors and the cloud. For information about configuring application on IR1101 for edge computing, see:

- https://developer.cisco.com/docs/iox/#!phase-1-configuring-application-hosting-for-the-cisco-ir1101-industrial-integrated-services-router

RPoP High Availability Implementation with Dual-LTE

In a normal operational mode, IR1101 connects to HER securely over Tunnel0 over Primary LTE module (Cellular 0/1/0). Therefore, Tunnel0 becomes the primary mode of communication between the IR1101 and the HER. When connectivity over primary cellular interface fails, the communication between the IR1101 and the HER must be restored and secured. IR1101 ISR has an Expansion Module that adds the dual LTE capability which allows us to have WAN redundancy. This restoration will establish the connectivity between the IR1101 and the HER over the second LTE module (Cellular0/3/0). This activation of Tunnel to carry the load in the event of Cellular0/1/0 failure is referred as Failover. When connectivity over cellular0/1/0 is restored, the IR1101 and the HER can communicate securely using Cellular0/1/0. This switchover is known as Recovery. For the switchover to be automatic, EEM script is configured on the IR1101. The EEM script tracks the line-protocol of the cellular interface. The following configuration is applied on the IR1101.

```
track 3 interface Cellular0/1/0 line-protocol

EEM Script Configuration
*************************
event manager applet Failover
 event track 3 state down
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface cellular 0/3/0"
 action 4  cli command "no shutdown"
 action 5  cli command "interface tunnel0"
 action 6  cli command "tunnel source Cellular 0/3/0"
 action 7  cli command "exit"
 action 8  cli command "no ip route 0.0.0.0 0.0.0.0 Cellular 0/1/0"
 action 9  cli command "ip route 0.0.0.0 0.0.0.0 Cellular 0/3/0"
 action 10  cli command "end"
 action 99 syslog msg "NOTE: Cellular 0/1/0 down, switching to Cellular 0/3/0"

event manager applet Recovery
 event track 3 state up
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "no ip route 0.0.0.0 0.0.0.0 Cellular 0/3/0"
 action 4  cli command "ip route 0.0.0.0 0.0.0.0 Cellular 0/1/0"
 action 5  cli command "interface cellular 0/3/0"
 action 6  cli command "shutdown"
 action 7  cli command "interface tunnel0"
 action 8  cli command "tunnel source Cellular 0/1/0"
 action 9  cli command "end"
 action 99 syslog msg "NOTE: Connectivity Restored on Cellular 0/1/0"
```

Figure 189 RPoP Dual-LTE (Active/Standby) Failover State

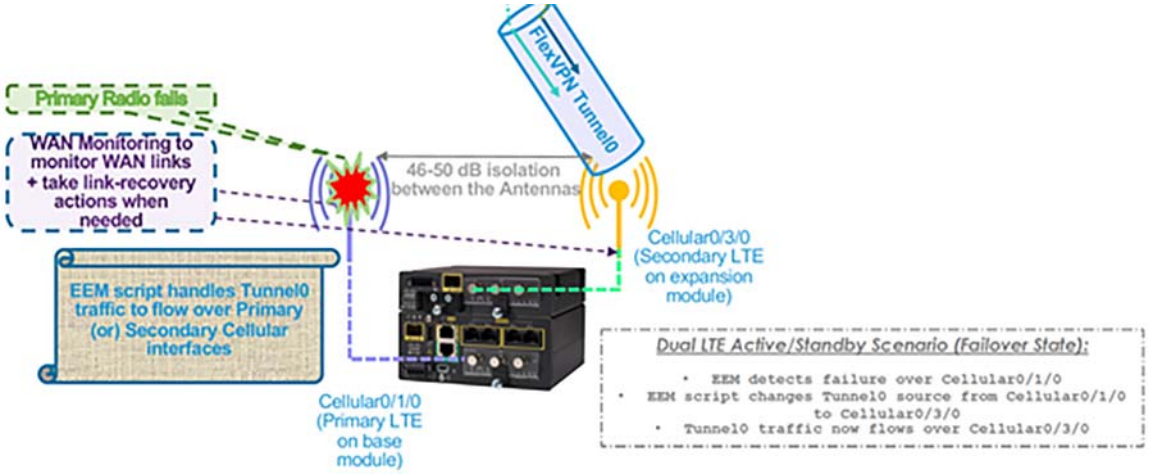
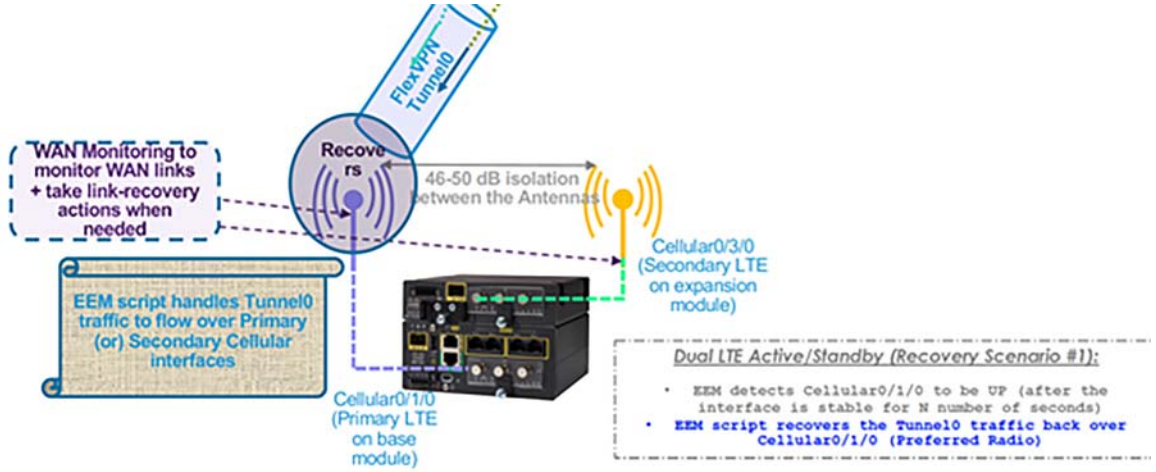


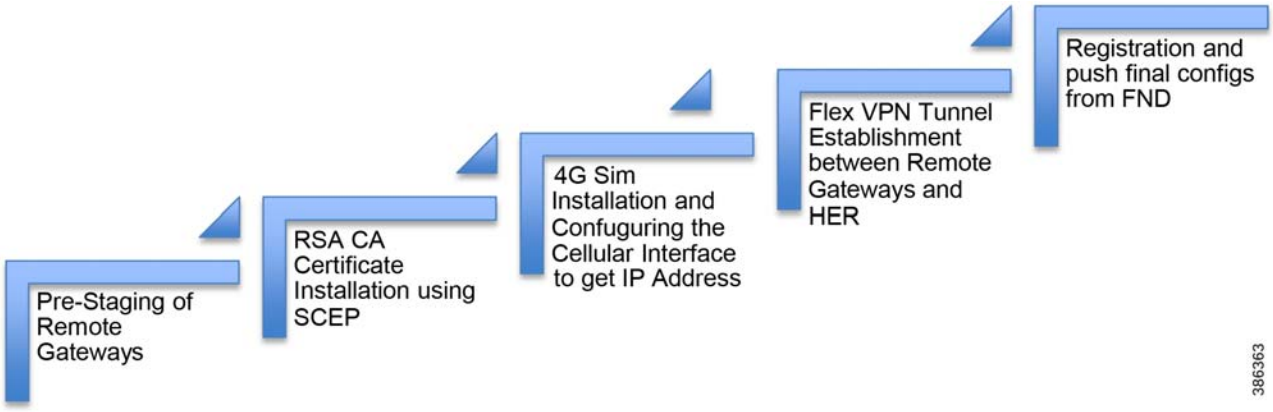
Figure 190 RPoP Dual-LTE (Active/Standby) Recovery State



Implementing RPoP with Cellular Backhaul to CCI Headend

This section provides high level steps to implement Cisco Connected Grid Router (CGR1240) or Industrial Routers (IR8x9/IR1101) as remote gateways for aggregating traffic between RPoPs and to CCI Headend in secure way.

Figure 191 RPoP Implementation Flow



Pre-Staging of Remote Gateways and RSA CA Certificate Installation:

For Pre-staging of Remote Gateways, refer to Secure Onboarding of Field Area Router—CGR1240, page 209 and the subsection Pre-Staging a CGR, page 210 for the required pre-staging of FAR.

4G SIM Installation and Configuring the Cellular Interface to Obtain IP Address

To install the SIM card, consult the following:

Refer to the following hyperlink for installation SIM on IR1101:

- IR1101 SIM installation (requires a pluggable LTE module installed on the gateway)

Refer to the following hyperlink for installation SIM on IR807:

- IR807 SIM installation

Refer to the following hyperlink for installation SIM on IR829:

- IR829 SIM installation

Refer to the following hyperlink for installation SIM on IR809:

- IR809 SIM installation

Refer to the following hyperlink for installation SIM on CGR:

- CGR SIM installation SIM installation

Flex VPN Tunnel Establishment between Remote Gateways and HER

For Secure Communication between Remote Gateways and HER, refer to Secure Onboarding of Field Area Router—CGR1240, page 209 and the subsection Secure Tunnel Establishment, page 213 for the required pre-staging of FAR.

Registration and Push final configs from FND

For FND Registration of Remote Gateways, refer to FAR Registration into FND (NMS), page 214 and Final Configuration Push from FND to CGR, page 217.

Remote PoP with LoRaWAN Access Network

This section covers implementation details on LoRaWAN gateway Remote PoP in standalone mode and virtual mode (behind IR829) while router and gateway being managed by Field Network Director (FND) and radio being managed by ThingPark Enterprise (TPE).

Note: IR1101 and IR829 provide Cellular connectivity to IXM to reach Headend Router. In this scenario, we have used IR 829.

IXM Standalone Mode with IR829 Cellular Backhaul

This section covers the implementation details of an IXM gateway in standalone mode with Ethernet connectivity to an IR829, since this Ethernet connection is not encrypted in this mode, it is strongly recommended that the IXM gateway and the IR829, and the Ethernet connection between them are deployed in a physically secured environment.

Prerequisites:

- LoRaWAN Gateway connected over Ethernet to IR829
- HER configured with VPN (sample HER FlexVPN configuration included in this section)
- IR8x9/IR1101 router with enterprise access through VPN (sample router configuration with FlexVPN included in this section) via Remote PoP.
- ThingPark Enterprise installed along with Application server integration (the installation details are discussed int the LoRaWAN Access Network section).
- FND should be installed.
- USB plugged into IXM with packer forwarder and pubkey.
- Console connection to IXM and IR829 for configuration.

Configuring FlexVPN on HER:

1. Configure hostname (reachable via IP address), secret password, username, and password:

```
hostname rtp
enable secret cisco
username administrator privilege 15 password 0 C1sc0123!
```

2. Configure NTP, time zone, and DNS server:

```
ntp server 10.0.1.1
clock timezone PST -7 0
ip name-server 10.0.1.6
```

3. Generate rsa key with size of 2048:

```
crypto key generate rsa general-keys label rsakey
```

4. Create a trustpoint for installing the certificate:

```
crypto pki trustpoint ca enrollment terminal serial-number none

subject-name serialNumber=PID:ASR1006-X
SN:FXS1950Q3Z8,CN=asr.actility.com,OU=iot,O=actility,L=rtp,St=nc,C=us revocation-check none
rsakeypair rsakey
```

5. Install the certificate from Flash:

```
crypto pki import ca pkcs12 flash:asr.pfx password cisco
```

6. Enable SSH version:

```
ip ssh version 2:
```

7. Create AAA model with authorization and authentication configured locally:

```
aaa new-model
authorization network local-group-author-list local
aaa authentication login default local
```

8. Configure FlexVPN on HER.

Note: TPE subnet is advertised over tunnel to IR829, which assists in the successful communication between IXM and TPE:

```
crypto pki certificate map R1-R2-MAP 1
subject-name co cn = rtp.actility.com

crypto ikev2 authorization policy R1-R2-AUTH-POLICY pool testvpn
netmask 255.255.255.0 route set interface
route set remote ipv4 172.16.3.0 255.255.255.0 route set remote ipv4 10.0.1.0 255.255.255.0

crypto ikev2 profile R1-R2-PROFILE match certificate R1-R2-MAP identity local dn authentication
remote rsa-sig authentication local rsa-sig pki trustpoint ca
aaa authorization group cert list local-group-author-list R1-R2-AUTH-POLICY
virtual-template 2
crypto ipsec transform-set R1-R2-TRANSFORM-SET esp-aes esp-sha256-hmac mode tunnel

crypto ipsec profile R1-R2-IPSEC-PROFILE
set transform-set R1-R2-TRANSFORM-SET
set ikev2-profile R1-R2-PROFILE
interface Virtual-Template2 type tunnel
ip unnumbered Loopback10
tunnel source GigabitEthernet0/0/3
tunnel mode ipsec ipv4
tunnel protection ipsec profile R1-R2-IPSEC-PROFILE
interface Loopback10
ip address 172.16.121.1 255.255.255.0
ip local pool testvpn 172.16.121.2
```

Configuring the Router

1. Configure hostname, secret password, username, and password:

```
hostname rtp
enable secret cisco
username administrator privilege 15 password 0 C1sc0123!
```

2. Configure NTP, time zone, and DNS server:

```
ntp server
10.0.1.1 clock
timezone PST -7 0
ip name-server
10.0.1.6
```

3. Generate RSA key with size of 2048:

```
crypto key generate rsa general-keys label rsakey
```

4. Create a trustpoint for installing the certificate:

```
crypto pki
trustpoint ca
enrollment
```

```
terminal
serial-number none

subject-name serialNumber=PID:IR829G-LTE-NA-K9
SN:FCW2215003P,CN=rtp.actility.com,OU=iot,O=actility,L=rtp,St=nc,C=
us revocation-check none
rsakeypair rsakey
```

5. Install the certificate from Flash:

```
crypto pki import ca pkcs12 flash:rtp.pfx password cisco
```

6. Enable SSH version:

```
ip ssh version 2
```

7. Configure the outside-facing cellular interface to reach HER:

```
interface Cellular0
 description Connection to DMZ UCSB
 ip address negotiated
 encapsulation slip
 dialer in-band
 dialer idle-timeout 0
 dialer string lte
 dialer watch-group 1
 dialer-group 1
 pulse-time 1
 !
ip route 0.0.0.0 0.0.0.0 Cellular0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
```

8. Create AAA model with authorization and authentication configured locally:

```
aaa new-model
aaa authorization network local-group-author-list
local aaa authentication login default local
```

9. Configure FlexVPN on the router and apply to the tunnel interface. Assuming HER is configured for FlexVPN, the tunnel should come up after applying below configuration:

Note: IXM subnet is advertised over the tunnel to HER, which assists in successful communication between IXM and TPE. FlexVPN helps carry data securely between IXM and Data Center and therefore other VPN technologies can be used as a substitute.

```
crypto pki certificate map R1-R2-MAP 1 subject-name co ou = iot
crypto ikev2 authorization policy R1-R2-AUTH-POLICY route set interface
route set remote ipv4 172.16.32.0 255.255.255.248

crypto ikev2 profile R1-R2-PROFILE match certificate R1-R2-MAP identity local dn authentication
remote rsa-sig authentication local rsa-sig pki trustpoint ca
aaa authorization group cert list local-group-author-list R1-R2-AUTH-POLICY
crypto ipsec transform-set R1-R2-TRANSFORM-SET esp-aes esp-sha256-hmac mode tunnel

crypto ipsec profile R1-R2-IPSEC-PROFILE
set transform-set R1-R2-TRANSFORM-SET
set ikev2-profile R1-R2-PROFILE
```

```
interface Tunnel0
ip address negotiated
ip virtual-reassembly in
tunnel source GigabitEthernet0
tunnel mode ipsec ipv4
tunnel destination 172.16.120.1
tunnel protection ipsec profile R1-R2-IPSEC-PROFILE
```

10. Configure local default gateway interface for LoRaWAN on the router:

```
interface gigabitEthernet1
ip address 172.16.32.1 255.255.255.248
ip virtual-reassembly in
no shutdown
exit
```

11. Create a DHCP pool for LoRaWAN to get an IP address:

```
ip dhcp pool modempool
network 172.16.32.0255.255.255.248
default-router 172.16.32.1
dns-server 10.0.1.6
exit

ip dhcp excluded-address 172.16.32.1
ip dhcp excluded-address 172.16.32.3 172.16.32.6
```

12. Configuring NAT for the outside devices to reach the virtual mode IXM

```
ip nat inside source list 1 interface Loopback500 overload

interface Vlan101
ip nat inside

interface tunnel 100
ip nat outside
```

Follow the steps in Implementing LoRaWAN Access Network, page 141 to configure IXM, on-boarding IXM into FND and TPE and to make IXM available to forward traffic.

IXM Virtual Mode Using IR829

This section covers implementation details on LoRaWAN gateway in virtual mode behind IR829 while router and gateway being managed by Field Network Director (FND) and radio being managed by ThingPark Enterprise (TPE).

Prerequisites:

- LoRaWAN Gateway (switched to virtual mode) connected over Ethernet to IR829.
- IR829 router connected to internet via Cellular Interface.
- LRR image, LRR pubkey to upload in FND.
- Head End Router (HER) configured with FlexVPN for tunnel termination from IR829.
- ThingPark Enterprise installed along with Application server integration (the installation details are discussed in Implementing LoRaWAN Access Network, page 141.
- FND is installed.
- IR829 flash loaded with lrr.ini and credentials.txt files customized for accessing TPE. “lrr.ini” file is updated with TPE address whereas “credentials.txt” file is updated with credentials to access the router/gateway. Note: This is not mandatory but can be used to manage custom files through FND.

Virtual Mode (Behind IR829):

credentials.txt:

```
administrator
CXXXXXXXXXX
```

lrr.ini:

```
    ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;LRR custom configuration for TPE IAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

[trace]
          level=0

[suplog]
    nfr920=0
networkconfigtpe=1
networkconfigvpnfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/vpn.cfg
networkconfiginterfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/interfaces.config
networkconfigntpfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/ntp.conf

[services]
  checkvpn2=0
  ipfailover=0

[ifacefailover]
    enable=0

[lrr]
    nblrc=1
uidmode=fromtwaonly
usegpstime=0

[laplrc:0]
addr=tpe-cci.actility.local
port=2404
    type=${LK_TCP_CLIENT}|${LK_SSP_SLAVE}|${LK_SSP_RECONN}|${LK_TCP_NONBLK}
    iec104t1=60

[support:0]
;ssh parameters
; Address is configurable via suplog menu
addr=xxx
user=support
pass=[2ca6e5f79a74b74382bc2eeebb21085b]
pass_crypted_k=0
port=22
;ftp parameters
ftpaddr=172.16.3.2
ftpuser=ftp-support
ftppass=[791551405f8f938548a7d4cef3ccf779]
ftpport=21
use_sftp=0


[download:0]
           ftpaddr=172.16.3.2
           ftpuser=ftp-lrc
           ftppass=[558d3b006f639a810bbb8e33caa6a769]
           ftpport=21
           use_sftp=0
```

```
[versions]
            hardware_version=
           os_version=
           custom_build_version=
            configuration_version=
```

On-boarding of IXM Gateway and IR 829 into FND

Preparing CSV:

Prepare a CSV file with “eid”, “deviceType”, “adminUsername” and “adminPassword” fields for router to be successfully registered to FND.

Note: We prepare the CSV with IR829 details only and not LoRaWAN gateway.

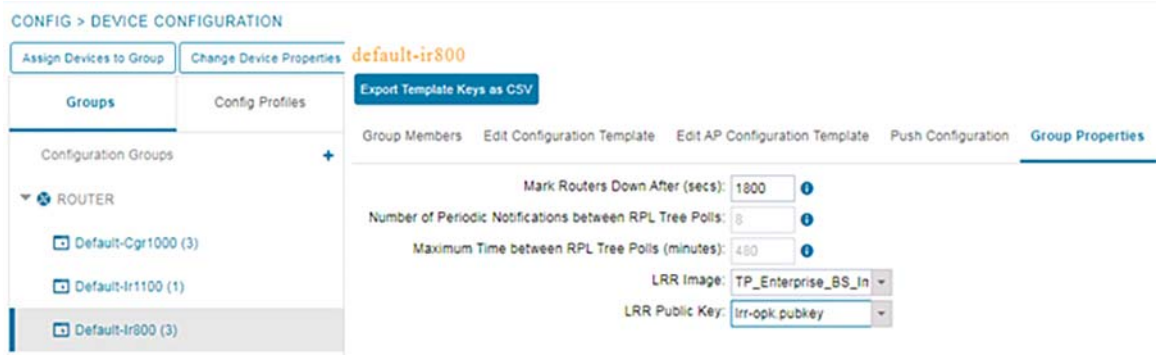
Fields description mentioned below:

- eid: Combination of PID and serial number from the router
- deviceType: type of the device
- adminUsername: username configured to access the router with privilege 15
- adminPassword: password configured to access the router with privilege 15

Pre-staging FND:

- The csv which we generate in the above section will be uploaded into FND. Go to FND UI, Click **Devices**-> **Field Devices**-> **Add Devices** and upload the csv file.
- Upload the **LRR packet forwarder** and **pubkey** to FND through **Config**-> **Device File Management.**
- Assign the **LRR packet forwarder** and **pubkey** to the template.
- At this point pre-staging is done for registering the IR829 router and LoRaWAN Gateway.

Figure 192 On IR829 Selecting LRR Image and LRR Public Key in Group Properties Page



Configuring the IR829 Router:

For configuring IR829 router, consult the following:

1. Refer to the following guide to provide cellular connectivity to IR829:
   - https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_cellular.html

2. For SCEP Enrollment and Flex VPN tunnel-based configuration, refer to Secure Onboarding of Field Area Router—CGR1240, page 209 and the subsections CGR Interface Configuration, page 210 and Pre-Staging a CGR, page 210.
3. After this step, we can able to establish secure communication via FlexVPN between HER (Head End Router) and IR829.
4. For WSMA, HTTP, EEM, and CGNA profiles, refer to Final Configuration Push from FND to CGR, page 217.
5. After this step, user can register IR829 with FND.
6. To enroll IXM Gateway, CGNA LPWA register profile needs to be pushed into the IR829 device.

```
!
cgna profile cg-nms-lpwa-register
 add-command show virtual-lpwa 1 modem status | format flash:/managed/odm/cg-nms.odm
 add-command show virtual-lpwa 1 packet-forwarder info | format flash:/managed/odm/cg-nms.odm
 add-command show virtual-lpwa 1 packet-forwarder status | format flash:/managed/odm/cg-nms.odm
 add-command show virtual-lpwa 1 modem statistics | format flash:/managed/odm/cg-nms.odm
 add-command show virtual-lpwa 1 modem info | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://cci-iot-fnd.cimconccibgl.cisco.com:9121/cgna/ios/lpwa
 gzip
!
```


Switching to Virtual Mode

User can use the switchover EXEC command to switch to the virtual mode. Once the IXM is switched over to virtual mode, user need to have an IR829 to bring it back to standalone mode.

Note: Use this command, if you are fully aware of your environment and confident of switching over and managing it via IR8x9.

```
Gateway#switchover
```

Configuring Virtual-LPWA Interface on the IR800 Series

The Cisco LoRaWAN Gateway is connected to IR800 series via an Ethernet cable with PoE+ to work as a LoRaWAN gateway. By creating a VLPWA interface on the IR800 series, user can:

- Manage hardware and software of the Cisco LoRaWAN Gateway.
- Send and receive VLPWA protocol modem message to monitor the status of the Cisco LoRaWAN Gateway.
- Send SNMP traps to the IoT Field Network Director (IoT FND).

Note: Cisco IOS Release 15.6(3)M or later is required for the IR800 series to manage the Cisco LoRaWAN Gateway.

Note: User need to install the Actility Thingpark LRR software as the LoRa forwarder firmware, which is loaded through the Cisco IOS software, for the Cisco LoRaWAN Gateway to work (discussed in later sections).

Refer to the following URL for more details:

- https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_vlpwa.html

Configuring Ethernet Interface and Creating VLPWA Interface

When user configure IP address for the Vlan interface, the IP address allocated must be aligned with the prefix configured for the DHCP pool allocated to the LoRaWAN interface. The Cisco LoRaWAN Gateway communicates through IOS, therefore a private IPv4 address is assigned with NAT being configured.

Configuring IR829

Each LoRaWAN gateway or virtual-lpwa must be isolated in a dedicated VLAN. If you put it in a VLAN shared with other devices, it may cause the virtual-lpwa interface not being operational. Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR829 and create the VLPWA interface.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface vlan vlan-id	Configures the vlan interface. Note: The VLAN ID can be different from the vlpwa ID.
Step 3	ip address address mask	Configures the vlan interface IP address. Note: IP address should be default router address in its associated DHCP pool.
Step 4	exit	Exits to global configuration mode.
Step 5	interface gigabitEthernet ID	Configures the Gigabit Ethernet port.
Step 6	switchport mode access	Sets trunking mode to ACCESS on the given port.
Step 7	switchport access vlan ID	Sets VLAN when interface is in access mode.
Step 8	exit	Exits to global configuration mode.
Step 9	interface Virtual-LPWA vlpwa-id	Creates VLPWA interface. Note: The value of vlpwa-id should be the same as the option 43 hex number which is specified in DHCP pool. See the DHCP section.
Step 10	end	Exits to privileged EXEC mode.
Step 11	write memory	Saves the configurations.

The following is an example on IR829 using the VLAN method:

```
<#----Define DHCP Pool for LoRa Modem----#>
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.3 192.168.1.6
!
ip dhcp pool modempool1
 network 192.168.1.0 255.255.255.248
 default-router 192.168.1.1
 option 43 hex
!
interface Virtual-LPWA1
 no shutdown
 lpwa modem environment PKTFWD_ROOT /tmp/mdm/pktfwd/firmware
```

```
 lpwa modem environment LXC_STORE_PATH /tmp/mdm/pktfwd/firmware/usr/etc/lrr
 lpwa modem password root admin
 lpwa modem ntp server address 10.40.100.100
!
interface GigabitEthernet1
 switchport access vlan 101
!
interface Vlan101
 ip address 192.168.1.1 255.255.255.248
!
end
!
```

Monitoring the LoRaWAN Gateway

The following commands indicate LPWA status:

```
*Jan 19 12:39:34.409: %LINK-3-UPDOWN: Interface Virtual-LPWA1, changed state to up
*Jan 19 12:39:35.409: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-LPWA1, changed state
to down
*Jan 19 12:39:35.537: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up
*Jan 19 12:40:21.575: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to
save new IOS PKI configuration
*Jan 19 12:40:22.567: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-LPWA1, changed state
to up
```

On the IR800 series, beginning in privileged EXEC mode, use these commands to monitor the Cisco LoRaWAN Gateway

```
IR800#show virtual-lpwa 1 modem info (Displays modem information.)
Name : Virtual-LPWA 1
ModemImageVer : 2.0.32
BootloaderVer : 20180130_cisco
ModemAgentVer : 1.02
SerialNumber : FOC23318QFA
PID : IXM-LPWA-800-16-K9
UTCTime : 23:39:51.330 UTC Wed Aug 24 2016
IPv4Address : 192.168.1.2
IPv6Address : none
FPGAVersion : 61
TimeZone : UTC
LocalTime : Wed Aug 24 23:39:51 UTC 2016
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x30690b06 MSB = 0x00f14200
LoRaSerialNumber : FOC232939DA
LoRaCalc :
<141,129,121,113,105,101,97,93,84,75,66,57,48,43,39,35-144,131,123,115,107,103,99,95,86,78,69,61,52
,48,44,40>
CalTempCelsius : 41
CalTempCodeAD9361 : 98
RSSIOffset : -202.72,-203.00
AESKey : Unknown

IR800#show virtual-lpwa 1 modem status (Displays modem status.)

Name : Virtual-LPWA 1
Status : Running
Uptime : 1:00:32.040000
Door : DoorClose
Upgrade Status : Ready
```

FND Registration of IXM

We need to trigger registration request for lpwa profile manually to register IXM Gateway:

```
IR829_FGL194520VV#cgna exec profile cg-nms-lpwa register
```

After registration IR 829 will appear on FND as shown below:.

Figure 193 IXM Registration Message on IXM Events Page

Figure 194 IXM Status after Registration on FND

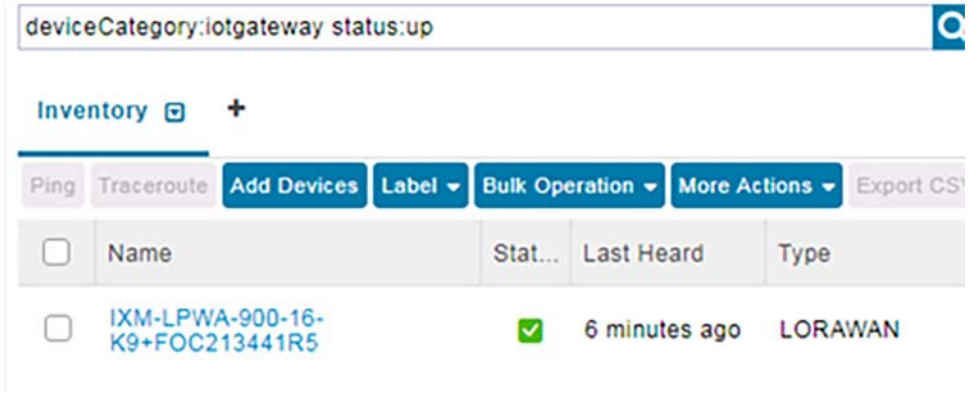


Figure 195 IXM Device as a Sub-device along with IR829

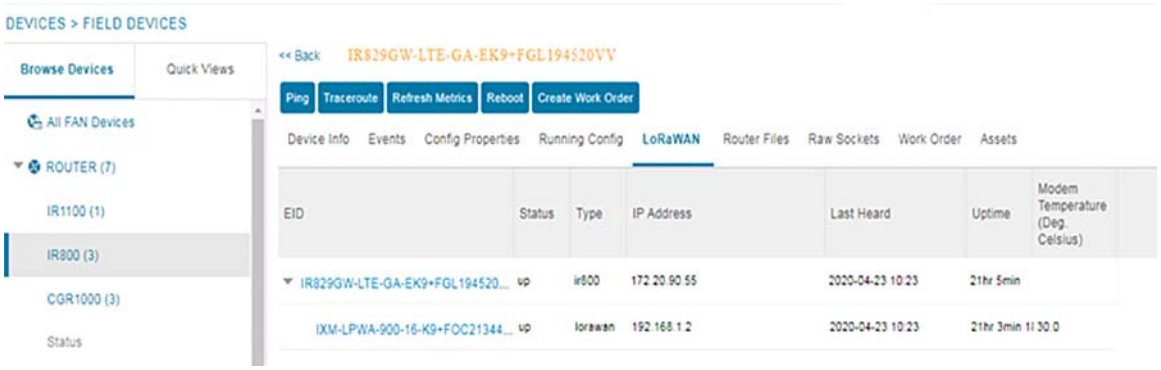
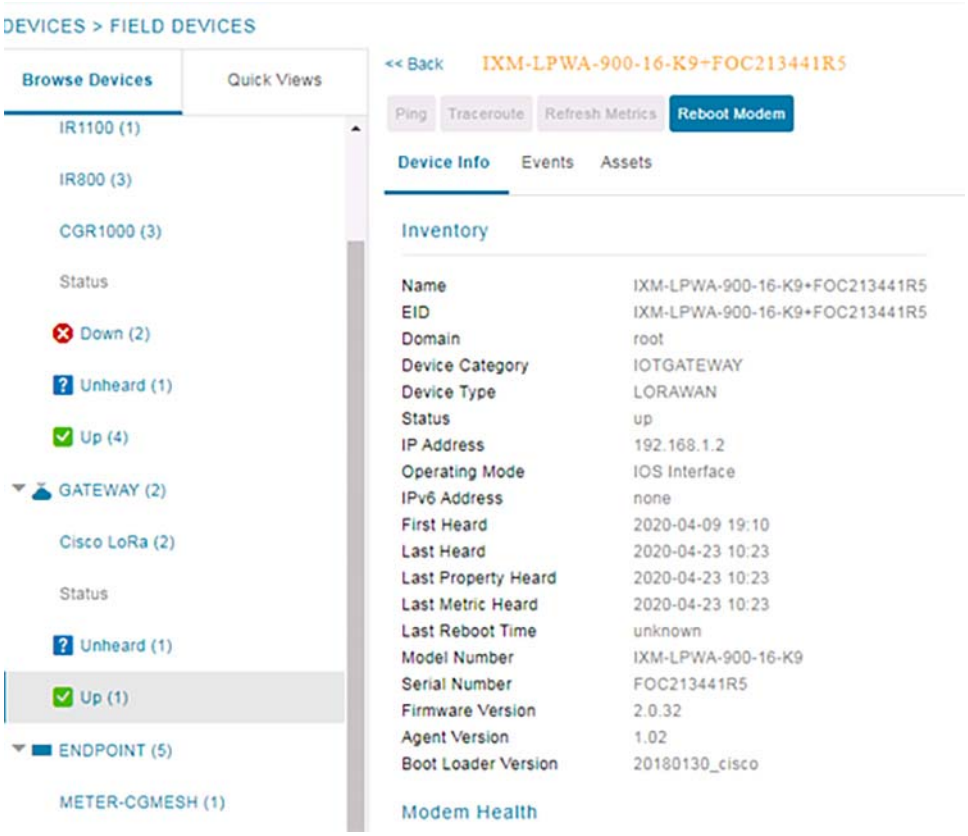


Figure 196 IXM Dashboard View in FND



Connecting to TPE

Pre-staging for IXM-TPE Connectivity

The prerequisites for TPE connectivity are:

- Installing LRR image and LRR Public Key on IXM Gateway
- Two files ‘credentials.txt’ and ‘lrr.ini’ have to be pushed to IXM Gateway

These two files have to be pushed onto the IXM Gateway in one of the two ways:

- Copying the files to IXM using **Configuration Template** in FND
- By custom file management

A sample of the two files namely credentials.txt and lrr.ini are shown below. Unlike standalone mode the credentials.txt file here will use the enable password, username and password of IR829 instead of IXM (refer to the section Implementing LoRaWAN Access Network, page 141 for details about these two files).

credentials.txt:

```
administrator
XXXXXXX
```

lrr.ini:

```
        ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;LRR custom configuration for TPE IAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

[trace]
          level=0

[suplog]
    nfr920=0
networkconfigtpe=1
networkconfigvpnfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/vpn.cfg
networkconfiginterfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/interfaces.config
networkconfigntpfile=/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/ntp.conf

[services]
  checkvpn2=0
  ipfailover=0

[ifacefailover]
    enable=0

[lrr]
    nblrc=1
uidmode=fromtwaonly
usegpstime=0

[laplrc:0]
addr=tpe-cci.actility.local
port=2404
    type=${LK_TCP_CLIENT}|${LK_SSP_SLAVE}|${LK_SSP_RECONN}|${LK_TCP_NONBLK}
    iec104t1=60

[support:0]
;ssh parameters
; Address is configurable via suplog menu
addr=xxx
user=support
pass=[2ca6e5f79a74b74382bc2eeebb21085b]
pass_crypted_k=0
port=22
;ftp parameters
ftpaddr=172.16.3.2
ftpuser=ftp-support
ftppass=[791551405f8f938548a7d4cef3ccf779]
ftpport=21
use_sftp=0

[download:0]
           ftpaddr=172.16.3.2
           ftpuser=ftp-lrc
           ftppass=[558d3b006f639a810bbb8e33caa6a769]
           ftpport=21
           use_sftp=0

[versions]
            hardware_version=
           os_version=
           custom_build_version=
            configuration_version=
```

Using Configuration Template in FND

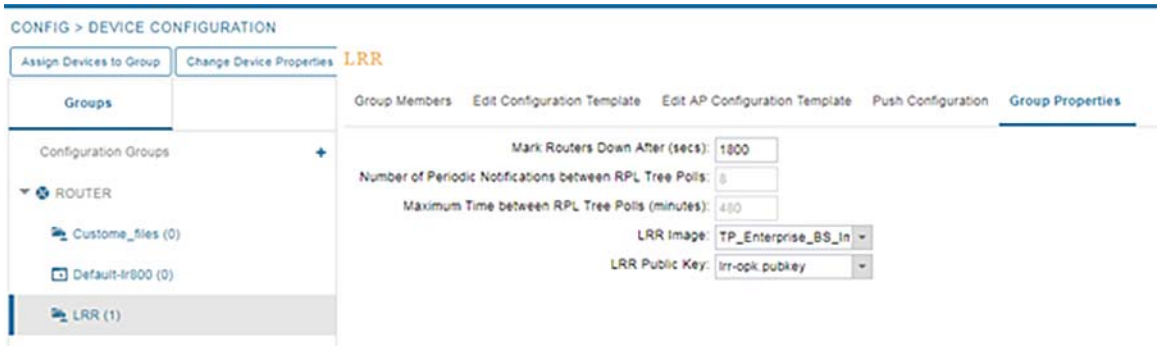
After the IXM and IR829 is registered to FND, go to FND UI and create two templates under **Config -> Device Configuration** for:

- Installing LRR image and LRR Public Key
- Uploading custom files to IXM.

For uploading and installing LRR Packet forwarder Image and LRR Public key into IXM (Template 1).

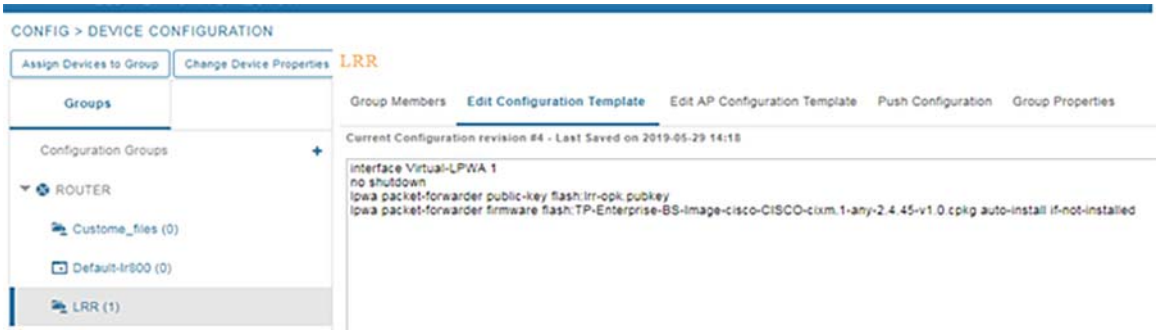
1. Go to **Config->Device Configuration,** select **IR Gateway Group** (on the left pane), select **Group properties**, and select **LRR Image** and **LRR Public Key** from the drop-down menu as shown in Figure 197.

Figure 197 LRR forwarder Image and LRR Public Key Upload



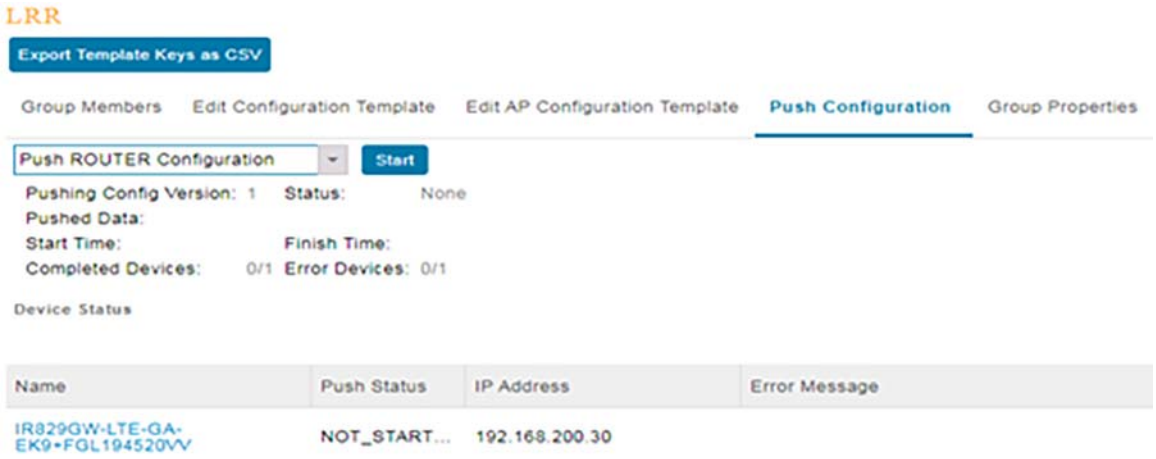
2. For installing the **LRR Packet forwarder Image** and **LRR Public key**, user need to edit the configuration as shown below**.**

Figure 198 LRR forwarder Image and LRR Public Key Configuration Template



3. Push the configuration as shown below, which will install the **LRR Packet forwarder Image** and **LRR Public key.**

Figure 199 LRR forwarder Image and LRR Public Key Configuration Push

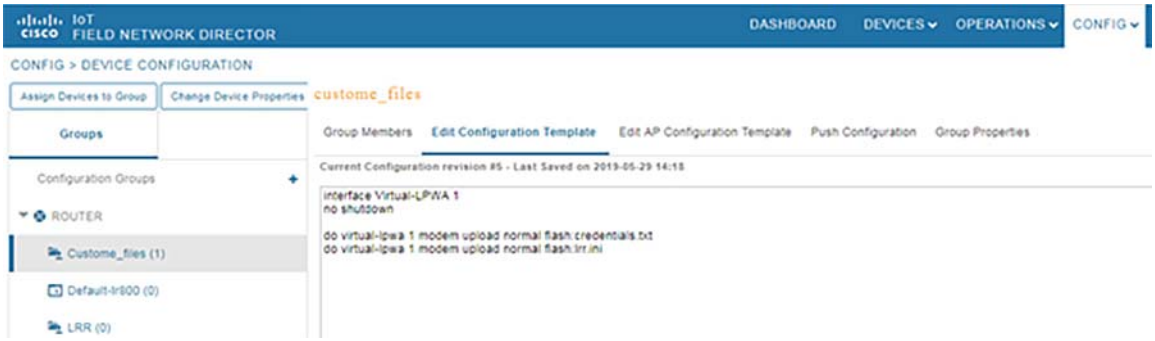


For uploading lrr.ini and credentials.txt files into IXM Gateway:

1. Follow the step below only if “lrr.ini” and “credentials.txt” files are loaded in USB. Otherwise, refer to “Custom file management” section. To upload the custom files to gateway, change the router to custom files template and push the configuration.

   a. Go to **Config->Device Configuration**, select **IR Gateway Group** (on the left pane), select **Edit Configuration Template**, and select the configuration Template as show in Figure 200.

Figure 200 lrr.ini and credentials.txt Configuration Template



   b. Go to Push Configuration tab and select **Push Router Configuration** dropdown and select Device. Select Start which will push the configuration to IR device as shown below.

   c. This will push the commands to IR device, in which the “lrr.ini” and “credentials.txt” are loaded into IXM.

Custom File Management:

Follow this section if FND is not used for uploading custom files; otherwise, refer to Installing and Configuring TPE, page 142.

1. Using console, login to the IXM using root and password set under virtual-LPWA interface.
2. Go to the directory “/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr/” and edit the files “credentials.txt” and “lrr.ini” with gateway credentials and TPE address. (as discussed in Prerequisites)

Debugging the LoRaWAN Gateway

Refer to the following link for debugging:

- https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_vlpwa.html

Cisco Wireless Gateway for LoRaWAN Software Configuration Guide

- https://www.cisco.com/c/en/us/td/docs/routers/interface-module-lorawan/software/configuration/guide/b_lora_scg/b_lora_scg_chapter_01010.html

For more reference commands:

- https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_vlpwa.html

Remote PoP with CR-Mesh over Cellular Network Backhaul

This section provides implementation details of Cisco Connected Grid Router (CGR1240) aggregating traffic to CCI Headend in secure way using Cellular Network Backhaul.

Installation of 4G-LTE Module in CGR

The installation steps for an LTE module in CGR are provided below:

1. SIM Selection and Importance of Lights

- https://www.cisco.co/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/modules/4g_lte/b_4g_cgr1000.html

2. Antenna Selection for CGR:

The antenna used is ANT-4G-OMNI-OUT-N Outdoor omnidirectional stick antenna for 2G/3G/4G Cellular CGR 1240, 1120, 2010

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing/cg_antenna_install_guide/Overview.pdf

3. 4G SIM Installation:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/modules/4g_lte/b_4g_cgr1000.ht ml

Configuration of Cellular Interface (4G LTE Module)

Prerequisites

To configure the 4G LTE module, you must meet the following requirements:

- Have 4G LTE network coverage where your router will be physically located. For a complete list of supported carriers, see the product data sheet.
- Subscribe to a service plan with a wireless service provider and obtain a SIM card.
- Contact your ISP and get your access point name (APN).
- Install the SIM card before configuring the 4G LTE module.

Guidelines and Limitations

The following guidelines and limitations apply to configuring the 4G LTE module:

- Global Positioning System (GPS) and Short Message Service (SMS) are not supported.
- Data connection can be originated only by the module.

- Throughput: Due to the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or congestion in a given network.
- Cellular networks have higher latency compared to wired networks. Latency rates depend on the technology and carrier. Latency may be higher because of network congestion.
- Any restrictions that are a part of the terms of service from your carrier.
- The 4G LTE module can be plugged into slots 3 or 6 of Cisco 1240 Connected Grid Router. Therefore, the interface names used to configure the module can be 3/1 or 6/1.
- The 4G LTE module can be plugged into slots 3 or 4 of Cisco 1120 Connected Grid Router. Therefore, the interface names used to configure the module can be 3/1 or 4/1.
- CGM-4G-LTE-MNA is not compatible with CGR 1120, CGM-4G-LTE-MNA-AB is compatible with both platforms.

Configuring the Cellular Interface

To obtain the Dynamic IP Address use the following configuration:

```
<snip>
!
interface Cellular3/1
description Connection to DMZ UCSB
ip address negotiated
encapsulation slip
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer watch-group 1
dialer-group 1
ipv6 address autoconfig
ipv6 enable
pulse-time 1
end
!
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ip route 0.0.0.0 0.0.0.0 cellular 3/1
script dialer lte
!
!controller Cellular 0/1/0
!lte sim data-profile 1 attach-profile 1 slot 0
!
</snip>
```

For detailed information about 4G-LTE configuration for CGR Interface, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/modules/4g_lte/b_4g_cgr1000.html

Debugs on CGR after Successfully Obtaining IP Address

```
Jun 11 10:39:21.781: %CELLWAN-2-BEARER_UP: Instance id=0, Default bearer (bearer_id=5) in
Cellular3/1 is now UPdo
Jun 11 10:39:24.066: %LINK-3-UPDOWN: Interface Cellular3/1, changed state to up
Jun 11 10:39:25.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular3/1, changed state to
up
```

Pre-staging and CGR Onboarding

For pre-staging and CGR onboarding in a remote PoP site, refer to Secure Onboarding of Field Area Router (CGR1240), page 108.

Remote PoP with Digital Subscriber Line (DSL) Backhaul

This section describes the implementation of the RPoP IR1101 with the DSL modem (DSL SFP-VADSL2+-I) to connect to the CCI Headend via DSL backhaul.

Asymmetric Digital Subscriber Line (ADSL) Backhaul

The IR1101 Router DSL SFP-VADSL2+-I provides Annex A support on ADSL2+. Annex A and reach-extended Annex L mode-1 is supported on ADSL2. This setup complies with TR-100/TR-105. ADSL2/2+ works in auto mode; the configuration on DSLAM auto-negotiates automatically with the DSL controller.

- For Auto-negotiation handshake procedure, the SFP is compliant with ITU-T G.994.1 DSL TRx and for the Physical Layer Management is compliant with ITU-T G.997.1 for DSL TRx.
- The DSL SFP complies with the ITU-T G.99x standard, supporting AVD2 CPE mode only.
- The router supports LLC/SNAP and the VCMux ethernet-bridged encapsulation option.
- All PPPoX encapsulation is configured via PPPoE only. Internally, packet translation is handled via ATM. There is no PPPoA configuration like there is with the c111x ISR.
- ADSL-PVC is configurable in the Controller VDSL 0/0/0: Each SFP supports 8 PVCs.
- Each PVC supports mapping to/from 802.1q Vlan tagging.
- VPI range is 0-255, VCI range is 32-65535.

The 'mode' reflected in **show controller vdsl 0/0/0** will always be PTM (Packet transfer mode). Internally packet translation to ATM is handled (AAL5).

Configuring ADSL2/2+

The router supports Asymmetric Digital Subscriber Line (ADSL) 2/2+. For configuration and display commands, see the detailed sections below. The **show controller vdsl 0/0/0** is the fundamental command for validation. The ADSL2/2+ works in auto mode (the configuration on DSLAM auto-negotiates automatically with the DSL controller). Operation mode on the IR1101 controller cannot be configured to specific xDSL protocol.

- Annex A is supported on ADSL2+. Both Annex A and reach-extended Annex L mode-1 is supported on ADSL2. This complies with TR-100/TR-105.
- For Auto-negotiation handshake procedure, the SFP is compliant with ITU-T G.994.1
- The DSL TRx is Physical Layer Management compliant with ITU-T G.997.1 for DSL TRx.
- The DSL SFP complies with the ITU-T G.99x standard, supporting AVD2 CPE mode only. It also supports the LLC/SNAP and VCMux ethernet bridged encapsulation option.
- All PPPoX encapsulation is configured via PPPoE only. Internally, packet translation is handled using ATM. There is no PPPoA configuration like there is with the c111x ISR.
- VPI range is 0-255, VCI range is 32-65535.The 'mode' reflected in show controller vdsl 0/0/0 will always be PTM (Packet transfer mode). Internally packet translation to ATM is handled (AAL5).
- ADSL-PVC is configurable in the Controller VDSL 0/0/0:
  - Each SFP supports 8 PVCs.

- Each PVC supports mapping to/from 802.1q VLAN tagging.

Step 1: Upgrade the IR1101 to the latest Image.

```
ADSL-DSL-1101#show controllers vdsl 0/0/0

Controller VDSL 0/0/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'META'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x9162
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'META'                   '    '
Modem Vendor Specific:  0x0000                   0x0000
Modem Vendor Country:   0xB500                   0x0000
Serial Number Near:     EA0462D1B001V5311TR 1_62_8463
Serial Number Far:
Modem Version Near:     1_62_8463 MT5311
Modem Version Far:
Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.992.3 (ADSL2) Annex A
TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running
Failed full inits:      0

Short inits:            0
Failed short inits:     0

Modem FW  Version:
Modem PHY Version:
Modem PHY Source:       System
Line 0:
                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     enabled                 enabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          0                       0
Line Attenuation:         9.6 dB                 dB
Signal Attenuation:      22.0 dB                 32.0 dB
Noise Margin:            28.3 dB                 6.9 dB
Attainable Rate:        11568 kbits/s            778 kbits/s
Actual Power:            0.0 dBm                12.2 dBm
Total FECC:             0                        96876
Total ES:               0                        1789
Total SES:              0                        1
Total LOSS:             0                        1
Total UAS:              2267                     331364
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA            2048            NA               508
SRA Previous Speed:        NA               0            NA                 0
Previous Speed:            NA            2048            NA               508
Reed-Solomon EC:           NA               0            NA                 0
```

```
CRC Errors:                NA            1838            NA                 0
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA            1.00            NA              4.00
Actual INP:                NA            0.00            NA              2.60

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

ADSL-DSL-1101#show controllers vdsl 0/0/0 local

```
SFP Vendor PID:                 SFPV5311TR
SFP Vendor SN:                  MET20240016
Firmware embedded in IOS-XE:    1_62_8463
Running Firmware Version:       1_62_8463
Management Link:                up
DSL Status:                     showtime
Dumping internal info:          idle
Dying Gasp:                     armed


Step 2: CPE Configuration
```

IR1101 CPE Peer Configuration:

1. Configure the PVC VPI and VCI parameters.

```
controller VDSL 0/0/0
adsl-pvc 0/33
  bridge-dot1q 1
  encapsulation llcsnap
  default-pvc
!
interface GigabitEthernet0/0/0
no ip address
media-type sfp
!
```

2. Configuring the Gigabit Ethernet Interface and enabling PPPoE

```
interface GigabitEthernet0/0/0.1
encapsulation dot1Q 1
pppoe enable group global
pppoe-client dial-pool-number 1
!
```

3. Dialer Configuration to get IP Address from BRAS

```
interface Dialer1
ip address negotiated
no ip redirects
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname dslpeer
ppp chap password 0 dslpeerpass
ppp ipcp route default
!
```

BRAS Configuration

In CCI, the ISR acts as the PPPoE Server and the IR1101 can be configured as a PPPoE client, so that a tunnel can be established for the IR1101 to PPPoE Server for the WAN access. At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication Protocol (PAP). After the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Note: PPPoE combines Ethernet and PPP to provide an authenticated method of assigning IP addresses to client systems. The ISR is configured as a DHCP server which provides an IP address to PPPoE clients after successful authentication.

Prerequisite:

The user must have an enabled license on the BRAS Router.

```
license udi pid ISR4451-X/K9 sn FOC24221T1Y
license accept end user agreement
license boot level appxk9
license boot level uck9
license boot level securityk9
diagnostic bootup level minimal
spanning-tree extend system-id

ip dhcp excluded-address 42.42.42.1 42.42.42.9
!
username dslpeer password 0 dslpeerpass
!
ip dhcp pool 42-42-42-pool
 network 42.42.42.0 255.255.255.0
 default-router 42.42.42.1•
 lease infinite
!
```

Create a broadband Group:

```
bba-group pppoe global
 virtual-template 1
!
interface GigabitEthernet0/0/0
 ip address 42.42.42.1 255.255.255.0
 load-interval 30
 negotiation auto
 pppoe enable group global
 arp timeout 10
!
interface GigabitEthernet0/0/0.1
 pppoe enable group global
!
```

After configuring the broadband group, virtual-access is created automatically. Then the virtual template must be created.

Interface configuration and username configuration:

```
interface Virtual-Template1
 ip unnumbered GigabitEthernet0/0/0
 peer default ip address dhcp-pool 42-42-42-pool
 keepalive 30
ppp authentication chap pap
```

For Authenticated Users, an IP Addresses is provided, the dhcp pool (42-42-42-pool) which we have created earlier will be linked here:

```
BRAS-Router-ADSL(config-subif)#interface Virtual-Template1
BRAS-Router-ADSL(config-if)# ip unnumbered GigabitEthernet0/0/0
BRAS-Router-ADSL(config-if)# peer default ip address dhcp-pool 42-42-42-pool
BRAS-Router-ADSL(config-if)# keepalive 30
BRAS-Router-ADSL(config-if)# ppp authentication chap pap
*Dec 15 10:24:39.486: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
```

Add the relevant routes, the next hop is the IP that the IR1101 Dialer acquires:

```
!
ip route 10.0.0.0 255.255.255.0 42.42.42.3 >> dialer ip, change as necessary
```

IR1101 Configuration:

ADSL-DSL-1101#show run | sec controller

```
controller VDSL 0/0/0
 adsl-pvc 0/33
  bridge-dot1q 1
  encapsulation llcsnap
  default-pvc
```

ADSL-DSL-1101#show run int gi0/0/0

```
interface GigabitEthernet0/0/0
 no ip address
 media-type sfp
end
```

ADSL-DSL-1101#show run int gi0/0/0.1

```
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 pppoe enable group global
 pppoe-client dial-pool-number 1
end
```

ADSL-DSL-1101#show run int dialer1

```
interface Dialer1
 ip address negotiated
 no ip redirects
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dslpeer
 ppp chap password 0 dslpeerpass
 ppp ipcp route default
end
```

BRAS Configuration:

BRAS-Router-ADSL#show run | inc lic

```
license udi pid ISR4451-X/K9 sn FOC24221SXQ
license accept end user agreement
license boot level appxk9
license boot level uck9
license boot level securityk9
```

BRAS-Router-ADSL#show ip int brief | inc up

```
GigabitEthernet0/0/0   unassigned      YES TFTP   up                    up
GigabitEthernet0/0/0.1 42.42.42.1      YES manual up                    up
GigabitEthernet0/0/3   unassigned      YES NVRAM  up                    up
```

BRAS-Router-ADSL#show run | sec dhcp

```
ip dhcp excluded-address 42.42.42.1 42.42.42.9
ip dhcp pool 42-42-42-pool
 network 42.42.42.0 255.255.255.0
 default-router 42.42.42.1
 lease infinite
```

BRAS-Router-ADSL#show run | inc username

```
username dslpeer password 0 dslpeerpass
BRAS-Router-ADSL#
```

BRAS-Router-ADSL#show run | sec bba

```
bba-group pppoe global
 virtual-template 1
```

BRAS-Router-ADSL#show run int gi 0/0/0

```
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
end
```

BRAS-Router-ADSL#show run int gi 0/0/0.1

```
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 ip address 42.42.42.1 255.255.255.0
 pppoe enable group global
 arp timeout 10
end
```

BRAS-Router-ADSL#show run int virtual-template 1

```
interface Virtual-Template1
 ip unnumbered GigabitEthernet0/0/0.1
 peer default ip address dhcp-pool 42-42-42-pool
 no keepalive
 ppp authentication chap pap
end
```

Flex VPN Spoke:

```
ADSL-DSL-1101(config)#
int lo0
ip address 192.168.200.20 255.255.255.255
no shut
!
*Dec 22 08:16:13.345: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
!
crypto ikev2 keyring KEYRING
 peer ANY-PEER
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco1234
  pre-shared-key remote cisco1234
 !


 aaa new-model
!
aaa authorization network FLEX_LOCAL local
!
ip domain name CCI.COM
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
crypto ikev2 profile IKEV2_PROFILE
 match identity remote fqdn domain CCI.COM
 identity local fqdn ADSL-DSL-1101.CCI.COM
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list FLEX_LOCAL FlexVPN_Author_Policy
!

crypto ipsec profile IPSEC_PROFILE
 set ikev2-profile IKEV2_PROFILE
```

Very high-speed Digital Subscriber Line (VDSL2) Backhaul

The IR1101 Router DSL SFP-VADSL2+-I provides VDSL2 Annex A and B support conforming to ITU-T standards G.993.2 (VDSL2). This xDSL SFP also complies with TR-114 (VDSL2 Annex A and B performance) and TR-115 (VDSL2 Feature validation tests by University of New Hampshire). The SFP complies with ITU-T G.99x standard with supporting AVD2 CP Emode only.

- Configurable Band Plan, conforms to North America Annex A (G.998) and Europe Annex B (G.997, 998) Band Plans subject to the 3072/4096 and 8-band/4-passband constraints.
- Supports all VDSL2 profiles (8a/b/c/d, 12a/b, 17a, 30a).
- Supports EU type Upstream Band 0 (US0).
- Complies with ITU-T G.994.1 Handshake Procedure for DSL TRx.
- Complies with ITU-T G.997.1 Physical Layer Management for DSL TRx
- Complies with ITU-T G.993.5 Self-FEXT Cancellation (Vectoring) for CPE mode
- Supports Robust Overhead Channel (ROC)
- Supports Online Reconfiguration (OLR) including Seamless Rate Adaptation (SRA) with D/L change and Bit Swapping

- Supports Upstream /Downstream Power Back Off (UPBO/DPBO)
- Supports DELT.
- Supported maximum MTU size on VDSL2 is 1800 Bytes
- Standard compliance VDSL2 mode is PTM (Packet transfer mode)
- Supports VDSL2 Vectoring

Configuring the IR1101 VDSL2 and BRAS Router

For configuration and display commands, see the detailed sections below. The **show controller vdsl 0/0/0** is the fundamental command for validation.

```
router# configure terminal
router(config-controller)# controller vdsl 0/0/0
router(config-controller)# carrier-set a43|a43c|b43
router(config-controller)# end
```

In the CCI environment, ISR acts as a PPPoE Server and the IR1101 can be configured as a PPPoE client, so that a tunnel can be established for the IR1101 to PPPoE Server for WAN access. At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Note: PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. ISR is configured as a DHCP server which provides IP address to PPPoE clients after successful authentication.

```
IR1101 Configuration:
interface Dialer1
 mtu 1492
 ip address negotiated
 no ip redirects
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname dslpeer
 ppp chap password 0 dslpeerpass
 ppp ipcp route default
end
!
```

Configuring the Gigabit Ethernet Interface and enabling PPPoE

```
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native

 pppoe enable group global
 pppoe-client dial-pool-number 1
end
```

ISR BRAS Configuration (PPPoE Server Configuration)

Prerequisite:

The user must have an enabled license on the BRAS Router.

```
license udi pid ISR4451-X/K9 sn FOC24221T1Y
license accept end user agreement
license boot level appxk9
license boot level uck9
license boot level securityk9
diagnostic bootup level minimal
spanning-tree extend system-id
```

BRAS acts as a PPPoE Server and after successful authentication with PPPoE provides an IP Address to IR1101 dialer interface:

```
ip dhcp excluded-address 41.41.41.1 41.41.41.9
ip dhcp pool 41-41-41-pool
 network 41.41.41.0 255.255.255.0
 default-router 41.41.41.1
 lease 2
!
username dslpeer password 0 dslpeerpass
```

Create a broadband Group :

```
bba-group pppoe global
 virtual-template 1
!
```

After configuring the broadband group, virtual-access is created automatically and then the virtual template must be created.

Interface configuration and username configuration:

```
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 ip address 41.41.41.1 255.255.255.0
 pppoe enable group global
!
```

For Authenticated Users, provide an IP Addresses. The dhcp pool (41-41-41-pool) which was created earlier is linked here:

```
interface Virtual-Template1
 ip unnumbered GigabitEthernet0/0/0.1
 peer default ip address dhcp-pool 41-41-41-pool
 ppp authentication pap chap
```

Add relevant routes, the next hop being the IP address that IR1101 Dialer acquires:

```
!
ip route 10.0.0.0 255.255.255.0 41.41.41.3 >> dialer ip, change as necessary
```

Monitoring and Debugging the PPPoE Configuration

Use the following global configuration commands to display the PPPoE session statistics:

```
#show pppoe session [status|packets|log]
#show ip interface pppoe
```

Use the following global configuration command to debug the PPPoE configuration:

```
# [no] debug pppoe detail
```

Router#show pppoe session

```
     1 client session
Uniq ID   PPPoE   RemMAC          Port                    VT   VA          State
           SID   LocMAC                                       VA-st       Type
    N/A     25   c014.fec2.1530  Gi0/0/0.1               Di1  Vi2         UP
                 c014.fe49.8200                              UP
```

Router#show pppoe session packets

```
Total PPPoE sessions 1
SID      Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
25       1094033         1809554         166942234       178601278
```

VDSL2 Controller Configuration Commands

This section describes some of the CLI commands specific to controller configuration.

Table 27 CLI Commands for VDSL2 controller configuration

Brief	Format	Command Default	Description
Bitswap		Default enabled	Bitswap
capability	capability *[annex-j]*	none	Set the DSL SFP capability
carrier-set	carrier-set*[a43 b43 a43c*	a43 b43 a43c	DSL SFP Carrier Set
default			Set a command to its defaults
description			Controller-specific description
exit			Exit from controller configuration mode
help			Description of interactive help
mac-address	mac-address*<MAC address>*	MAC is preconfigured by default	DSL SFP MAC Address. There is no need to configure anything to get the controller working.
modem vdsi		N/A	Modem configuraion
mpls			Not applicable to the IoT Router. Inherited from the c111x.
no			Negate a command or set its defaults
shutdown			shutdown vdsi controller
sra		default is enabled	Seamless Rate Adaption

VDSL Example

The following example is from a VDSL configuration:

```
VDSL-DSL-1101#show controllers vdsL 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status:          UP
                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'META'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x30A4
Chip Vendor Country:    0xB500                   0xB500
```

```
Modem Vendor ID:         'META'                    'BDCM'
Modem Vendor Specific:   0x0000                    0x0000
Modem Vendor Country:    0xB500                    0xB500
Serial Number Near:      MET20240017 V5311TR 1_62_8463
Modem Version Near:      1_62_8463 MT5311
Modem Version Far:       v10.08.48
Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.993.2 (VDSL2) Profile 17a
TC Mode:                 PTM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Failed full inits:       0
Short inits:             0
Failed short inits:      0
Modem FW  Version:
Modem PHY Version:
Modem PHY Source:        System
Line 0:
                         XTU-R (DS)              XTU-C (US)
Trellis:                  ON                      ON
SRA:                      enabled                 enabled
SRA count:                0                       0
Bit swap:                 enabled                 enabled
Bit swap count:           0                       0
Line Attenuation:          1.7 dB                 dB
Signal Attenuation:        2.8 dB                 dB
Noise Margin:             14.8 dB                 20.3 dB
Attainable Rate:         94595 kbits/s             64275 kbits/s
Actual Power:            11.2 dBm                 12.7 dBm
Per Band Status:         D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):    1.1     1.3     2.6     0.0     0.0     0.0     N/A
Signal Attenuation(dB):  2.1     2.0     3.9     0.0     0.0     0.0     N/A
Noise Margin(dB):        15.0    14.8    14.7    17.5    19.5    20.8    N/A
Total FECC:              690                      0
Total ES:                113                      0
Total SES:               45                       0
Total LOSS:              16777184                          0
Total UAS:               426                      31
Total LPRS:              0                        0
Total LOFS:              23                       0
Total LOLS:              0                        0
                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA           94697            NA             38167
SRA Previous Speed:        NA               0            NA                 0
Previous Speed:            NA           94595            NA             38025
Reed-Solomon EC:           NA               0            NA                 0
CRC Errors:                NA               0            NA              2674
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA            5.00            NA              5.00
Actual INP:                NA            2.00            NA              2.00
Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

Configuring the Flex VPN Tunnel between IR1101 dialer interface and HER (Pre-Shared Key)

In a FlexVPN Hub-and-Spoke design, spoke routers are configured with a normal static VTI with the tunnel destination of the Hub IP address. The Hub is configured with a Dynamic VTI. The DVTI on the Hub router is not configured with a static mapping to the peer IP address. The VTI on the Hub is created dynamically from a pre-configured tunnel template “virtual-template” when a tunnel is initiated by the spoke router/peer. The dynamic tunnel spawns a separate “virtual-access” interface for each spoke tunnel, inheriting the configuration from the cloned template.

Hub Configuration

Details:

```
License is required for ISR 4451:
license udi pid ISR4431/K9 sn FOC18094C2P
license accept end user agreement
license boot level appxk9
license boot level uck9
license boot level securityk9
spanning-tree extend system-id
!

ISR-HER(config)#int Loopback0
*Dec 15 07:40:56.217: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISR-HER(config-if)#ip address 192.168.200.1 255.255.255.0
ISR-HER(config-if)#no shut
ISR-HER(config-if)#end
```

FLEX VPN Configuration:

```
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
interface GigabitEthernet0/0/2
 ip address 10.40.100.100 255.255.255.0
 negotiation auto
!
```

Create a Tunnel Template (tunnel of source is the WAN interface using Lo0 as the IP for the Tunnel)

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source GigabitEthernet0/0/2
 tunnel protection ipsec profile IPSEC_PROFILE
end
```

Create a PSK Keyring – Use address 0.0.0.0 to match all peers; use symmetric PSK key for simplicity.

```
crypto ikev2 keyring KEYRING
 peer ANY-PEER
 address 0.0.0.0
 pre-shared-key local cisco1234
 pre-shared-key remote cisco1234
 exit
```

Create IKEv2 Profile – Specify the FQDN local identity, match any peer on the domain name, specify authentication PSK, specify using the Keyring, and specify cloning the Virtual Template.

```
crypto ikev2 profile IKEV2_PROFILE
 match identity remote fqdn domain CCI.COM
 identity local fqdn ISR-HER.CCI.COM
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list FLEX_LOCAL FlexVPN_Author_Policy
```

```
 virtual-template 1
```

Create the IPSec Profile – Set the IKEv2 Profile; the default Transform set is used so there is no need to specify it.

```
crypto ipsec profile IPSEC_PROFILE
 set ikev2-profile IKEV2_PROFILE
```

Specify the IPSec Profile on the Tunnel Template

```
interface virtual-template 1 type tunnel
 tunnel protection ipsec profile IPSEC_PROFILE
```

SPOKE Configuration

```
VDSL-DSL-1101(config)#int lo0
*Dec 15 07:51:28.465: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
VDSL-DSL-1101(config-if)#ip address 192.168.200.10 255.255.255.0
VDSL-DSL-1101(config-if)#no shut
```

Create a PSK Keyring – Use address 0.0.0.0 for lab purposes to match all peers; use the symmetric PSK key for simplicity.

```
crypto ikev2 keyring KEYRING
 peer ANY-PEER
 address 0.0.0.0
 pre-shared-key local cisco1234
 pre-shared-key remote cisco1234
 exit
```

Create IKEv2 Profile – Specify the FQDN local identity, match any peer on the domain name, specify authentication PSK, specify using the Keyring.

```
crypto ikev2 profile IKEV2_PROFILE
 match identity remote fqdn domain CCI.COM
 identity local fqdn VDSL-DSL-1101.CCI.COM
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
```

Create IPSec Profile – Set the IKEv2 Profile, the default Transform set is used so there is no need to specify it.

```
crypto ipsec profile IPSEC_PROFILE
 set ikev2-profile IKEV2_PROFILE
```

Create SVTI – Use Lo0 as the tunnel interface, specify the tunnel source and the tunnel destination as the Hub WAN IP, specify the IPSec Profile.

```
interface tunnel0
 ip unnumbered loopback 0
 tunnel source dialer 1
 tunnel destination 10.40.100.100
 tunnel protection ipsec profile IPSEC_PROFILE
```

Verification:

BRAS :

```
ISR-HER#
*Dec 15 08:04:48.585: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
up
ISR-HER#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/2   10.40.100.100   YES manual up                    up
GigabitEthernet0/0/3   unassigned      YES NVRAM  up                    up
Loopback0              192.168.200.1   YES manual up                    up
Virtual-Access1        192.168.200.1   YES unset  up                    up
Virtual-Template1      192.168.200.1   YES unset  up                   down
ISR-HER#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.40.100.100/500     41.41.41.10/500       none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify:
PSK
      Life/Active Time: 86400/106 sec
 IPv6 Crypto IKEv2  SA
ISR-HER#show crypto ipsec sa
interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.40.100.100
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.40.100.100/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (41.41.41.10/255.255.255.255/47/0)
   current_peer 41.41.41.10 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.40.100.100, remote crypto endpt.: 41.41.41.10
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/2
     current outbound spi: 0x20F0B4BE(552645822)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xACBECD6A(2898185578)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2001, flow_id: ESG:1, sibling_flags FFFFFFFF80000008, crypto map:
Virtual-Access1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3448)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x20F0B4BE(552645822)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2002, flow_id: ESG:2, sibling_flags FFFFFFFF80000008, crypto map:
Virtual-Access1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3448)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     outbound ah sas:
     outbound pcp sas:
```

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-9/sec-flex-vpn-xe-16-9-book/sec-cfg-ikev2-flex.html

Remote PoP Management using Cisco DNA Center

This section describes setting up the management of RPoP Gateways, IR1101 and IR1800 series routers and the IE switches connected behind them using the Cisco DNA Center.

RPoP Gateway IR1101 and IR1800 Onboarding using DNAC

To discover an IR1101 or IR1800 on Cisco DNA Center, the appliance must have IP reachability to the remote gateway, and CLI and SNMP management credentials must be configured on the device. After discovery, the devices are added to Cisco DNA Center inventory, allowing the controller to make configuration changes through provisioning.

As discussed in the section “Multi-VRF routes extension from HER to RPoP Gateway” VRFs are extended from the HER to the remote gateways over FlexVPN tunnels. For the management of the Remote gateways using Cisco DNA Center, a separate VRF called Management_VN is configured on the HER and fusion router which has the reachability to the Shared services as discussed in “Shared Services Reachability” section. This provides the IP reachability of the remote gateway to the Cisco DNA Center. Make sure a static route is configured on the Cisco DNA Center appliance for the configured IP prefix on the remote gateway.

In this implementation, the example below shows the configuration that is used on the remote gateways. These configurations must be staged using Local Manager or CLI.

Configuration required on the gateways for Cisco DNA Center Discovery:

```
hostname <hostname>
username <username> privilege 15 password 0 <password>
enable secret <secret>

ip domain name <domain_name>
!
crypto key generate rsa modulus 2048•
ip ssh version 2•
line vty 0 15•
login local•
transport input ssh•
transport preferred none
!

snmp-server group default v3 priv
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
snmp-server view SNMPv3All iso included
snmp-server view SNMPv3None iso excluded
snmp-server community <CommunityString> RW
snmp-server user <user> default v3 auth sha <auth_password> priv aes 128 <priv_password>
```

Configuration required to enable IP reachability using FlexVPN tunnel:

Pre-requisites:

- The FlexVPN tunnel is established between the HER and the RPoP Gateways. Refer to the “FlexVPN Tunnel Establishment”section.
- Required prefixes are allowed using the IKEv2 prefix injection (advertise mGRE Tunnel source loopbacks using FlexVPN access-list).

```
vrf definition Management_VN
 rd 1:10
 !
```

```
 address-family ipv4
  route-target export 1:10
  route-target import 1:10
 exit-address-family
!

interface Loopback26
 description Tunnel26 source IP
 ip address 10.22.22.26 255.255.255.255
end

interface Tunnel26
 description Tunnel for Management_VN
 vrf forwarding Management_VN
 ip address 10.254.254.26 255.255.255.0
 no ip redirects
 ip nhrp map 10.254.254.6 10.22.22.6
 ip nhrp network-id 6
 ip nhrp nhs 10.254.254.6
 ip nhrp registration timeout 30
 cdp enable
 tunnel source Loopback26
 tunnel mode gre multipoint
end

router bgp 65550
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf Management_VN
  redistribute connected
  redistribute static
  neighbor 10.254.254.6 remote-as 65550
  neighbor 10.254.254.6 activate
 exit-address-family
interface Loopback100
 vrf forwarding Management_VN
 ip address 192.100.0.2 255.255.255.255
end
```

Verification:

Spoke2_IR1101#sh ip route vrf Management_VN

<Snip>

```
      10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
B        10.10.0.0/16 [200/0] via 10.254.254.6, 00:05:31


B        10.10.100.0/24 [200/0] via 10.254.254.6, 00:05:31
B        10.10.201.0/24 [200/0] via 10.254.254.6, 00:05:31
B        10.40.100.0/24 [200/0] via 10.254.254.6, 00:05:31
C        10.254.254.0/24 is directly connected, Tunnel26
L        10.254.254.26/32 is directly connected, Tunnel26
B        10.255.255.20/30 [200/0] via 10.254.254.6, 00:05:31
      192.100.0.0/24 is variably subnetted, 2 subnets, 2 masks
B        192.100.0.0/24 [200/0] via 10.254.254.6, 00:05:31
C        192.100.0.2/32 is directly connected, Loopback100
      192.100.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.100.1.0/24 is directly connected, Vlan100
L        192.100.1.1/32 is directly connected, Vlan100
      192.168.70.0/30 is subnetted, 1 subnets
B        192.168.70.0 [200/0] via 10.254.254.6, 00:05:31
```

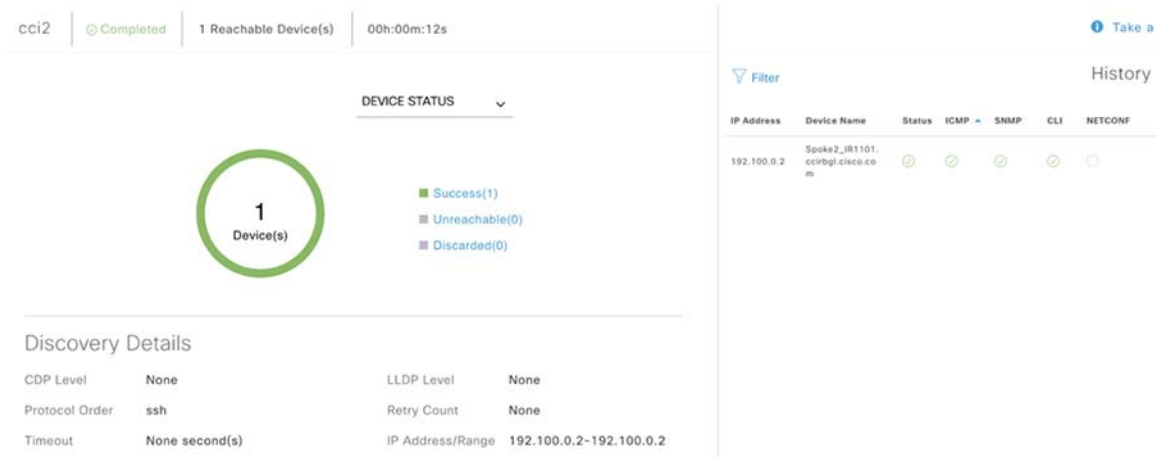
Verifying the reachability to the Cisco DNA Center from the remote gateway:

```
Spoke2_IR1101#ping vrf Management_VN 10.10.201.202 so Loopback100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.201.202, timeout is 2 seconds:
Packet sent with a source address of 192.100.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/51/80 ms
```

Follow the steps below to onboard the Remote gateways on the Cisco DNA Center:

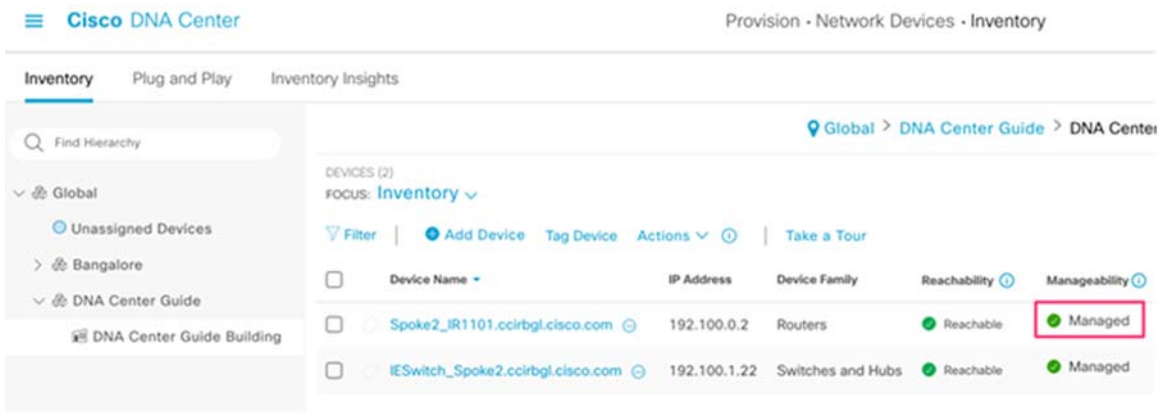
1. Discover the remote gateway using the Discovery tool; in this case use the Loopback 100 IP 192.100.0.2 to discover the gateway.

Figure 201 Cisco DNA Center RPoP Gateway discovery



2. After the device discovery is complete, assign the device from Unassigned Devices to the respective Site. Notice the device becomes a Managed node.

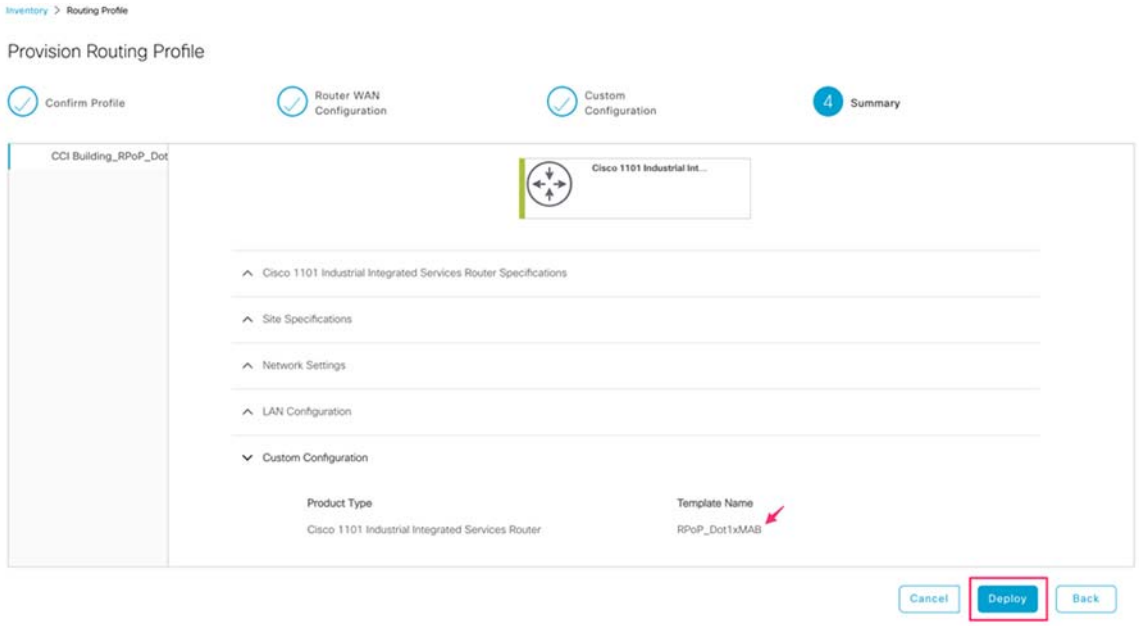
Figure 202 RPoP Gateway Management by Cisco DNA Center



3. Provision the remote gateway by pushing the “RPoP Dot1x_MAB Template”. Complete the steps in the document below to create and apply Day-N configuration templates in Cisco DNA Center.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01000.html#j5x_ntw_vbb

Figure 203 RPoP Gateway provisioning using DAY-N templates



IE Switch behind IR1101/IR1800 Onboarding using DNAC

Similarly to onboarding remote gateways on to the Cisco DNA Center, the IE Switches connected behind them can also be onboarded and managed. Two methods to onboard the IE Switches are PnP Onboarding and Manual Discovery.

Figure 204 IE Switch behind RPoP gateway topology view

PnP onboarding:

1. Make sure the Management vlan (eg: vlan 100) is created on the remote gateway and the same vlan is used for pnp startup-vlan (eg: pnp startup-vlan 100)

```
Vlan 100
  name Management_VN
pnp startup-vlan 100
```

2. Configure an SVI for Mangement vlan with the helper address.

```
interface Vlan100
 vrf forwarding Management_VN
 ip address 192.100.1.1 255.255.255.0
 ip helper-address 10.10.100.20
end
```

3. Configure the switchport of the gateway connected to the IE Switch as trunk.

4. In the DHCP scope of the Management vlan (Vlan 100 in this case), point DHCP option 43 with the IP address of DNA Center. This PnP will discover the IE switch.

5. Execute the following steps on the extended node switch before starting the onboarding process that connects the IE Switch to the switchport of the remote gateways:

```
delete /force sdflash:vlan.dat
delete /force sdflash:*.cer
delete /force sdflash:pnp*
delete /force /recursive sdflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pnp-tech-time
delete /f flash:pnp-tech-discovery-summary #Delete all the certificates in NVRAM delete /f nvram:*.cer
#Clear the crypto certificates in config mode crypto key zerosize
no crypto pki certificate pool
#Change the VTP mode to Transparent in config mode vtp mode off
vtp mode transparent exit
#Do write erase and reload
write erase
reload (enter no if asked to save)
```

6. After the device discovery is complete, assign the device from Unassigned Devices to the respective Site. You can Notice that the device becomes the Managed node.

7. Now provision the IE Switches with <<RPoP Dot1x_MAB Template>> and <Host Onboarding> templates.

Manual discovery:

To manually discover IE Switches on the Cisco DNA Center using the Discovery tool, the appliance must have IP reachability to the IE switch, and CLI and SNMP management credentials must be configured on the switch.

1. Configure the switchport of the gateway connected to the IE Switch as trunk.

2. Use the configurations below on the IE Switch.

```
hostname <hostname>
username <username> privilege 15 password 0 <password>
enable secret <secret>

ip domain name <domain_name>
!


crypto key generate rsa modulus 2048•
ip ssh version 2•
line vty 0 15•
login local•
transport input ssh•
transport preferred none
!
snmp-server group default v3 priv
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
snmp-server view SNMPv3All iso included
snmp-server view SNMPv3None iso excluded
snmp-server community <CommunityString> RW
snmp-server user <user> default v3 auth sha <auth_password> priv aes 128 <priv_password>
```

3. Create a Management VlanLAN (e.g: vlan 100) and an SVI which will be used to discover the node from the DNA Center.

```
Vlan 100
```

```
  name Management_VN
           interface Vlan100
  ip address dhcp
end
```

4. Verify the ping reachability from the IE Switch to the DNA Center.

```
IESwitch_Spoke2#ping 10.10.201.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.201.202, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/41/52 ms
```

5. To discover the IE Switch using the Discovery tool of DNA Center, use the Management vlan IP (eg: vlan 100).
6. When the device discovery is complete, assign the device from Unassigned Devices to the respective Site. Notice the device becomes the Managed node.
7. Now provision the IE Switches with <<RPoP Dot1x_MAB Template>> and <Host Onboarding> templates.

RPoP Dot1x_MAB Template:

```
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AUTHC_SUCCESS-AUTHZ_FAIL
 match authorization-status unauthorized
 match result-type success
!
class-map type control subscriber match-all DOT1X
 match method dot1x
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
```

```
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
 !
class-map match-all AUTOCONF-DEFAULT-CLASS
 match access-group name AUTOCONF-ACL-DEFAULT
class-map match-any AUTOCONF-TRUST-DSCP-CLASS
 match ip dscp 1
class-map match-any AUTOCONF-EGRESS-CLASS-1
 match ip dscp default
class-map match-any AUTOCONF-EGRESS-CLASS-0
 match ip dscp ef
class-map match-any AUTOCONF-TRUST-COS-CLASS
 match cos  1
class-map match-all AUTOCONF-VOIP-SIGNAL-CLASS
 match ip dscp cs3
class-map match-all AUTOCONF-VOIP-DATA-CLASS
 match ip dscp ef
!
!
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  50 class DOT1X_TIMEOUT do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
```

```
    20 authenticate using dot1x retries 2 retry-time 0 priority 10
  event inactivity-timeout match-all
   10 class always do-until-failure
    10 clear-session
  event authentication-success match-all
  event violation match-all
   10 class always do-until-failure
    10 restrict
  event authorization-failure match-all
   10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
    10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
  event session-started match-all
   10 class always do-until-failure
    10 authenticate using mab priority 20
  event authentication-failure match-first
   5 class DOT1X_FAILED do-until-failure
    10 terminate dot1x
    20 authentication-restart 60
   10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
    10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
    20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
    30 authorize
    40 pause reauthentication
   20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
    10 pause reauthentication
    20 authorize
   30 class MAB_FAILED do-until-failure
    10 terminate mab
    20 authenticate using dot1x retries 2 retry-time 0 priority 10
   40 class DOT1X_NO_RESP do-until-failure
    10 terminate dot1x
    20 authentication-restart 60
   50 class DOT1X_TIMEOUT do-until-failure
    10 terminate dot1x
    20 authenticate using mab priority 20
   60 class always do-until-failure
    10 terminate mab
    20 terminate dot1x
    30 authentication-restart 60
  event aaa-available match-all
   10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
    10 clear-session
   20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
    10 resume reauthentication
  event agent-found match-all
   10 class always do-until-failure
    10 terminate mab
    20 authenticate using dot1x retries 2 retry-time 0 priority 10
  event inactivity-timeout match-all
   10 class always do-until-failure
    10 clear-session
  event authentication-success match-all
  event violation match-all
   10 class always do-until-failure
    10 restrict
  event authorization-failure match-all
   10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
    10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
  event session-started match-all
   10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  50 class DOT1X_TIMEOUT do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
```

```
  30 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  50 class DOT1X_TIMEOUT do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  50 class DOT1X_TIMEOUT do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
```

```
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
  10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  50 class DOT1X_TIMEOUT do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
```

```
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map AUTOCONF-EGRESS-BW1-POLICY
 class AUTOCONF-EGRESS-CLASS-0
  priority percent 50
 class AUTOCONF-EGRESS-CLASS-1
  bandwidth remaining percent 43
 class class-default
  bandwidth remaining percent 50
policy-map AUTOCONF-TRUST-COS-POLICY
 class AUTOCONF-TRUST-COS-CLASS
  set cos 1
policy-map AUTOCONF-EGRESS-BW2-POLICY
 class AUTOCONF-EGRESS-CLASS-0
  priority percent 50
 class AUTOCONF-EGRESS-CLASS-1
  bandwidth remaining percent 11
 class class-default
  bandwidth remaining percent 67
policy-map AUTOCONF-CISCOPHONE-POLICY
 class AUTOCONF-VOIP-DATA-CLASS
  police cir 128000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit cs1
 class AUTOCONF-VOIP-SIGNAL-CLASS
  police cir 64000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit cs1
 class AUTOCONF-DEFAULT-CLASS
  police cir 10000000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit cs1
policy-map AUTOCONF-TRUST-DSCP-POLICY
 class AUTOCONF-TRUST-DSCP-CLASS
  set dscp 1
!
!
!
!
!
!
template DefaultWiredDot1xClosedAuth
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
!
template DefaultWiredDot1xLowImpactAuth
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
```

```
 service-policy type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
!
template DefaultWiredDot1xOpenAuth
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
```

Host Onboarding – Closed Authentication Template:

```
#foreach($interface in $interfaces)
 default interface $interface
#end
#foreach($interface in $interfaces)
 interface $interface
 switchport mode access
 access-session inherit disable interface-template-sticky
 access-session inherit disable autoconf
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 spanning-tree bpduguard enable
#end
```

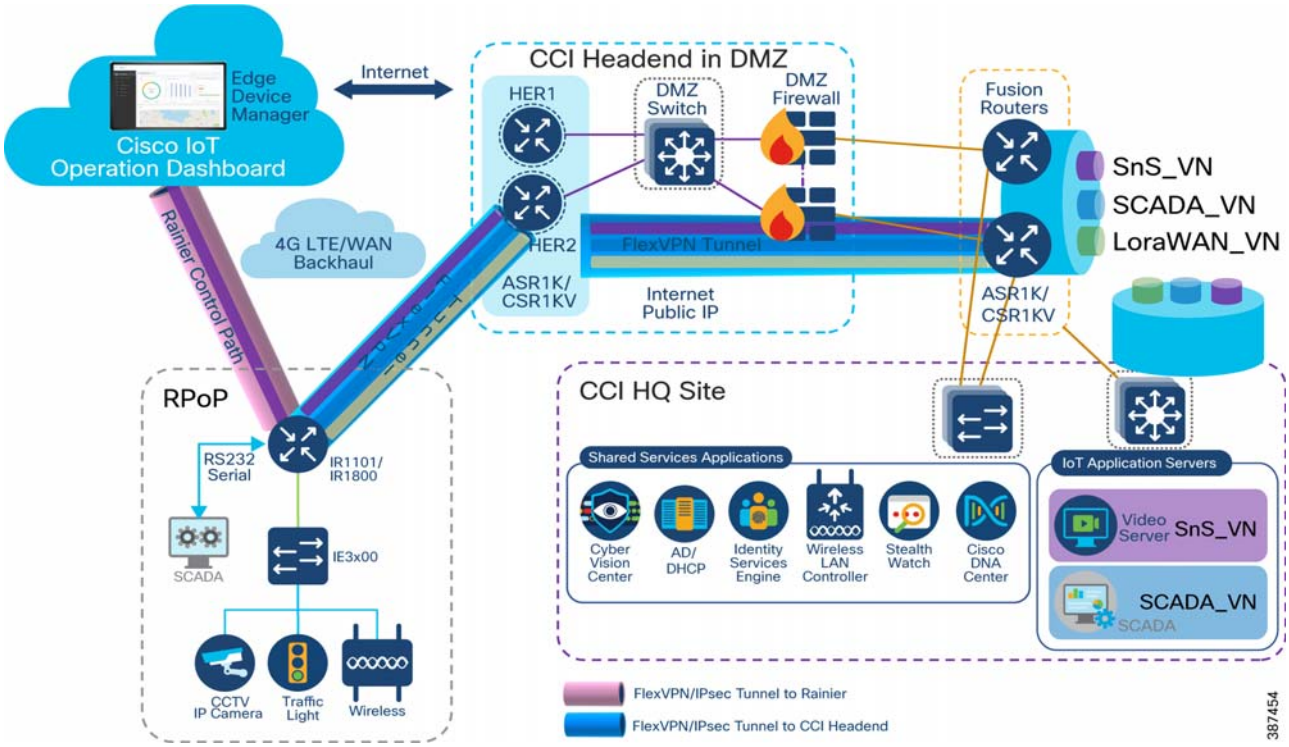
Remote PoP Management using IOTOD

This section describes the management of RPoP Gateways, IR1101 and the IE switches connected behind them using the PnP portal and IOTOD with sample configuration.

See the *CCI General Design* guide for RPoP design and architecture.

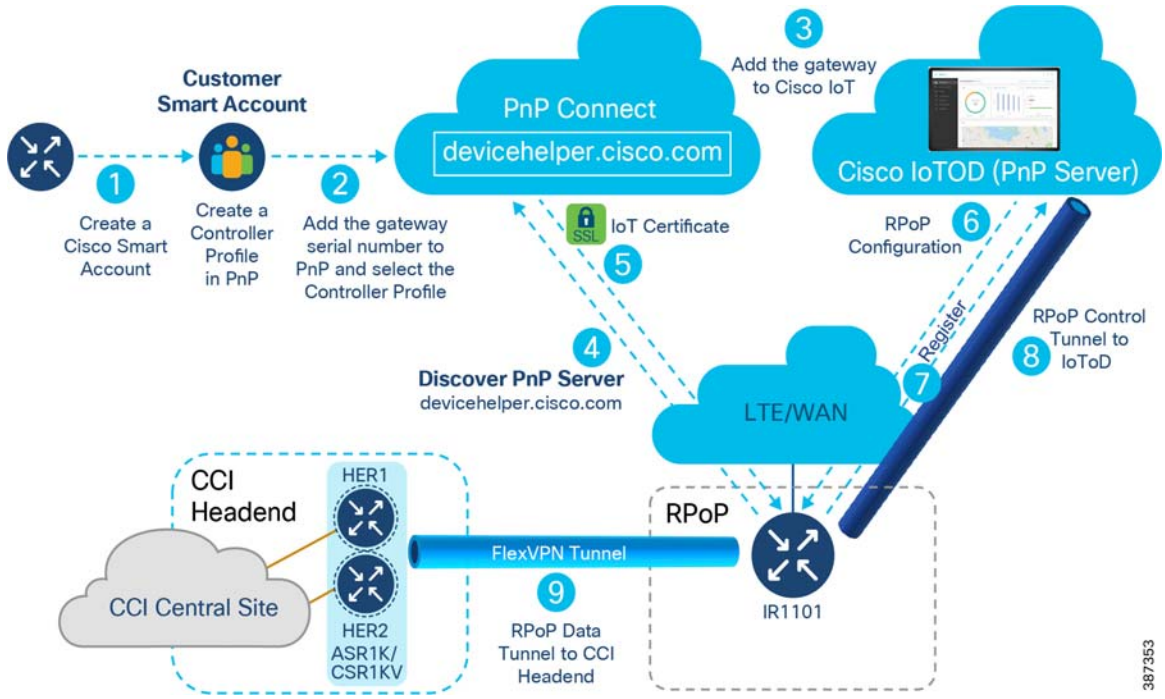
Architecture of RPOP with IR1101

Figure 205 IOTOD with IR1101 as RPOP device



PnP and IOTOD components

Figure 206 IOTOD with PnP



Prerequisites for Onboarding the IR1101 to IOTOD

Prerequisites are listed below.

- IR1101 with working SIM card
- IR1101 with GPS antenna connected to the Cellular module
- IR1101 added to the PnP URL & assigned appropriate controller profile

Adding the Certificate for controller profile in PnP URL

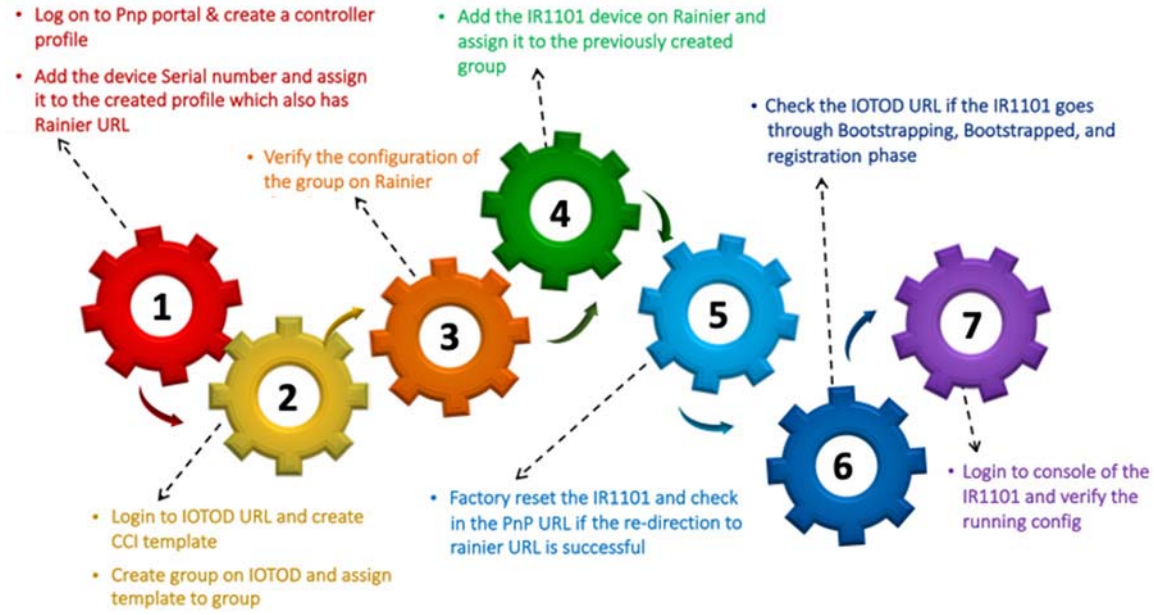
Install *openssl* on Mac/Windows/Linux and use the *openssl* command shown below for updating the certificate to the IOTOD controller profile.

openssl s_client -showcerts -servername<IOTOD URL>.io -connect <IOTOD URL>.io:443

This results in a chain of 3, and the last one of the certificate chains is for PnP use only.

Steps for onboarding of IR1101 to IOTOD

Figure 207 Onboarding of 1101 steps



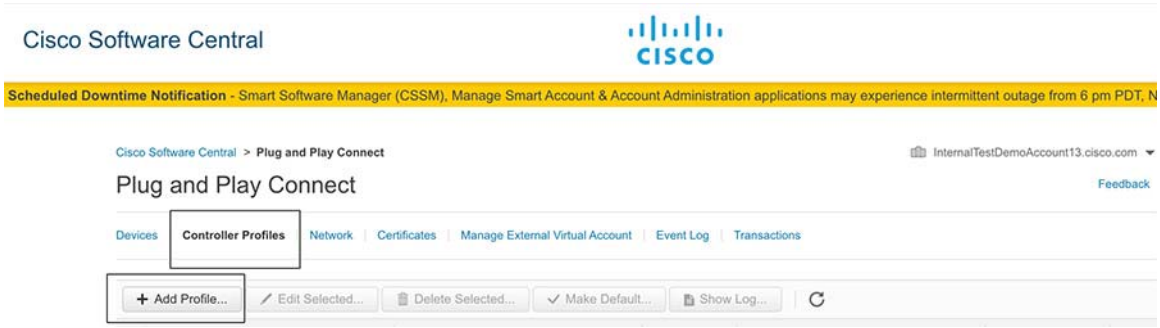
1. Login to the network plug and play portal and create the controller profile by specifying: the controller profile name, IOTOD https URL, and the SSL cert of the IOTOD URL to which the IR1101/IR1800 is to be registered.
2. Onboard the IR1101/ by adding the device serial number manually and then assign it to the Controller profile created in step 1.
3. Create the device-specific template with the bootstrap config. Configure the IR1101 and then assign it to a group on Rainier.
4. Manually add the device by specifying the IR1101 serial number, and name, then assign the template created in step 3.
5. Ensure the IR1101 has a valid SIM card and then factory reset the IR1101/IR1800. Verify that the PnP redirection to the Rainier URL is successful. If there are any errors, investigate the PnP event logs.
6. Look at the event log on Rainier for the specific device events and errors. The IR1101 goes through bootstrapping, registration phase, and a check for registration errors. For more details refer the Cisco EDM page: https://developer.cisco.com/docs/iotod/#!requirements-and-release-notes-overview.

Adding IR1101 to PnP

Note: A Smart Account is as a prerequisite for onboarding the PnP portal.

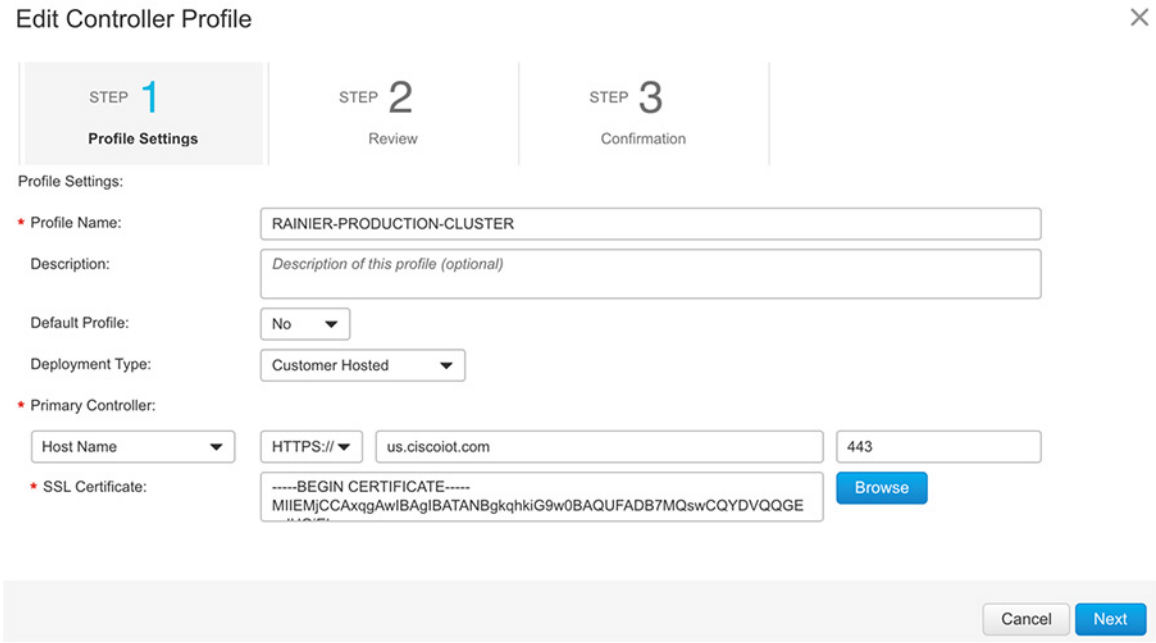
1. Login to the PnP URL, and then create a controller profile on IOTOD.

Figure 208 Create a controller profile on PnP



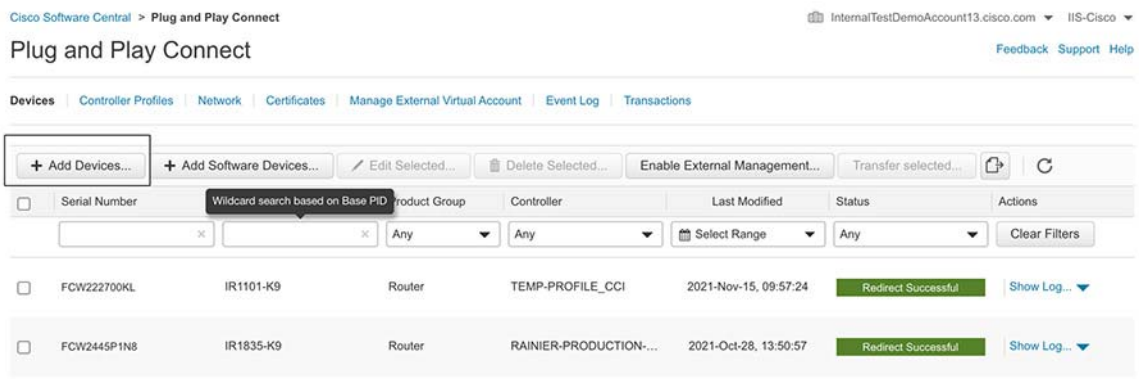
2. Specify the controller profile name, IOTOD URL, and SSL certificate of the assigned IOTOD URL.

Figure 209 Update IOTOD URL certs



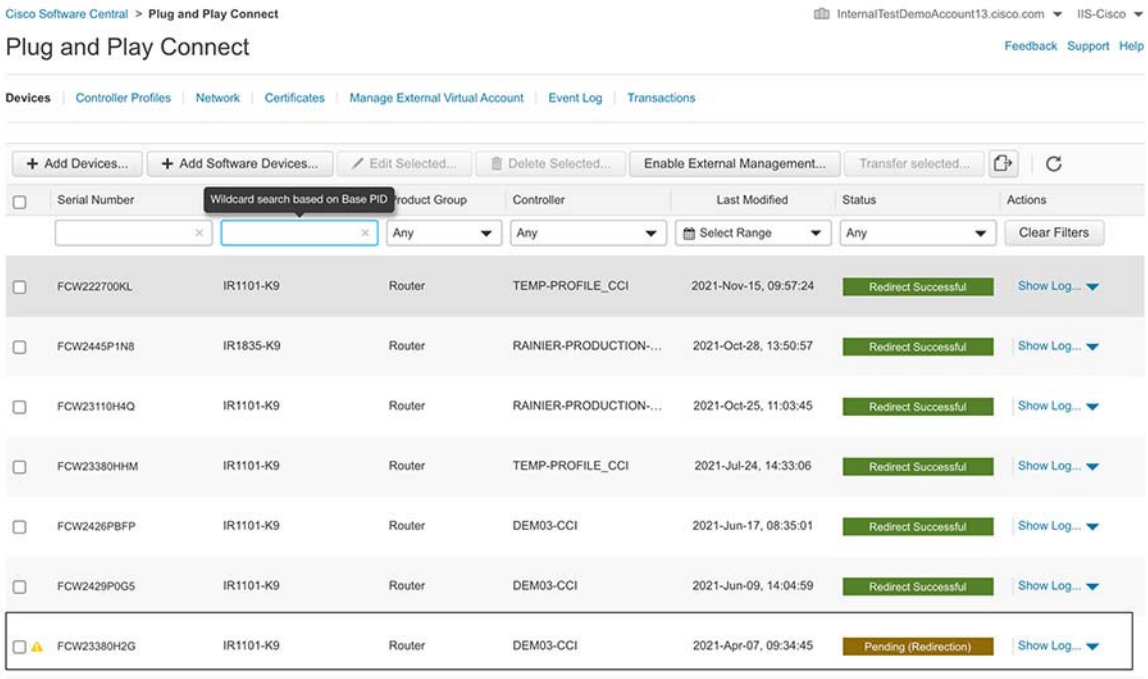
3. Add the IR1101 S/N to IOTOD .

Figure 210 Add IR1101 to PnP



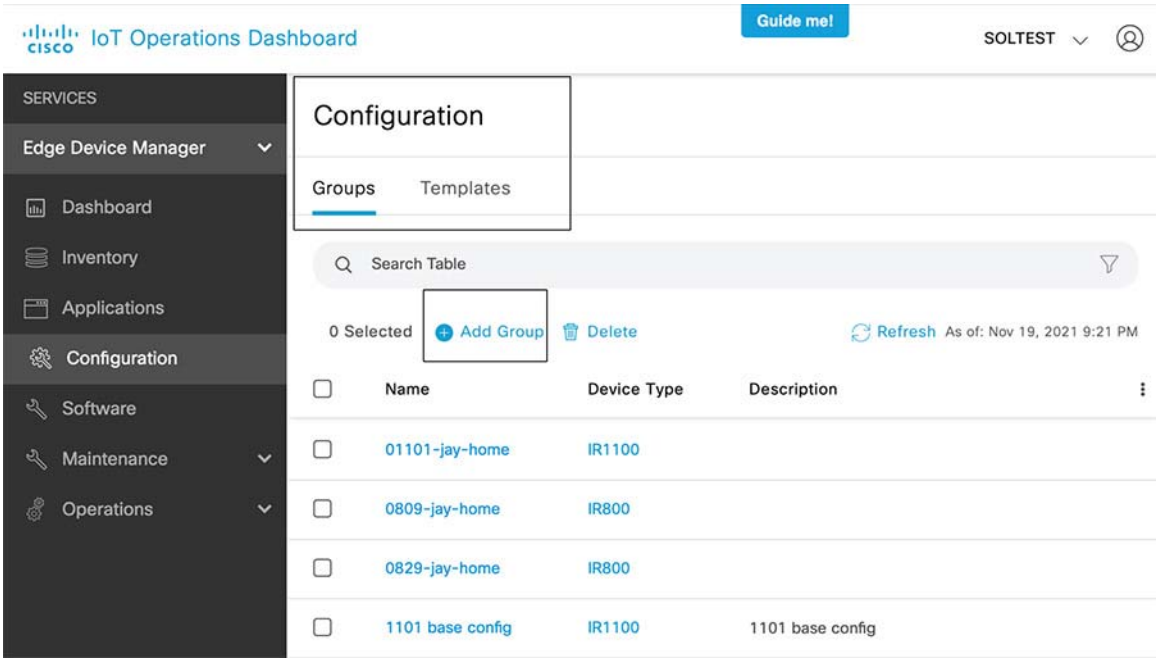
4. Factory reset the IR1101, and then verify the redirection to the IOTOD URL is successful.

Figure 211 Check the IR1101 redirection to IOTOD on PnP



5. Create a template for the IR1101 having a bootstrap config, CCI data tunnel config. Assign the template to the group.

Figure 212 Create template and groups on IOTOD



6. For the IR1101 config templates (Created using the Bootstrap config and CCI data tunnel config templates):
   - After login to IOTOD, the IOTOD has default templates which can be used to onboard the IR1101. The IR1101 the default template only includes the bootstrap configuration that is used to form the control tunnel with IOTOD.
   - The CCI custom config template must be present for the IR1101 to have a data tunnel to CCI Headend.
   - The CCI data tunnel template has these four services defined: SCADA_VN, SnS_VN, LoraWAN_VN and Lighting_VN. Each of these services are part of independent mGRE tunnels inside the FlexVPN data tunnel to CCI head end router & VRFs are extended from the HER to the 1101 over Flexvpn tunnels.
   - The CCI custom config template is pushed to the IR1101 using the established control path from the IR 1101.
7. The changes for the IR1101 config Bootstrap config (with Iox enabled) is shown below.

```
    <#assign cell_if = "Cellular 0/1/0">  Append the cellular interface number as per SIM Slot ,
Example if the SIM card is present in 0/1/0

controller cellular 0/1/0 Append the cellular interface number as per SIM Slot , Example if the SIM
card is present in 0/1/0
 lte modem link-recovery rssi onset-threshold -110
 lte modem link-recovery monitor-timer 20
 lte modem link-recovery wait-timer 10
 lte modem link-recovery debounce-count 6
!
interface Cellular0/1/0 Append the cellular interface number as per SIM Slot , Example if the SIM card
is present in 0/1/0
 description Cellular Connection to Firewall Public IP
 mtu 1430
 ip nat outside
 ip address negotiated
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
```

```
 ipv6 enable
 ip virtual-reassembly
!
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0 Append the cellular interface number as per SIM Slot , Example
if the SIM card is present in 0/1/0
!
dialer watch-list 1 ip 2.2.2.2 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip list 1
dialer-list 1 protocol ipv6 permit
!
!
```

8. The CCI data tunnel config for the IR1101 to establish a Tunnel to the CCI HER is shown below.

```
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list FLEX_ACL
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha512
 group 19
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
crypto ikev2 keyring FLEX_KEYS
 peer CCI-HER-1
  address 173.39.13.84
  pre-shared-key cisco
!
!
crypto ikev2 profile FLEX_CLIENT_PROF
 match identity remote address 173.39.13.84 255.255.255.192
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEX_KEYS
 dpd 30 3 periodic
 aaa authorization group psk list FlexVPN_Author default
!
 !
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile default_No_cert
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FLEX_CLIENT_PROF
!
 !
interface Loopback10
 ip address 192.168.100.96 255.255.255.255. change as required
!
!
interface Tunnel10
 ip unnumbered Loopback10
 tunnel source Cellular0/1/0 change as required
 tunnel destination 173.39.13.84 change as required
```

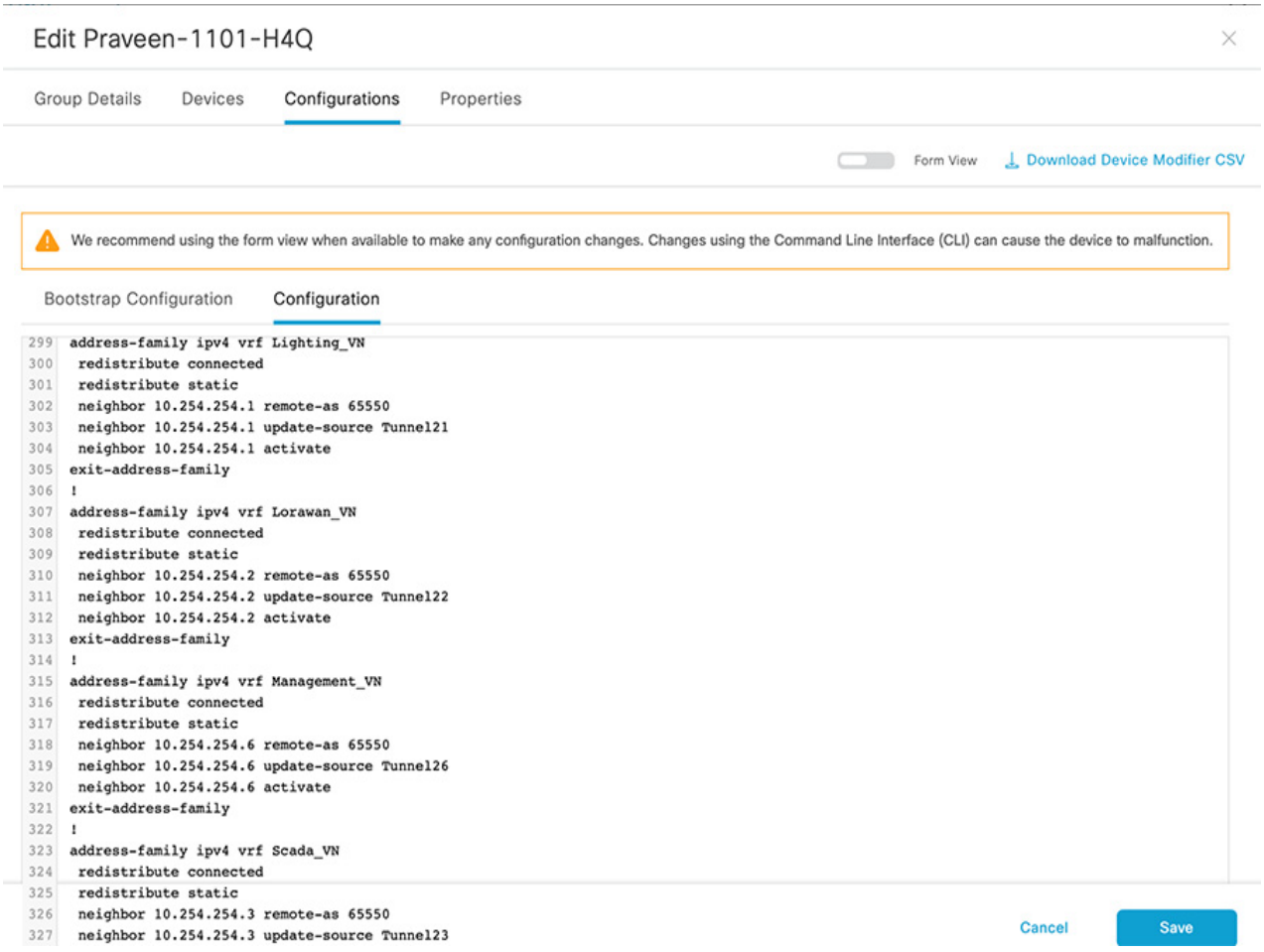
```
 tunnel protection ipsec profile default_No_cert
```

Enable new service in IR1101 from IOTOD using Push config

Using the push config option on IOTOD, after the IR1101 is registered on IOTOD, and then the updated config for SnS_VN . The configuration is shown below.

```
!
vrf definition SnS_VN
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!
!
interface Loopback24
 description Tunnel24 source IP
 ip address 10.22.22.34 255.255.255.255
!
!
interface Tunnel24
 description Tunnel for SnS_VN
 vrf forwarding SnS_VN
 ip address 10.254.254.34 255.255.255.0
 no ip redirects
 ip nhrp map 10.254.254.4 10.22.22.4
 ip nhrp network-id 4
 ip nhrp nhs 10.254.254.4
 ip nhrp registration timeout 30
 cdp enable
 tunnel source Loopback24
 tunnel mode gre multipoint
!
!
 address-family ipv4 vrf SnS_VN
  redistribute connected
  redistribute static
  neighbor 10.254.254.4 remote-as 65550
  neighbor 10.254.254.4 update-source Tunnel24
  neighbor 10.254.254.4 activate
 exit-address-family
!
!
ip access-list standard FLEX_ACL
 14 permit 10.22.22.34
 15 permit 10.254.254.34
```

Figure 213 IOTOD data tunnel changes



IR1101 control and data tunnels

Figure 214 Control and data tunnels

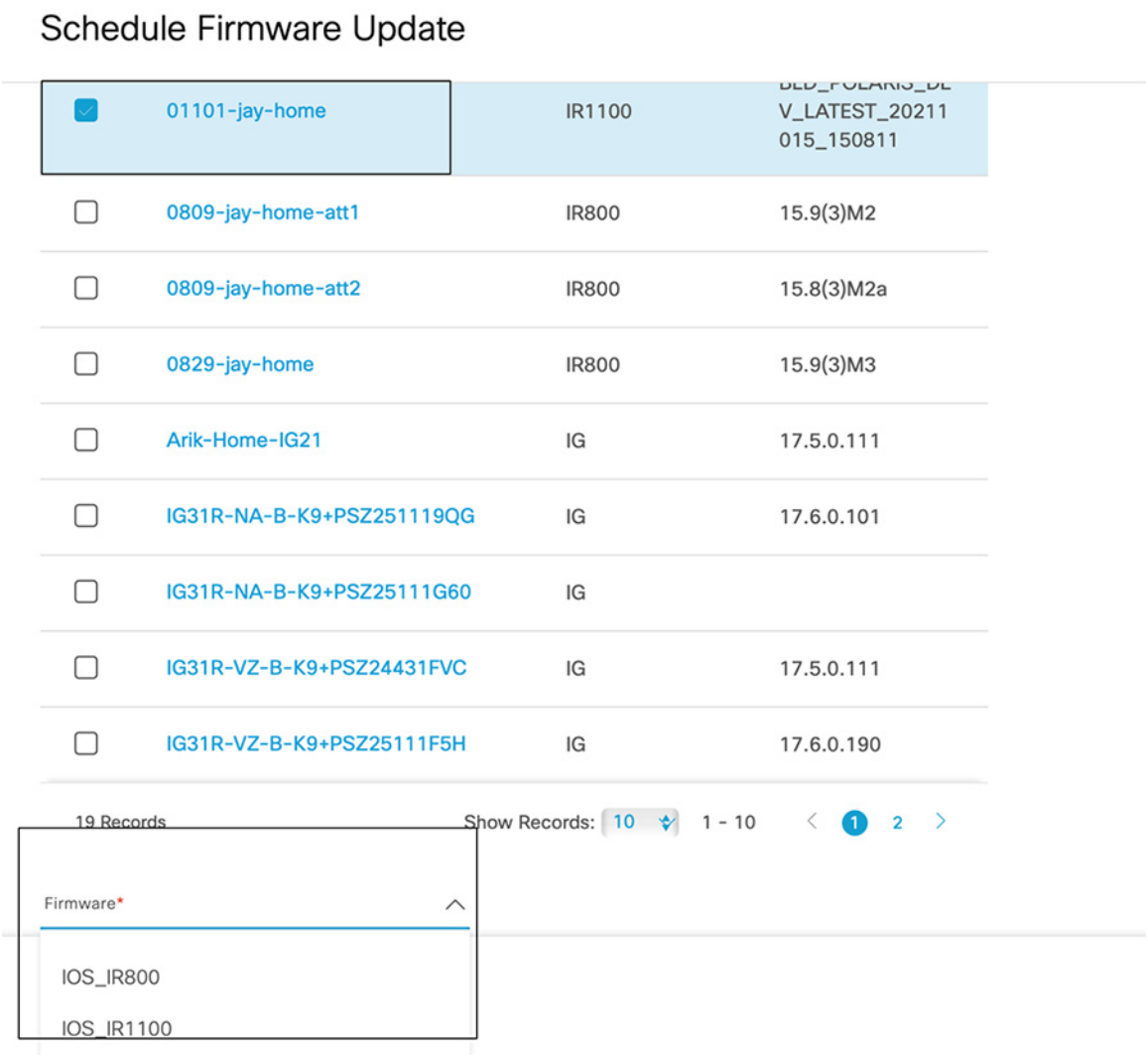
```
      _FCW2446P0E6#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1                               173.39.13.84/4500     none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/467 sec

Tunnel-id Local                 Remote                fvrf/ivrf            Status
2                               54.188.245.253/4500   none/ciscoiot        READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/725 sec
```

- After the config push is complete from IOTOD to the IR1101/IR1800 verify that there are two tunnels established. Tunnel-id1 is the data tunnel from the IR1800 to the CCI HER and Tunnel-id2 is the control tunnel from the IR1800 to IOTOD.

IR1101 Software update from Rainier

Login to Rainier and choose **software** from the left menu. Select on the device for the software update. Select the appropriate software version from drop-down list.

Figure 215 Software update to IR1101

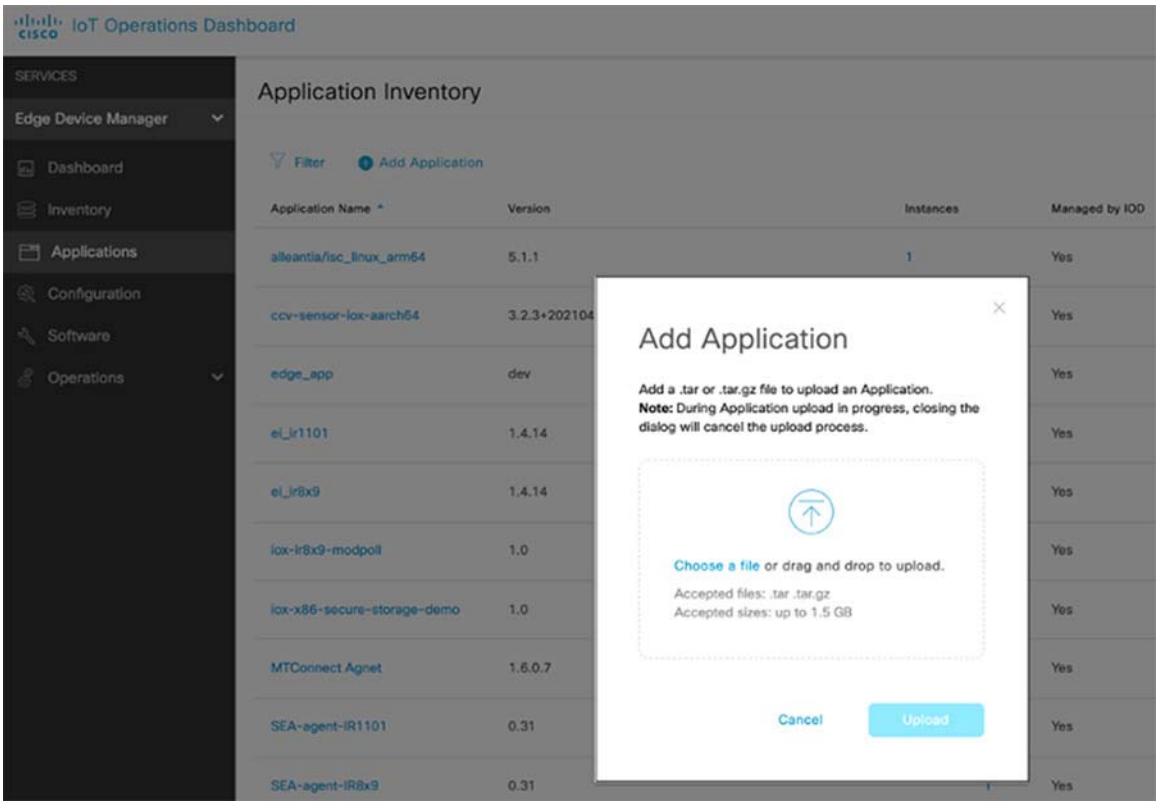


IR1101 IOX Application Install

To install IOX on the IR1101 complete the steps below.

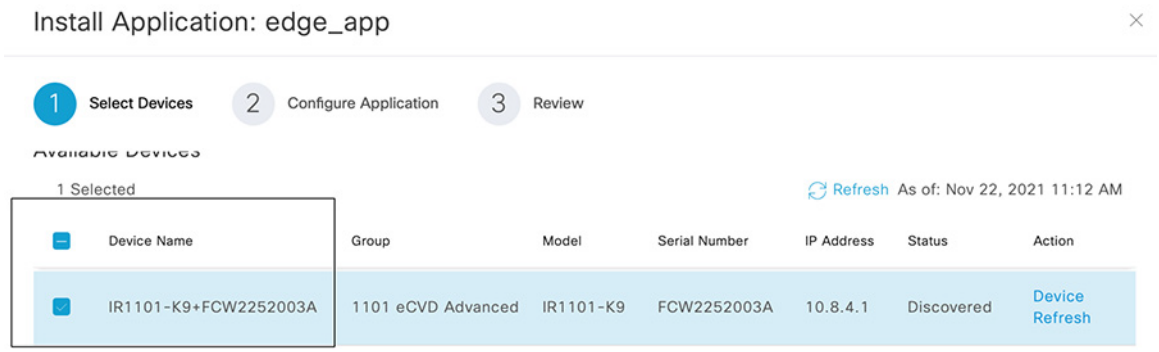
1. Upload the application from the Rainier page as shown below.

Figure 216 Upload application to IOTOD



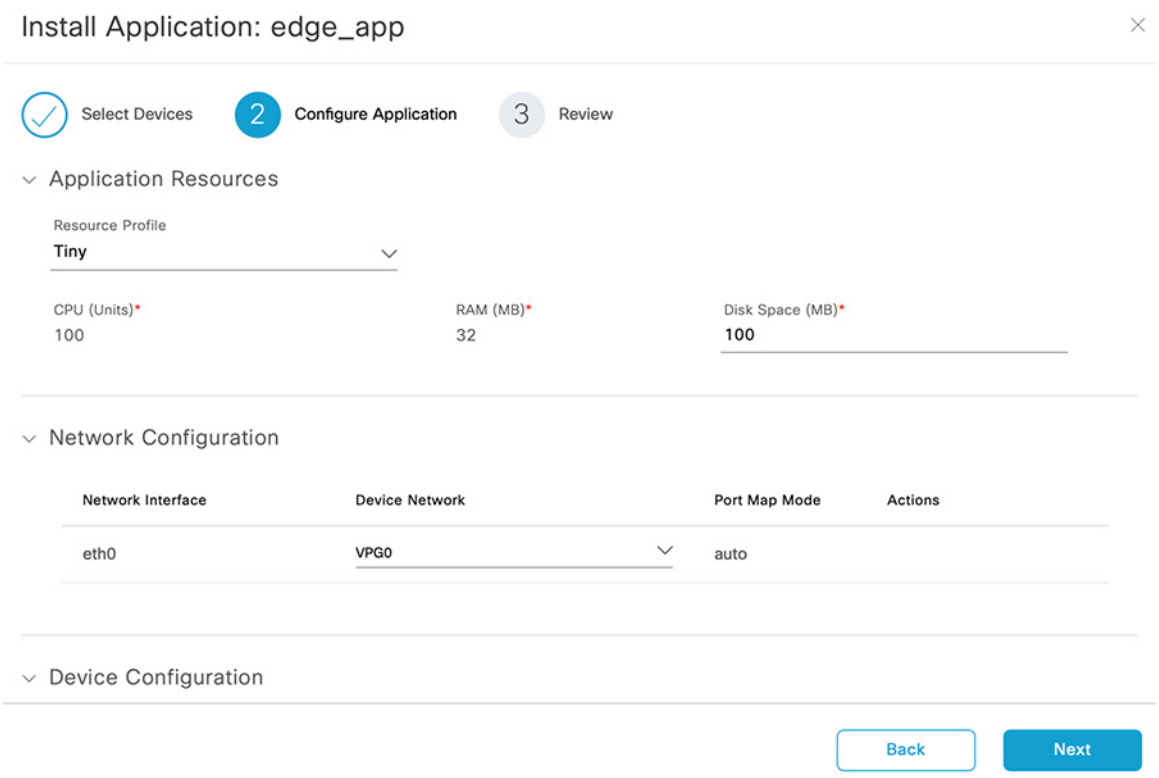
2. Select the device for the application installation.

Figure 217 Select device for software update from IOTOD



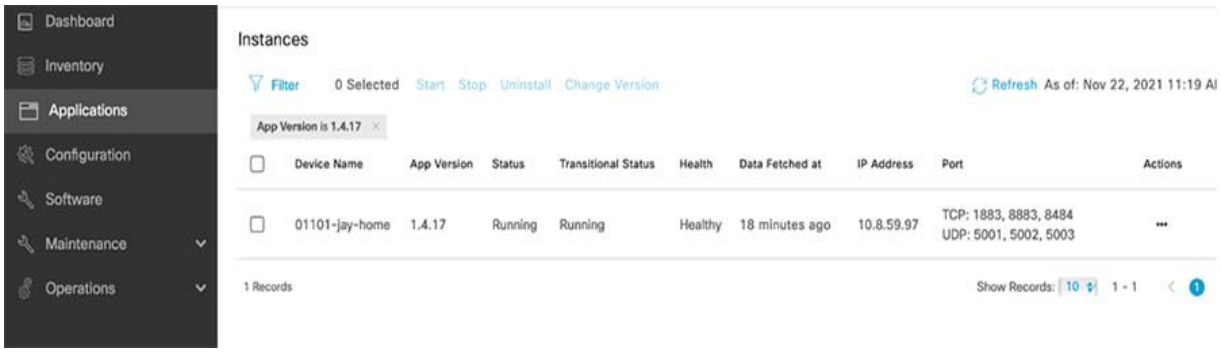
3. Select the appropriate resource type.

Figure 218 Install application on IR1101



4. Check the status of the application install from Rainier.

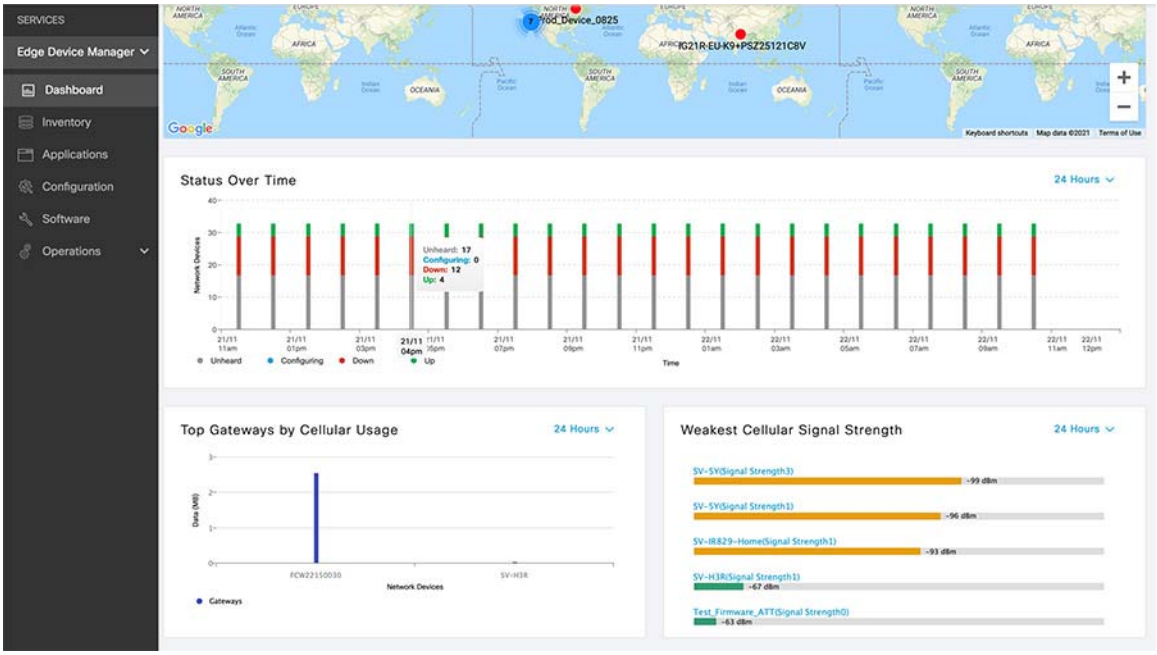
Figure 219 Check the status of application install from IOTOD



IOTOD dashboard details

The IOTOD dashboard shows details about the location where the IR1101 is placed. It also shows Cellular signal strength and the Online/Offline status of the onboarded devices for the tenant the user can access.

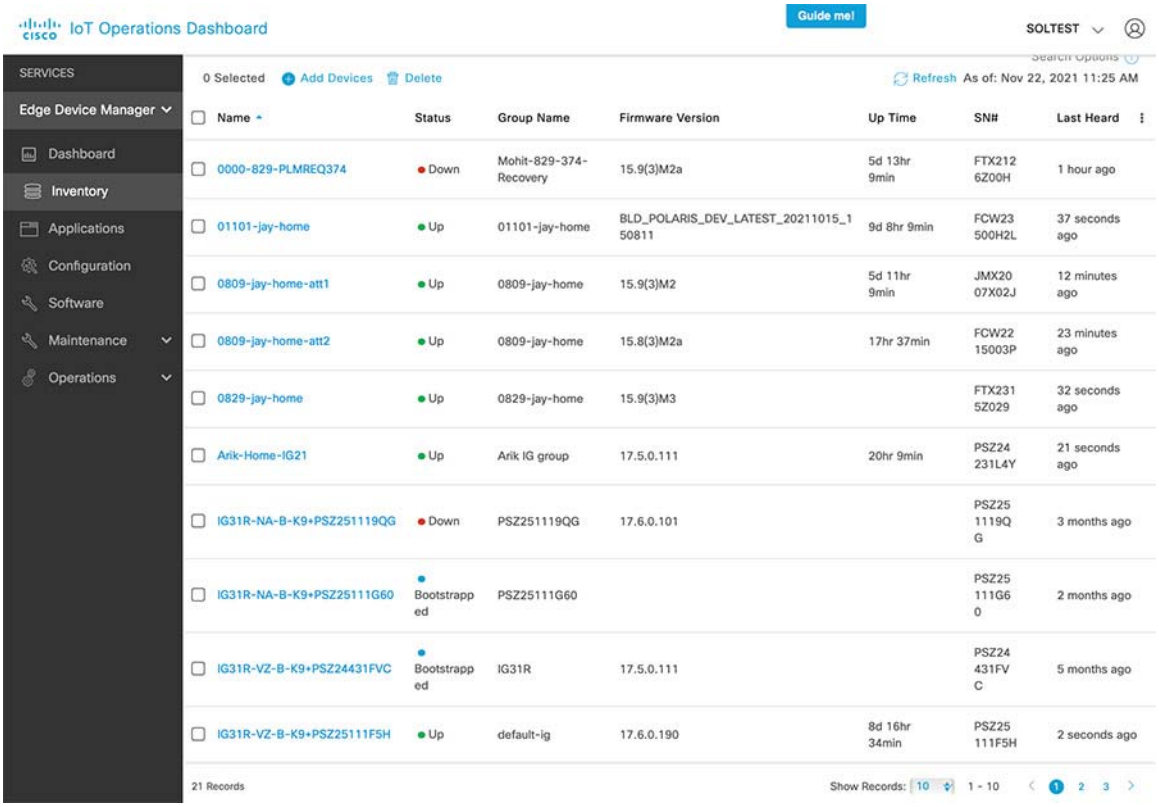
Figure 220 IOTOD dashboard



IOTOD Device Inventory

The IOTOD device inventory tab shows the status details about onboarded devices, such as the number of devices on Bootstrapping, and Bootstrapped and registered devices for the tenant the user can access.

Figure 221 IOTOD device inventory

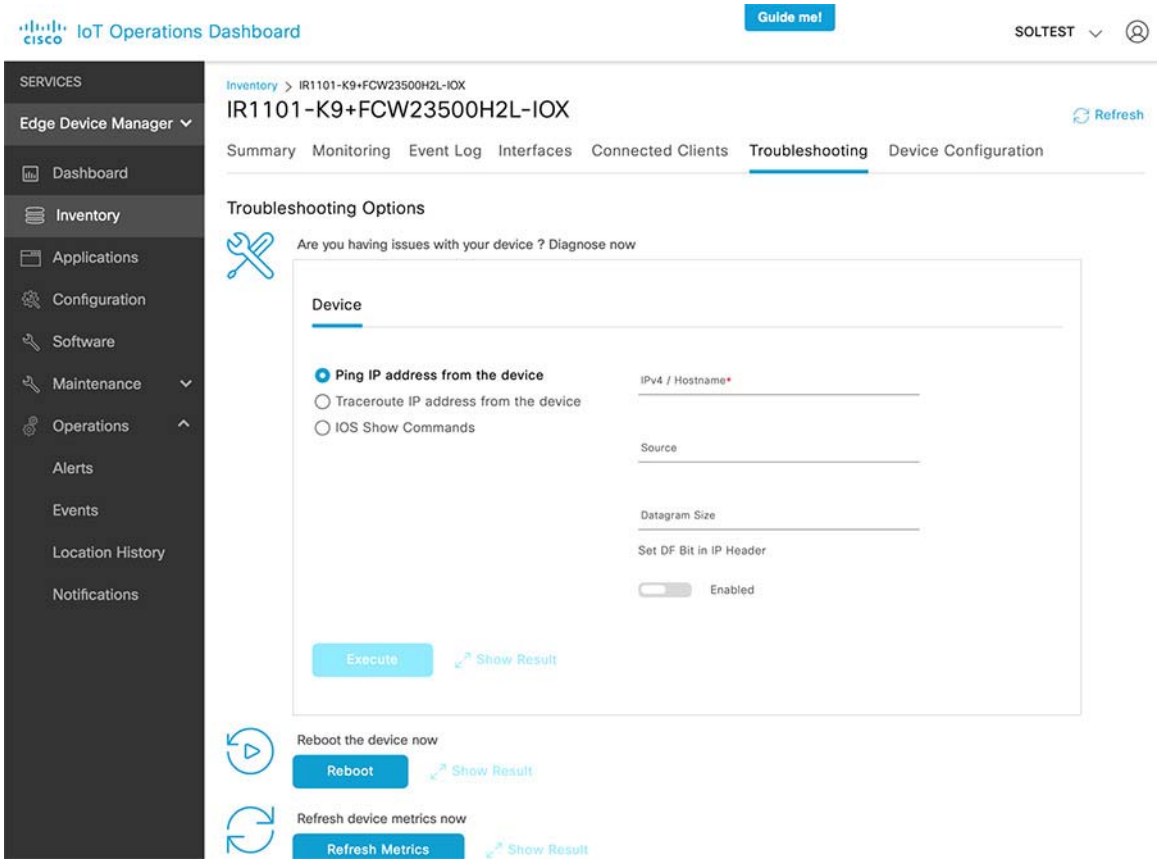


IOTOD Device Troubleshooting

From the device troubleshooting page for onboarded/registered devices on IOTOD these various troubleshooting commands can be run.

- Use the **ping** option to check the reachability to Internet from IR1101 or to the shared services via CCI data tunnel
- Use the **traceroute** command radio button to check the packet path details from the IR1101 to destination.
- User can reboot the IR1101 from the IOTOD dashboard as shown in the figure below.

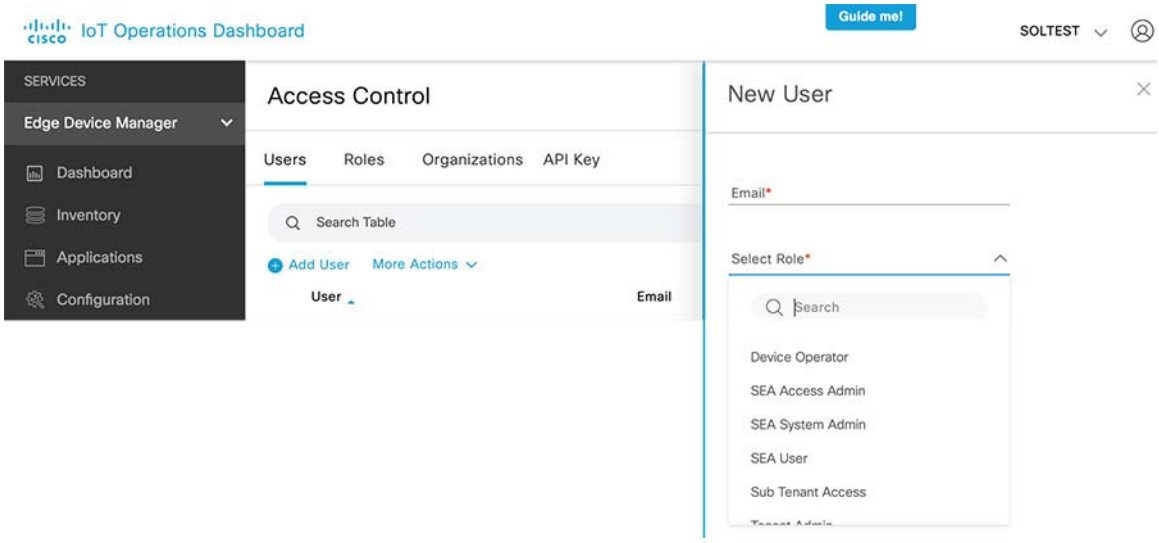
Figure 222 IOTOD troubleshooting page



Create a new user on IOTOD or delete an existing user

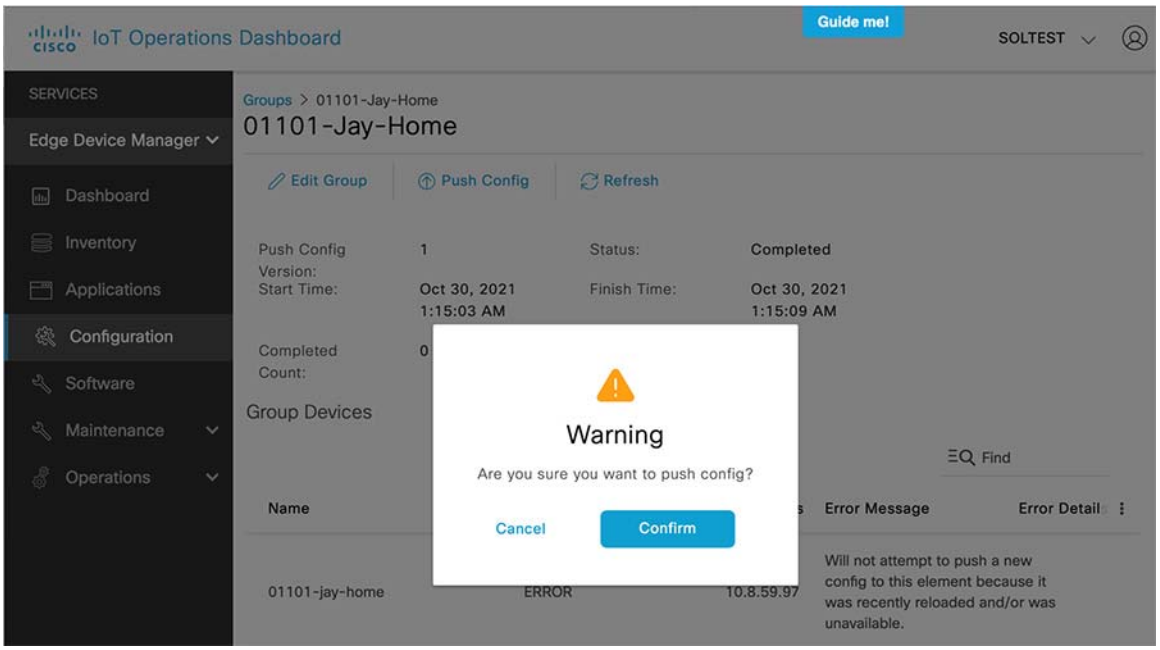
The Access control page lists the created users who have access to the tenant on IOTOD. New users and their roles can be added from this page. Created users can be deleted from this page

Figure 223 Creating a new user



To modify changes to the configuration of the onboarded gateways, use the push config. The gateway control tunnel to IOTOD has to be up to push updated config to gateways.

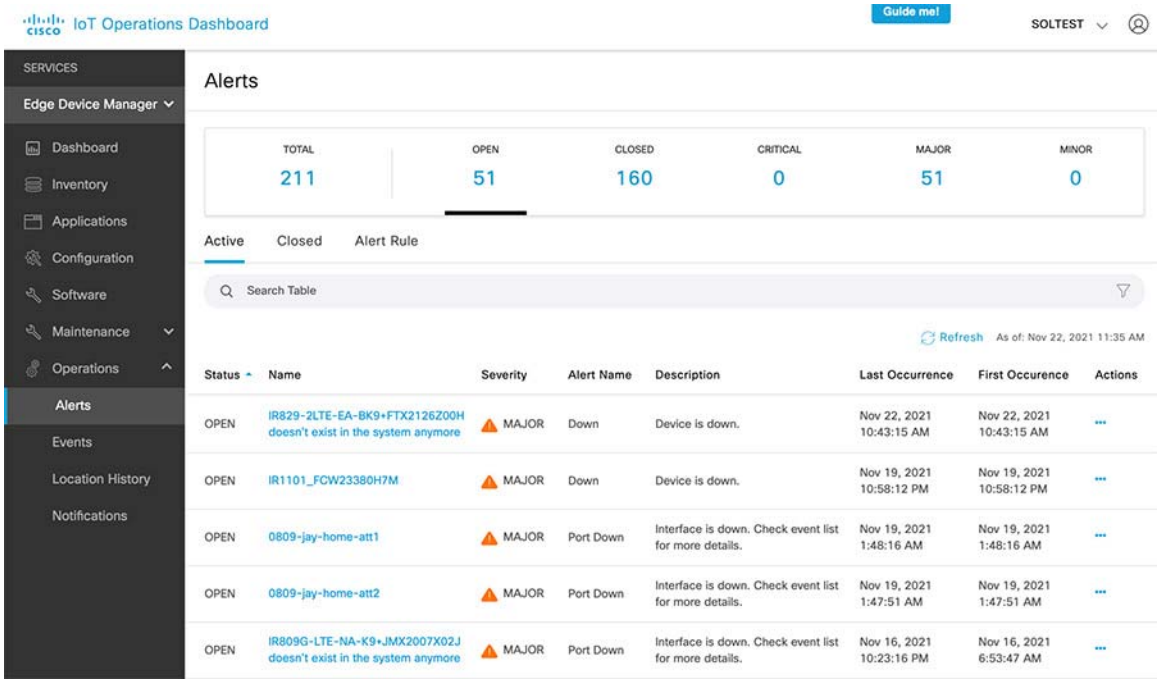
Figure 224 Push config



IOTOD Alerts

The alerts page under the operations tab shows the alerts generated for gateways under the tenant the current user. Alerts can be in active or closed state indicating if the gateway has recovered from this alert condition or not. You can close an alert from this page.

Figure 225 IOTOD alerts

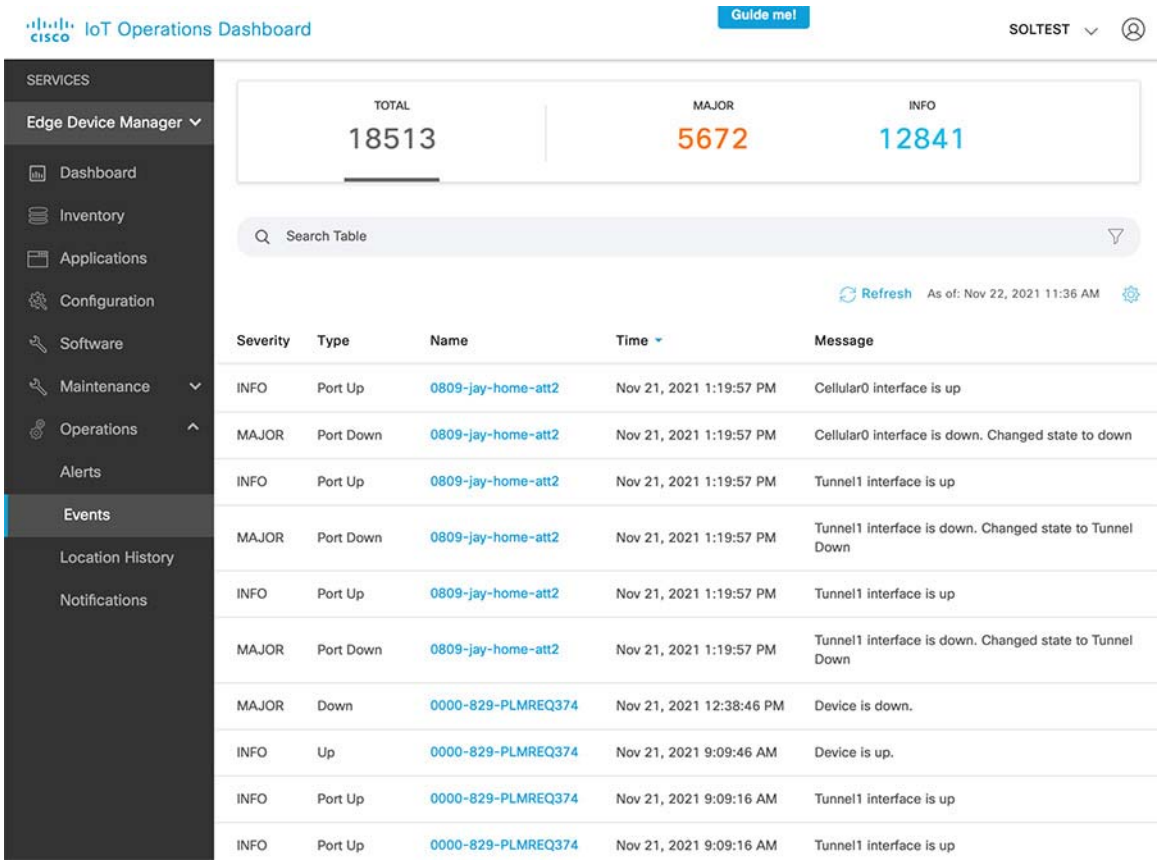


IOTOD events

The event section under the Operations page shows the events generated for all the gateways under the present tenant. The event section shows more details for alerts. but have more details

From the below figure, The events are generated after the control tunnel to IOTOD goes down and shows the time at which the IR1101 went offline.

Figure 226 IOTOD events



Configure the switchport of the gateway connected to the IE Switch as trunk.

In the DHCP scope of the Management vlan (Vlan 100 in this case), point DHCP option 43 with the IP address of DNA Center. This PnP will discover the IE switch.

Execute the following steps on the extended node switch before starting the onboarding processC that connects the IE Switch to the switchport of the remote gateways,. execute the following steps on the extended node switch before starting the onboarding process:

```
delete /force sdflash:vlan.dat
delete /force sdflash:*.cer
delete /force sdflash:pnp*
delete /force /recursive sdflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pnp-tech-time
delete /f flash:pnp-tech-discovery-summary #Delete all the certificates in NVRAM delete /f nvram:*.cer
#Clear the crypto certificates in config mode crypto key zerosize
no crypto pki certificate pool
#Change the VTP mode to Transparent in config mode vtp mode off
vtp mode transparent exit
#Do write erase and reload
write erase
reload (enter no if asked to save)
```

After the device discovery is complete, assign the device from Unassigned Devices to the respective Site. Notice that the device becomes the Managed node.

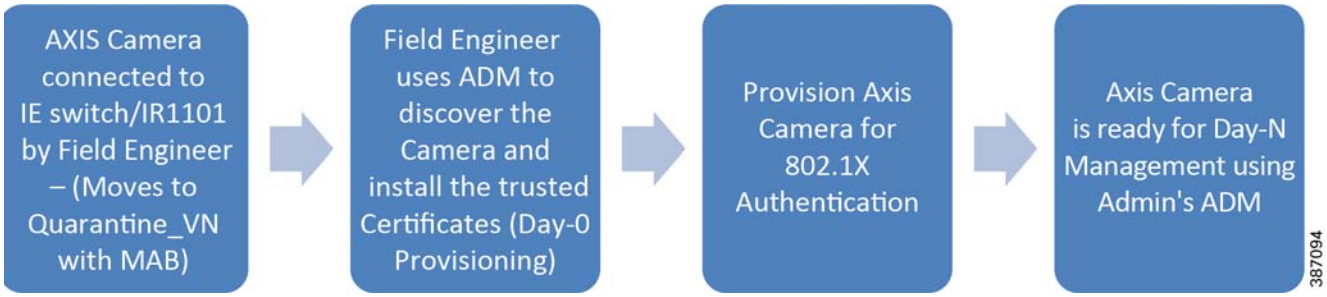
Now provision the IE Switches with <<RPoP Dot1x_MAB Template>> and <Host Onboarding> templates.

AXIS Camera Onboarding in CCI Network

The flow in Figure 245 shows the sequence for Axis Camera Onboarding in CCI Network. For more information, refer to the “Axis Camera Onboarding in CCI” section in the Connected Communities Infrastructure Design Guide at:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

Figure 227 Axis Camera Onboarding Sequence



Day-0 Camera Provisioning by a Field Engineer

1. In this stage, FE connects a brand new AXIS camera to:
   - IE switches access PoE port in the case of CCI PoP

- IR1101 FastEthernet port with PoE power injector in the case of CCI RPoP

2. Now the cameras are authenticated using the MAB method and the switch port is assigned a Quarantine_VN VLAN by ISE as per the available Authorization profile for MAB. Camera gets an IP from Quarantine VLAN IP pool from centralized DHCP server dedicated for Quarantine Network.

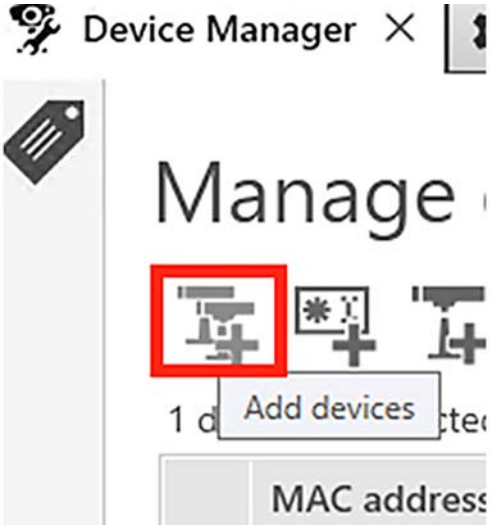
Figure 246 shows the Axis Camera is successfully authenticated using MAB and the respective Authorization policy is applied.

Figure 228 Axis Camera MAB Authentication

ADM Discovery for Day-0 Provisioning:

3. The Field Engineer connects their laptop to an IE switch in the access ring where the Axis camera is connected. FE discovers the Axis Camera which are part of Quarantine_VN by searching the network selecting **Device Manager-> Manage Devices -> Add devices**, as shown in Figure 247.

Figure 229 ADM Discovery of AXIS Camera in Quarantine_VN



4. Once the Camera is discovered, FE sets the password for the camera and shares it with admin.

5. FE must navigate to Device manager tab of ADM, right click on the camera, and click on **Enable /Update** on **IEEE 802.1X** option as shown in Figure 248.

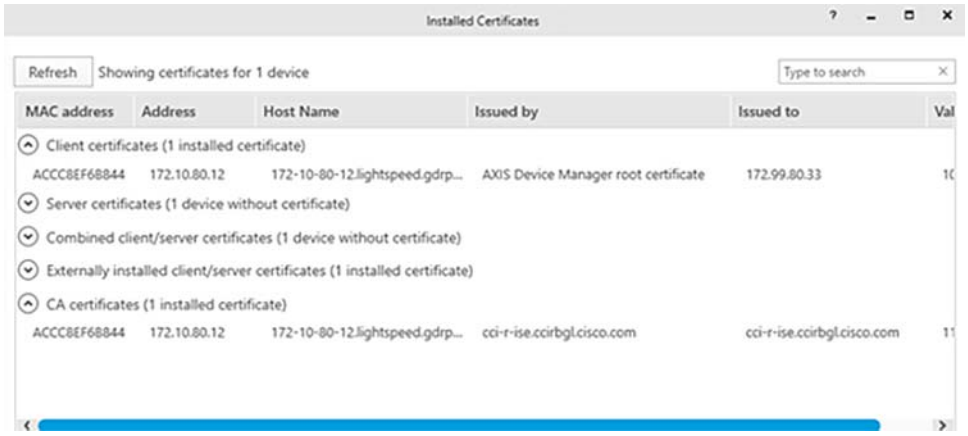
Configure the switchport of the gateway connected to the IE Switch as trunk.

Figure 230 Enabling 802.1x on AXIS Camera

This step installs the Root-CA and client certificates on the camera and enables the 802.1X.

6. The Camera certificates can be verified by right clicking on the camera and navigating to **Security->Certificates-> View installed certificates**. The device should have the client and CA certificates installed [optional].

Figure 231 Verifying Certificates



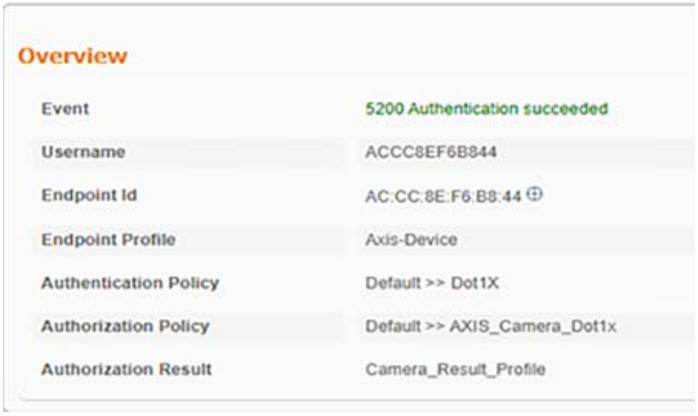
802.1X Authentication of the Camera:

7. At this stage the camera (802.1Xsupplicants) initiates the 802.1X process. Upon successful verification of certificates, the ISE authorizes the cameras and switch port in the network and assigns a VLAN (e.g., a subnet in SnS_VN) configured in an Authorization profile in ISE. Camera gets an IP from SnS_VN vlan IP pool from centralized CCI DHCP server.

It can be verified from RADIUS live logs on ISE that the Axis Camera is successfully authenticated using 802.1X and the respective Authorization policy is applied [optional] as shown in Figure 250.

Configure the switchport of the gateway connected to the IE Switch as trunk.

Figure 232 AXIS Camera 802.1x Authentication



Day-N Management of Axis Camera in CCI

Day N management involves:

- Discovering the cameras in the ADM in CCI Shared Service network by a central network administrator or simply admin.
- Day N Operations on the cameras like camera firmware upgrade, resolution setting, QoS configurations, etc., Refer to the Axis guide for more details on Day N operations which can be done using ADM.

Axis Camera Discovery in ADM by Admin

1. The Administrator now discovers the Axis Camera which are part of trusted SnS_VN by by clicking on **Add Devices** from an IP range under **Managed Devices** and entering the camera password (set by FE in step 4).

Figure 233 ADM Discovery of AXIS Camera in SnS_VN

2. Once the devices are discovered, select all the device(s) and follow the wizard to add the devices.
3. The cameras will be listed in the **Device Manager** tab with status OK as shown in Figure 252.

Figure 234 Discovered Cameras

Note: The FE must connect his laptop to the same switch as that of cameras or to any other switch of the same ring.

Note: Cameras are searched using IP range for quick discovery of camera for Day N management while the first option under Manage Devices is used in Day 0 management of cameras by Field Engineer.

Configure the switchport of the gateway connected to the IE Switch as trunk.

Upgrading Camera Firmware Using ADM

Once the cameras have been onboarded, the admin's ADM can be used to upgrade camera firmware to the latest available version for Day N management of cameras.

Figure 235 Upgrading Camera Firmware

For details on using ADM for camera upgrades refer to:

- https://www.axis.com/en-in/products/axis-device-manager/support-and-documentation

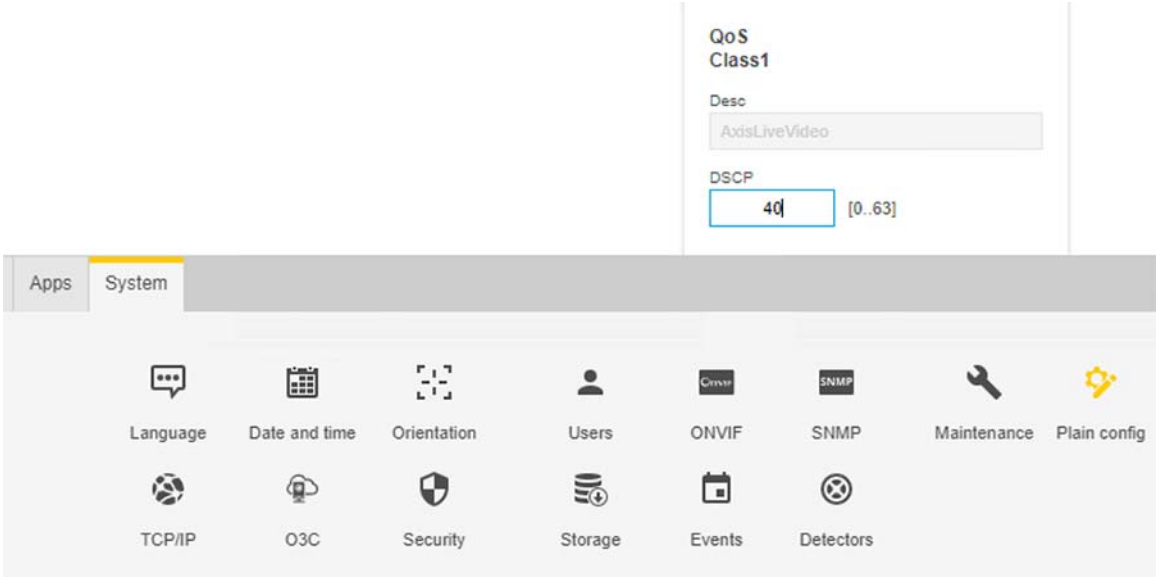
QoS Configuration:

For each type of network traffic supported by Axis Camera, you can enter a (Differentiated Services Codepoint (DSCP) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Follow the below steps to configure the QoS to DSCP 40.

1. On AXIS Camera from web browser, click the **Settings** option from bottom right corner and navigate to the System tab.
2. Select **PlainConfig->Network->QoS**.
3. Under QoS heading, set the DSCP value for class 1 as 40.
4. Then scroll down to the bottom to find and click the option **Save** to save the changes

Figure 254 shows the configuring DSCP value to 40 on the Axis Camera.

Figure 236 AXIS Camera QoS Settings



Data Center and Cloud Applications Implementation for Vertical Use Cases

This section covers the implementation of all Cisco and Partner-specific applications required in the CCI data center for vertical use cases. Cities Safety and Security applications, CIMCON street lighting management applications with Cisco Kinetic for Cities (CKC) integration, implementation of Schneider Electric, and Iteris partner applications for Roadways are a few of the vertical solutions validated in this CVD.

This chapter includes the following major topics:

Implementation of Cities Safety and Security Solution on CCI

Axis Camera Use Case Implementation in CCI

Axis communications offers a wide portfolio of IP-based products for security and video surveillance. Axis network cameras integrate easily and securely with CCI to build a complete security, video surveillance, and video analytics-based use case solution in CCI. To learn more about Axis cameras, refer to:

- https://www.axis.com/en-in/products/network-cameras

The main components of AXIS solution are,

- Axis Device Manager (ADM)—An on-premise tool that delivers an easy, cost-effective, and secure management of Axis devices. For more information, see: https://www.axis.com/en-in/products/axis-device-manager/.
- Axis Network Cameras—Robust outdoor cameras that provide excellent High-Definition (HD) image quality regardless of lighting conditions and the size and characteristics of the monitored areas.

This section describes Axis camera onboarding and management use case in CCI. The following two steps and roles are required for securely onboarding and Day-N management of the Axis cameras in CCI:

- Field Technician or Engineer (FT/FE)—An FE connects the camera to either PoP access ring or IR1101 Ethernet port in an RPoP for initial provisioning of the camera. FE uses Axis Device Manager (ADM) in their laptop/PC to discover cameras for initial provisioning, also known as Day 0 onboarding.
- Network Administrator—A central network administrator discovers the cameras using the ADM in CCI network after the successful authentication of the cameras in CCI for Day N management.

The following prerequisites should be completed prior to Axis camera onboarding by an FE:

- A separate Quarantine_VN created on in CCI to onboard untrusted hosts (in this case Axis Cameras before installing trust Certificates)
- The following ADM specific tasks must be completed by a FE prior to getting started with the onboarding of cameras:
  - Axis Camera is connected to one of IE switches access port in CCI PoP or IR1101 Ethernet port in case of an RPoP.
  - ADM installed and provisioned with CA certificate in FE's laptop/PC for Day 0 provisioning of cameras.
  - ADM application is deployed in CCI Shared Services network for Day N management by a Network Administrator (referred to as Administrator in this section).
  - ADM's CA certificate is shared with Administrator by FE for configuring it as trusted CA on ISE for successful 802.1X authentication.
  - FE will install ISE system certificate received from Administrator in his ADM as authentication server CA.
- Configure a separate DHCP server in Quarantine network for Cameras before Authentication.
- Access switches are configured with 802.1X and MAB profiles and applied to the switchports to which cameras are connected.
- Cisco ISE is configured with appropriate 802.1X and MAB authentication and authorization policies for the cameras in different sites.

Implementation Steps for the Prerequisites

1. A separate Quarantine_VN is created on Cisco DNA Center. For more information, see:

- https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/SD-Access-Distributed-Campus-Deployment-Guide-2019JUL.html#_Toc13487379

On the Fusion Router, using route-maps allows Quarantine_VN to communicate to ADM. Below is an example configuration on the Fusion router.

```
###SnS_VRF configuration with route-leaking###
vrf definition SnS_VN
 rd 1:4099
 !
 address-family ipv4
  import ipv4 unicast map CAMERA-NETWORK-TO-VRF
  export ipv4 unicast map SnS-VN-TO-GLOBAL
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family

###Route-map to import ADM network to SnS_VN###
route-map CAMERA-NETWORK-TO-VRF permit 10
 match ip address prefix-list SHARED_SERVICES_NETS ADM_NETS

###Route-map to import SnS_VN network to ADM###
route-map SnS-VN-TO-GLOBAL permit 10
 match ip address prefix-list SnS_VN_ROUTES

###Prefix-list matching ADM network###
ip prefix-list ADM_NETS seq 1 permit 10.10.99.0/24

###Prefix-list matching SnS_VN network for different PoP sites###
ip prefix-list SnS_VN_ROUTES seq 29 permit 172.16.70.0/24
ip prefix-list SnS_VN_ROUTES seq 34 permit 172.9.90.0/24
```

2. Install and configure ADM.

In CCI solution, management of cameras uses two instances of ADM:

- FE's laptop/PC has an instance of ADM for Day 0 provisioning of cameras.
- An ADM instance deployed in shared services for Day N management of cameras by CCI administrator.

ADM installation

The download link and the software requirements can be found at the following URL under Download and release notes options respectively:

- https://www.axis.com/en-in/products/axis-device-manager

After installation, start the ADM client and log on, selecting the local computer as the server.

Configuring and Generating CA Certificate on ADM and ISE

In CCI, ADM is used as CA for issuing client certificates to Axis cameras and ISE is used as RADIUS authentication server. For a detailed explanation on the configuration steps of ADM as CA for Axis cameras, refer to:

- https://www.axis.com/files/tech_notes/How_to_ADM_IEEE-802_1X_T85_FreeRADIUS_en.pdf

For successful 802.1X authentication, ISE must be configured to trust the certificates issued by ADM to the cameras and ADM must have ISE (authentication server) certificates installed. For completing these steps, the FE works closely with the Administrator on the steps discussed in this section.

The steps have been categorized into two parts for simplicity:

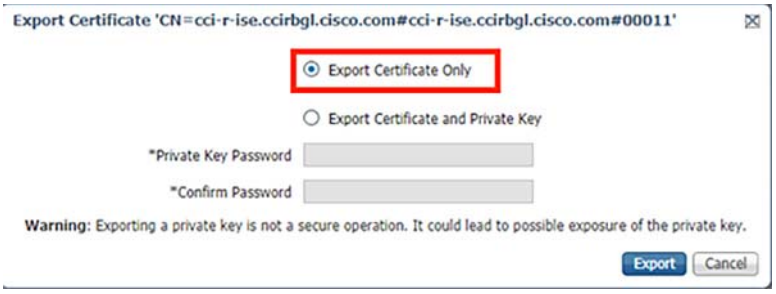
- Exporting ISE's certificate for configuration in ADM

- Exporting ADM's CA certificate for configuration in ISE

Exporting ISE's Certificate for Configuration in ADM

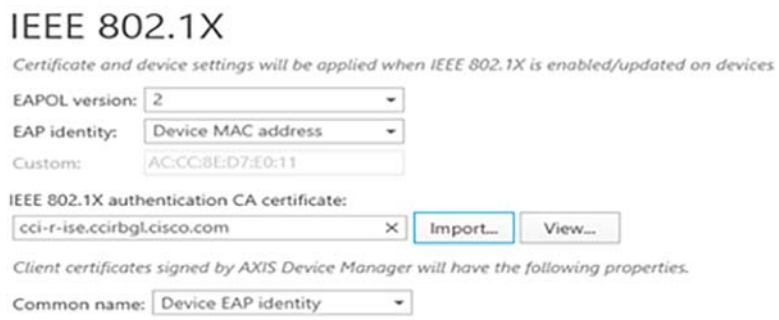
1. The Administrator logs onto ISE and exports the System Certificate which is being used for EAP authentication (EAP authentication checkbox is enabled for the certificate under **Usage**). This can be found on ISE by navigating to **Administration -> System -> Certificates -> System Certificates**. Export the certificate without the private key as shown in the Figure 237. Rename the certificate from <cert_name>.pem to <cert_name>.cer and share this certificate with the FE.

Figure 237 Exporting ISE's Authentication Server Certificate



2. On the ADM configuration tab, import the ISE's certificate obtained from step 1 as authentication CA as shown in Figure 238.

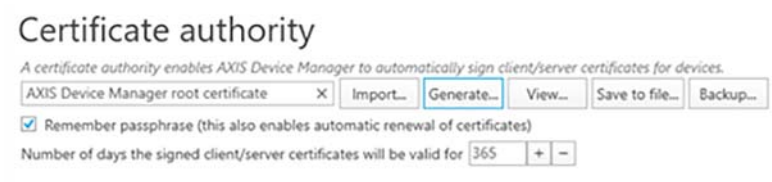
Figure 238 Configuring ISE as Authenticating CA



Exporting ADM's CA Certificate for Configuration in ISE

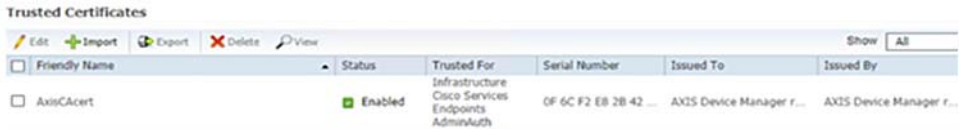
1. FE will use his ADM to navigate to **Configuration -> Security -> Certificates**. Under **Certificate authority**. click on **Generate**. Enter the passphrase of choice for the certificate. A CA certificate for ADM will be generated and will appear as shown in Figure 239. Save this certificate and share tit with the central admin.

Figure 239 Configuring ADM as CA for Axis Cameras



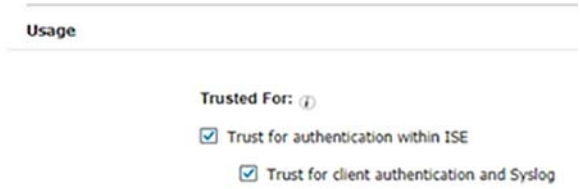
2. The Administrator will add the received certificate of FE's ADM from step 2 in the trusted certificate list of ISE by going to **Administration -> System -> Certificates -> Trusted Certificates** and then clicking on **Import** followed by choosing the ADM's certificate .The certificate will appear in the trusted certificate list as shown in Figure 240.

Figure 240 Adding ADM Certificate in ISE Trusted Certificates



3. The Administrator will verify that for the certificate imported in ISE in step 2, **Trust for client authentication** checkbox is enabled. This can be found in the **Edit** option under **Usage** for the certificate in the Trusted Certificate repository of ISE.

Figure 241 Trusting ADM Certificate for Client Authentication



4. A separate DHCP server is deployed in the ADM network (for example, VLAN 99, 10.10.99.x). Refer to Configuring DHCP and DNS Services, page 43 and configure a separate DHCP server for clients connected to Quarantine_VN. Push the NTP details with Option 042.

5. To configure access switches with 802.1X and MAB profiles and apply to the switchports to which cameras are connected, refer Endpoints Security Using 802.1X and MAC Authentication Bypass, page 366.

6. To configure Cisco ISE with appropriate 802.1X and MAB authentication and authorization policies for the cameras, refer to Endpoints Security Using 802.1X and MAC Authentication Bypass, page 366.

7. The conditions that should match for 802.1X are Network Access:EapAuthentication to EAP-TLS and Wired_802.1x as shown in Figure 242. Once created, apply to the policy set as shown in Figure 243.

8.

Figure 242 Cisco ISE 802.1X Policy Rules for Axis Camera Onboarding

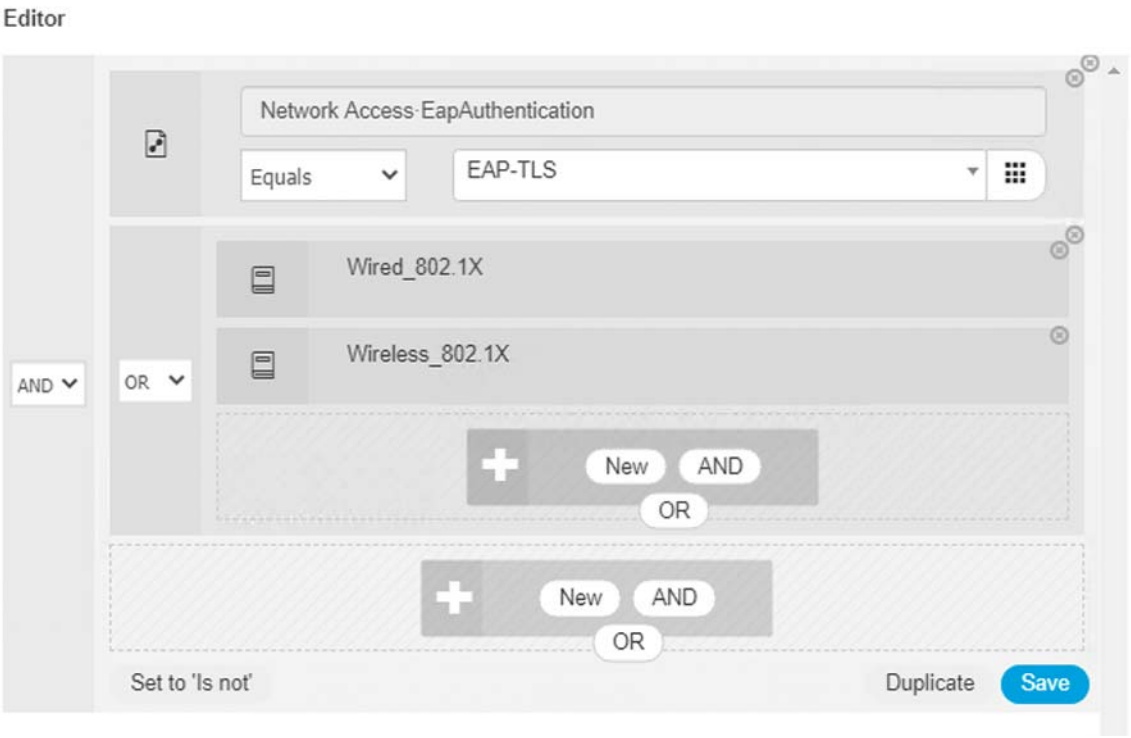
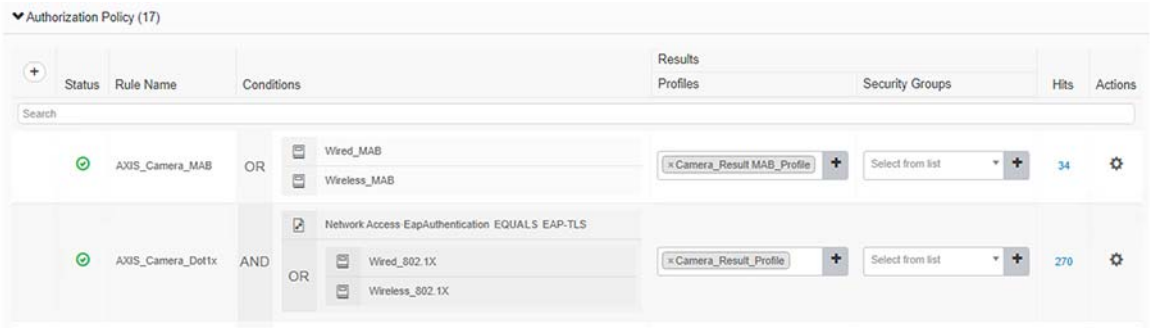


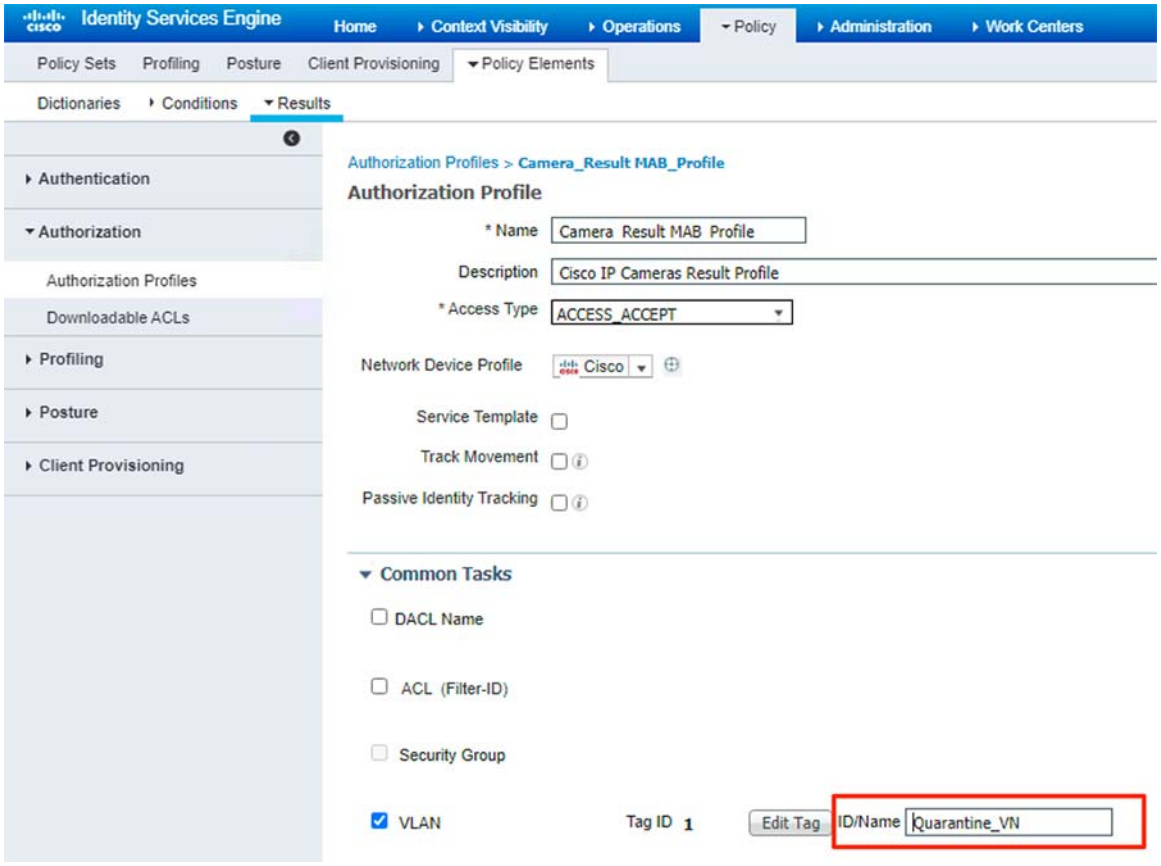
Figure 243 Cisco ISE 802.1X and MAB Authorization Polices for Axis Cameras



Note: In Multi-Site Fabric deployments, maintain the same VLAN names (as shown in Figure 244) across the sites in order to make Authorization Profile to work for all cameras connected across different sites.

Figure 244 shows the Authorization Policy for MAB profile with common VLAN name (Quarantine_VN).

Figure 244 Authorization Profile on ISE with Common VLAN Name

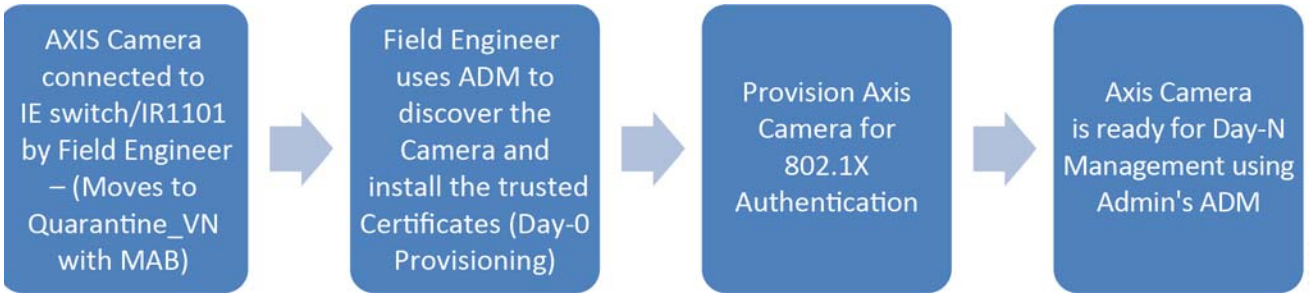


AXIS Camera Onboarding in CCI Network

The flow in Figure 245 shows the sequence for Axis Camera Onboarding in CCI Network. For more information, refer to the “Axis Camera Onboarding in CCI” section in the Connected Communities Infrastructure Design Guide at:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

Figure 245 Axis Camera Onboarding Sequence



Day-0 Camera Provisioning by a Field Engineer

1. In this stage, FE connects a brand new AXIS camera to:

- IE switches access PoE port in the case of CCI PoP
- IR1101 FastEthernet port with PoE power injector in the case of CCI RPoP

2. Now the cameras are authenticated using the MAB method and the switch port is assigned a Quarantine_VN VLAN by ISE as per the available Authorization profile for MAB. Camera gets an IP from Quarantine VLAN IP pool from centralized DHCP server dedicated for Quarantine Network.

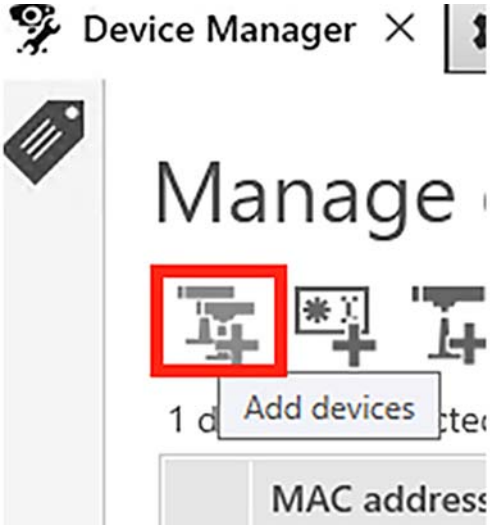
Figure 246 shows the Axis Camera is successfully authenticated using MAB and the respective Authorization policy is applied.

Figure 246 Axis Camera MAB Authentication

ADM Discovery for Day-0 Provisioning:

3. The Field Engineer connects their laptop to an IE switch in the access ring where the Axis camera is connected. FE discovers the Axis Camera which are part of Quarantine_VN by searching the network selecting **Device Manager-> Manage Devices -> Add devices**, as shown in Figure 247.

Figure 247 ADM Discovery of AXIS Camera in Quarantine_VN



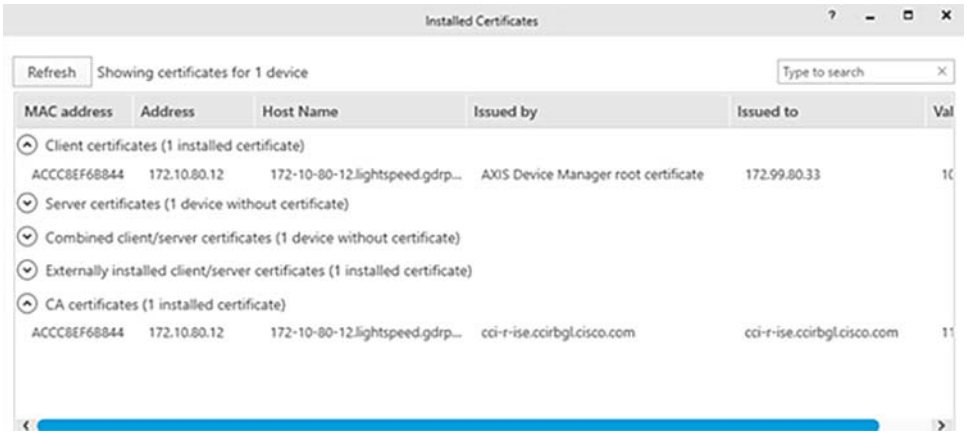
4. Once the Camera is discovered, FE sets the password for the camera and shares it with admin.
5. FE must navigate to Device manager tab of ADM, right click on the camera, and click on **Enable /Update** on **IEEE 802.1X** option as shown in Figure 248.

Figure 248 Enabling 802.1x on AXIS Camera

This step installs the Root-CA and client certificates on the camera and enables the 802.1X.

6. The Camera certificates can be verified by right clicking on the camera and navigating to **Security->Certificates-> View installed certificates**. The device should have the client and CA certificates installed [optional].

Figure 249 Verifying Certificates

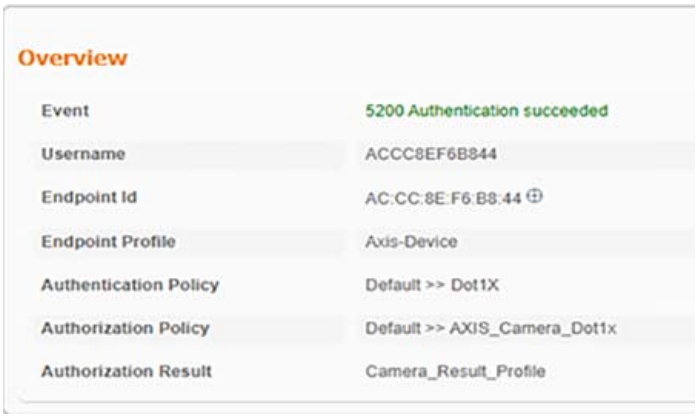


802.1X Authentication of the Camera:

7. At this stage the camera (802.1Xsupplicants) initiates the 802.1X process. Upon successful verification of certificates, the ISE authorizes the cameras and switch port in the network and assigns a VLAN (e.g., a subnet in SnS_VN) configured in an Authorization profile in ISE. Camera gets an IP from SnS_VN vlan IP pool from centralized CCI DHCP server.

It can be verified from RADIUS live logs on ISE that the Axis Camera is successfully authenticated using 802.1X and the respective Authorization policy is applied [optional] as shown in Figure 250.

Figure 250 AXIS Camera 802.1x Authentication



Day-N Management of Axis Camera in CCI

Day N management involves:

- Discovering the cameras in the ADM in CCI Shared Service network by a central network administrator or simply admin.
- Day N Operations on the cameras like camera firmware upgrade, resolution setting, QoS configurations, etc., Refer to the Axis guide for more details on Day N operations which can be done using ADM.

Axis Camera Discovery in ADM by Admin

1. The Administrator now discovers the Axis Camera which are part of trusted SnS_VN by by clicking on **Add Devices** from an IP range under **Managed Devices** and entering the camera password (set by FE in step 4).

Figure 251 ADM Discovery of AXIS Camera in SnS_VN

2. Once the devices are discovered, select all the device(s) and follow the wizard to add the devices.
3. The cameras will be listed in the **Device Manager** tab with status OK as shown in Figure 252.

Figure 252 Discovered Cameras

Note: The FE must connect his laptop to the same switch as that of cameras or to any other switch of the same ring.

Note: Cameras are searched using IP range for quick discovery of camera for Day N management while the first option under Manage Devices is used in Day 0 management of cameras by Field Engineer.

Upgrading Camera Firmware Using ADM

Once the cameras have been onboarded, the admin's ADM can be used to upgrade camera firmware to the latest available version for Day N management of cameras.

Figure 253 Upgrading Camera Firmware

For details on using ADM for camera upgrades refer to:

- https://www.axis.com/en-in/products/axis-device-manager/support-and-documentation

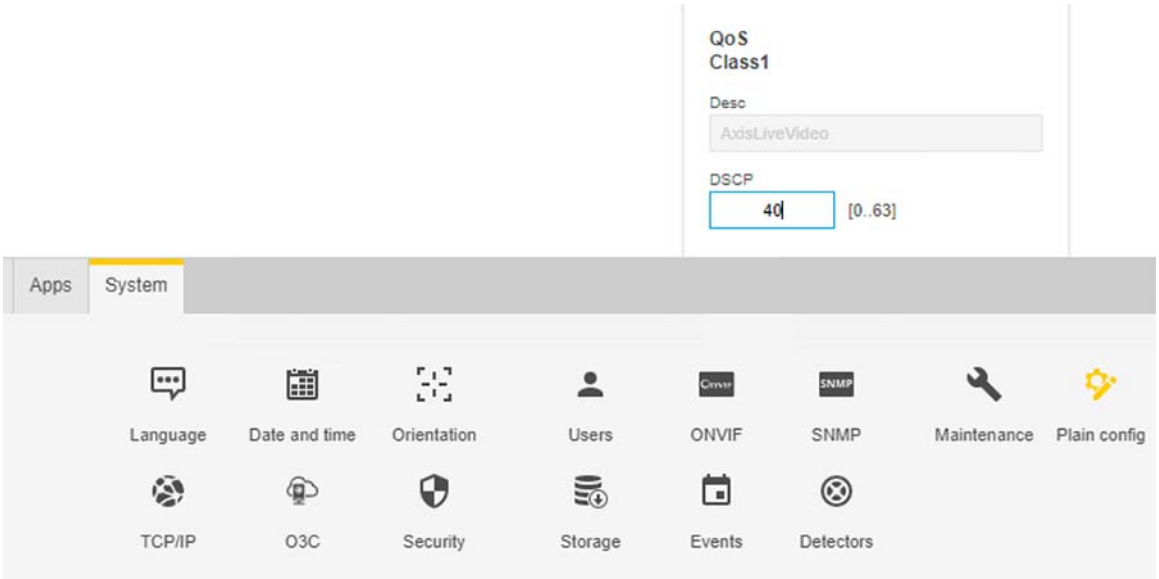
QoS Configuration:

For each type of network traffic supported by Axis Camera, you can enter a (Differentiated Services Codepoint (DSCP) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Follow the below steps to configure the QoS to DSCP 40.

1. On AXIS Camera from web browser, click the **Settings** option from bottom right corner and navigate to the System tab.
2. Select **PlainConfig->Network->QoS**.
3. Under QoS heading, set the DSCP value for class 1 as 40.
4. Then scroll down to the bottom to find and click the option **Save** to save the changes

Figure 254 shows the configuring DSCP value to 40 on the Axis Camera.

Figure 254 AXIS Camera QoS Settings



Partner Applications Implementations

This section covers the implementation of partner applications validated in this CVD for Cities and Roadways verticals on the CCI network.

Integrating Cisco Headend with CIMCON Cloud Service

To communicate securely between Cisco and CIMCON networks, this solution uses site-to-site FlexVPN establishment between the CIMCON LightingGale cloud service and the Cisco Headend. FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub and spoke topologies, and partial meshes (spoke-to-spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps.

To learn more about FlexVPN, refer to the following URL:

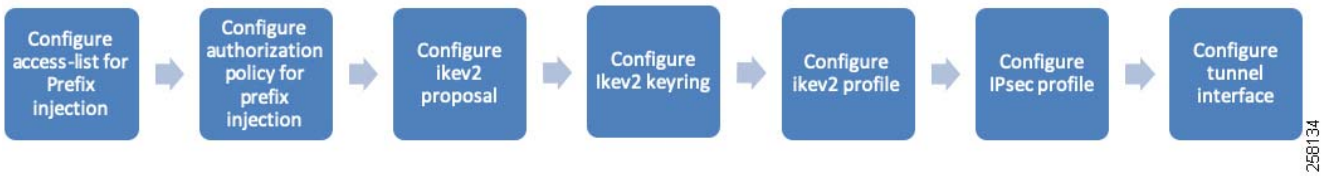
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-flex-vpn-15-mt-book/sec-intro-ikev2-flex.pdf

For the purpose of tunnel establishment, the following prerequisite information must be known beforehand:

1. CCI solution network's public IP
2. CIMCON LightingGale cloud service router public IP

To configure the tunnel, the steps to follow are shown in Figure 255.

Figure 255 Configuring Secure Communication between Cisco Headend and CIMCON LG Network



We will begin with bringing up the tunnel on the Cisco Headend side first followed by the tunnel configuration on CIMCON LG cloud service router.

1. Configure access-list for Prefix Injection

In order to dynamically send routes, the prefix-Injection method is used. First, an access-list of the routes that have to be propagated through the tunnel must be created, as shown in the following example:

```
ipv6 access-list NETipv6-list
 permit ipv6 2001:BEED::/64 any
```

The above example propagates the WPAN prefix over the tunnel.

2. Configure Authorization Policy for Prefix Injection

The next step in prefix-Injection is to create an authorization policy, as shown in the example below:

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list NET-list
 route set access-list ipv6 NETipv6-list
!
```

3. Configure IKEv2 Proposal

Next, the encryption, integrity, and group is selected by creating a proposal:

```
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
```

```
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
```

4. Configure IKEv2 Keyring

Configure the pre-shared key - Internet Key Exchange version 2 (IKEv2) keyring:

```
crypto ikev2 keyring mykeys
 peer CISCO-Router
  address <public ip of CIMCON LG cloudservice router>
  pre-shared-key CiscoCSR123
 !
```

5. Configure IKEv2 Profile

Next, the IKEv2 profile is created to match the remote host and to configure authentication and authorization, as shown in the example below:

```
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match identity remote address <public ip of CIMCON LG cloudservice router> 255.255.255.255
 match identity remote fqdn CSR.cimcon.com
 identity local fqdn CSR.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local mykeys
 aaa authorization group psk list mylist default
!
```

6. Configure IPSec Profile

The next step is to create an IPSec profile, as shown in the example below:

```
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
```

7. Configure Tunnel Interface

Finally, the tunnel interface to be used to building the tunnel is created, as shown in the example below:

```
interface Loopback110
 ip address 10.1.1.2 255.255.255.0
 ipv6 address 2001:DB:12::2/64
!
interface Tunnel110
 ip unnumbered Loopback110
 ipv6 enable
 tunnel source GigabitEthernet7
 tunnel destination <public IP of CIMCON LG cloud service router>
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
```

Repeat the above steps, but with necessary changes on the CIMCON LG cloud service router.

For more details on configuring the FlexVPN tunnel, refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html

CIMCON Lighting Management for Cities

CIMCON Lighting Management Application, which is called LightingGale, is one of the Cisco Smart Street Lighting solution partner's applications validated in this implementation on CCI network for the Smart Street Lighting vertical solution and its use cases.

Smart Street Lighting Management Using CIMCON LightingGale

As a prerequisite, the SLC nodes controlling via LightingGale (referred as LG throughout this document), LG cloud IP address, and the credentials must be obtained from the CIMCON team.

Once the cloud IP is obtained, the LG application can be accessed using the link on the browser.

Initial Steps in Controlling SLC Nodes

To begin the controlling of SLC nodes from the LG, the node must first be added using the SLC number listed on the back of the node (also obtained as a list from the CIMCON team along with CIMCON lights).

The following lists the high-level steps for adding a SLC node and controlling it via the LG. Refer to LG documentation provided by CIMCON for more detailed steps.

1. From the **LG** menu, select **Configurations-> SLC list**, as shown in Figure 256.

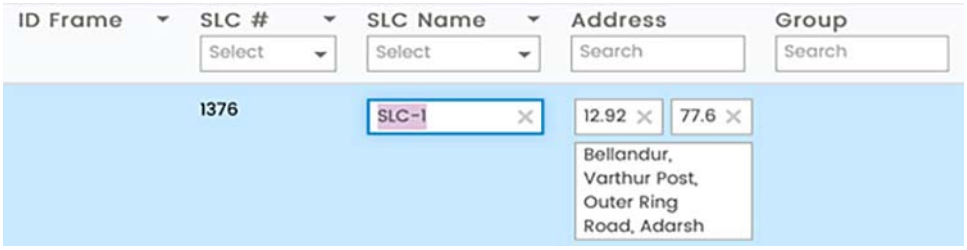
Figure 256 Adding a New SLC Node Configurations

2. Click **Add** from the bottom left, as shown in Figure 257:

Figure 257 Adding a New SLC Node View

3. Add the SLC details, including the latitude and longitude of the SLC node location in the tenant (configured in the CKC), as shown in Figure 258.

Figure 258 CIMCON LG Dialog Box for Adding SLC

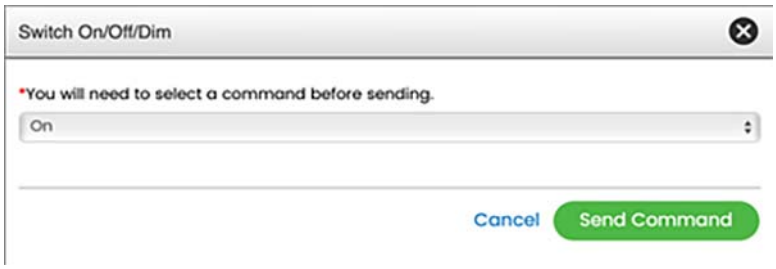


Performing ON/OFF/Dim on the SLC Nodes

Before performing the operations, ensure that SLC nodes are in manual mode. The following steps must be completed to perform the lighting control operations:

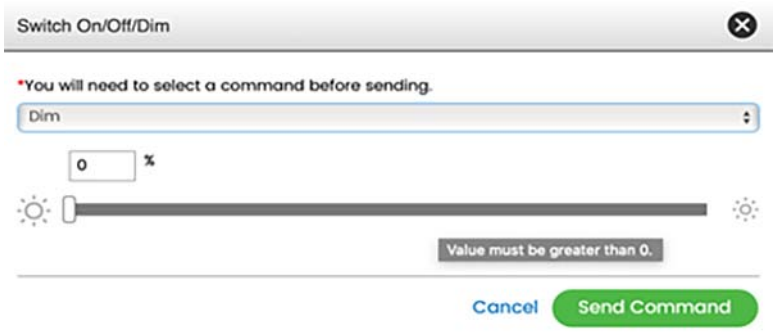
1. If mode is not manual, select **Commands-> SLC Commands** from the menu and then select the desired SLC and click on **Commands->mode->set**. Select **manual** from drop-down menu and save.
2. To perform ON/OFF/Dim, click on **Switch ON/Off/Dim** after ticking the checkbox against the desired SLC. Then select the operation as shown in Figure 259. Then Click **Send Command**.

Figure 259 Adding a Gateway



3. For dimming, select **Dim** from the drop down and slide the bar to the desired value. Then click **Send Command**, as shown in Figure 260.

Figure 260 Performing Dimming Operation



4. Finally, click on the read data from the top right corner.

Note: Cisco Solution Support includes troubleshooting to the edge of the network (SLC). Contact your service provider or manufacture for issues that may be discovered beyond the edge of the network.

Schneider Electric for Roadways

The Schneider Electric component of the solution comprises a UPS at the roadside edge, which is part of an edge fabric site. The UPS can communicate with the EcoStruxure application provided by Schneider Electric or some other monitoring software from a different vendor. When using the Schneider Electric software, the UPS will communicate with an application gateway in the data center fabric site, which, in turn, communicates with the EcoStruxure IT cloud application.

As part of the recommended fabric configuration, a VN is configured in Cisco DNA specifically for the Schneider Electric components. Using a separate VN for each service ensures that other services do not have access to the Schneider Electric components. When configuring the VN component in each fabric site, it is important to make sure that the same VN is used at the edge fabric as well as the data center fabric. This will ensure that the UPS at the edge can communicate with the application gateway.

To use the Schneider Electric EcoStruxure applications, an account must exist on the cloud application. Then an application gateway must be installed as a VM in the data center fabric. Afterward, the application gateway must be connected to the account in the EcoStruxure cloud application. When this is complete, the application gateway can discover the UPSs in all the edge fabric sites.

Once the UPS is provisioned and visible in the EcoStruxure application, alarms will show up as events happen. Those alarms can be seen on the UPS, application gateway, and cloud application.

Figure 261 Example Alarm from UPS

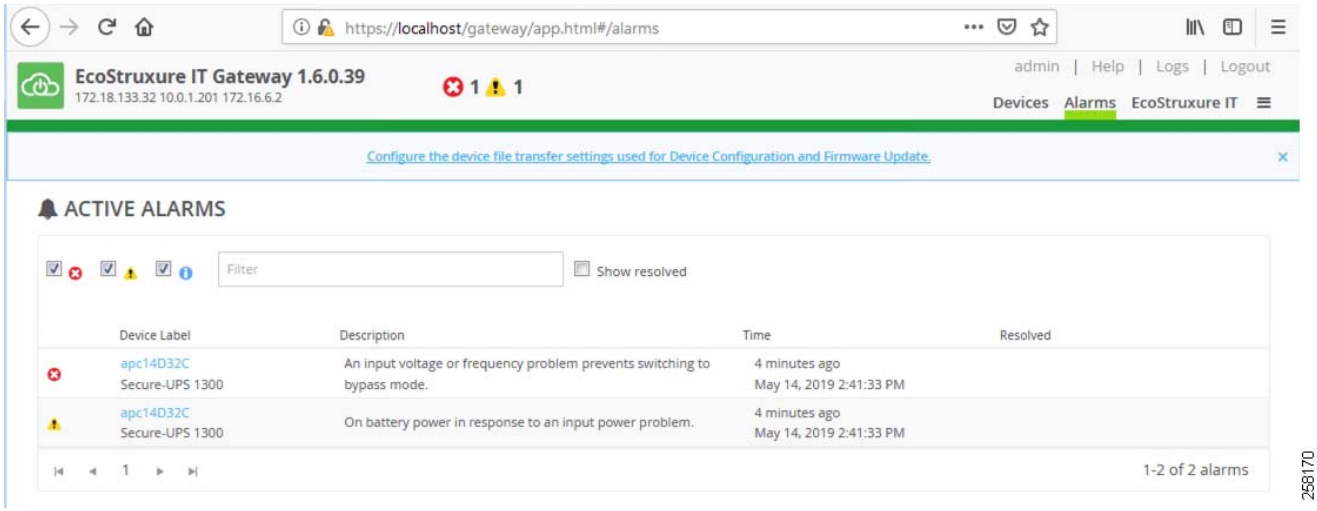


Figure 262 Example Alarm from EcoStruxure Application Gateway

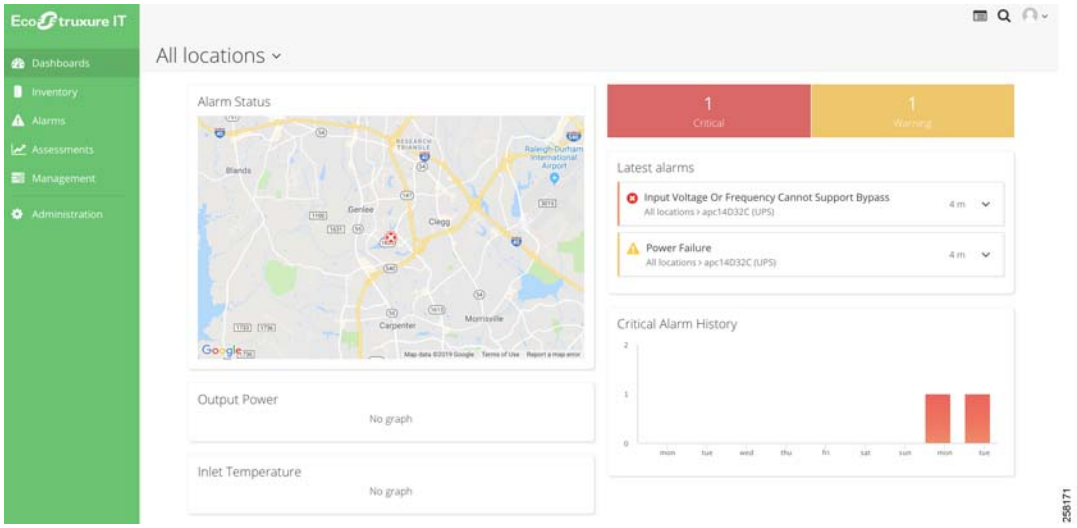


Figure 263 Example Alarm from EcoStruxure Cloud Application

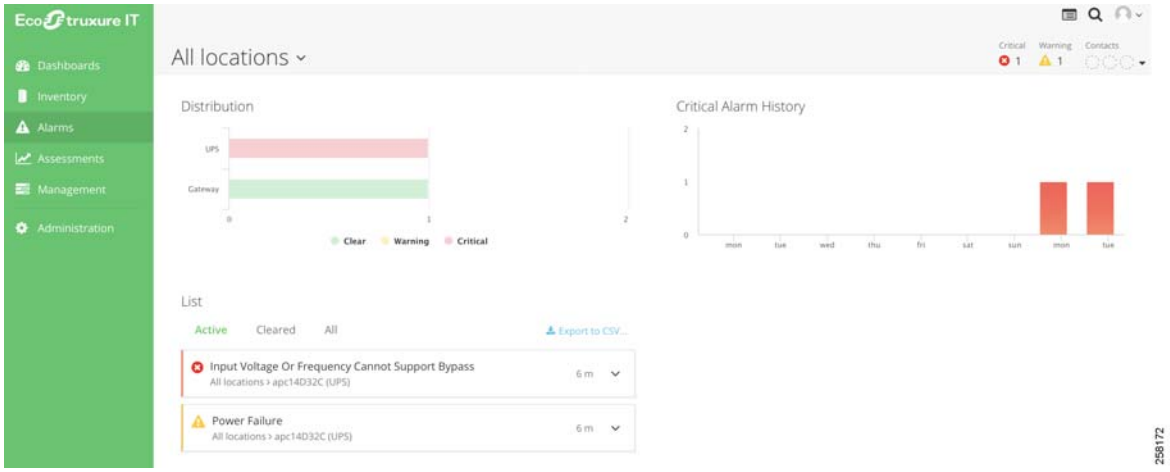


Figure 264 Another Alarm from EcoStruxure Cloud Application

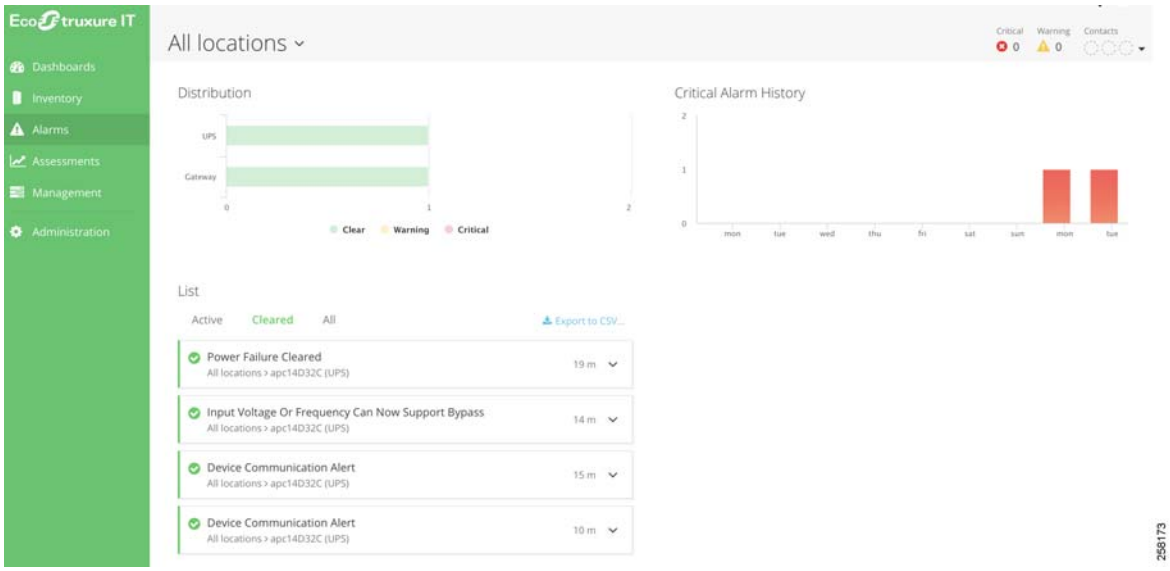


Figure 265 Example of Alarm Clearing on EcoStruxure Cloud Application

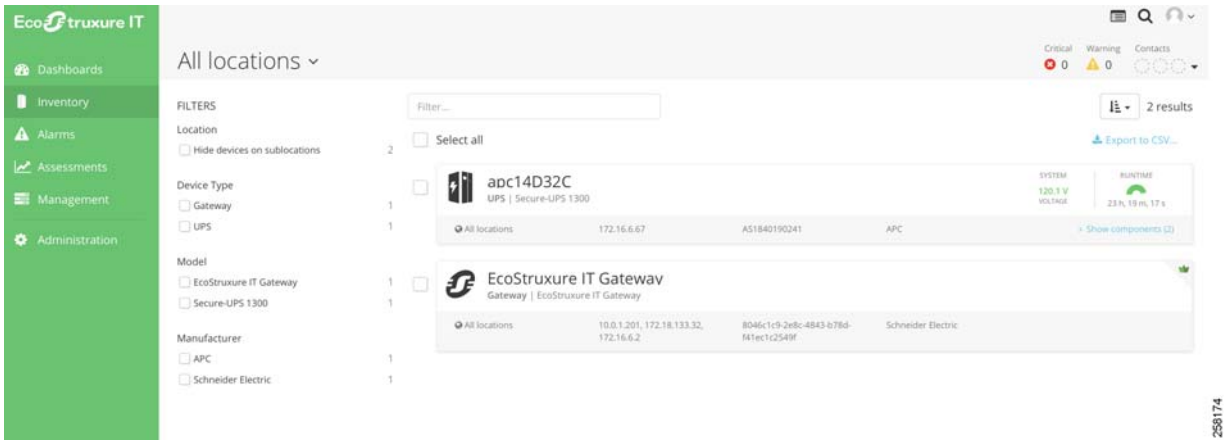
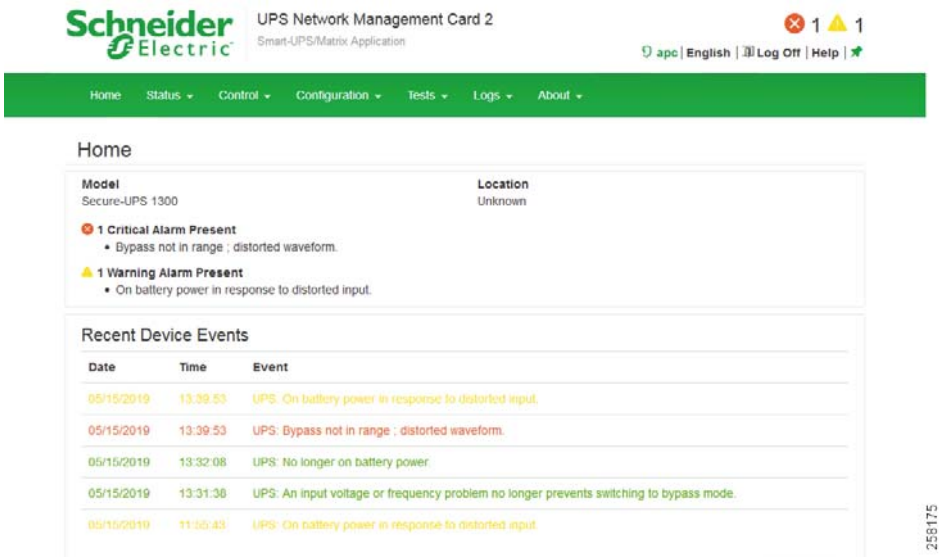


Figure 266 Example Showing Inventory from EcoStruxure Cloud Application



Iteris for Roadways

The Iteris component of the solution includes a video processing unit at the roadside edge, which is part of a local PoP site. The video can be viewed as an RTSP stream or incorporated into another traffic management software application. In this implementation, the video was viewed as an RTSP stream in the data center fabric site. Using Iteris software to manipulate or manage the traffic stream and incorporating the video into a traffic management software application are out of scope for this document. As part of the recommended fabric configuration, a VN is configured in Cisco DNA specifically for the Iteris components. Using a separate VN for each service ensures that other services do not have access to the Iteris components and vice versa. When configuring the VN component in each fabric site, it is important to make sure the same VN is used at the edge fabric as well as the data center fabric. This will ensure that the video server at the edge can communicate with the application in the data center fabric.

Integrating Wi-Fi Networks with DNA Spaces on Cloud

Cisco DNA Spaces is a powerful, end-to-end, in location services cloud platform that provides wireless customers with rich location-based services, including location analytics, business insight, customer experience management and cloud APIs.

It provides a single point of entry for all location technology and intelligence through a single dashboard interface. Cisco DNA Spaces delivers the industry's most scalable location-based marketing platform.

This section describes how to configure Cisco DNA Spaces with a 9800 controller using Direct Connection. Directly connecting the Catalyst 9800 is only advisable for small scale/single controller setups. For larger setups, Cisco recommends using the DNA Spaces Connector which improves the communication efficiency.

For more details, refer to the setup guide:

https://dnaspaces.cisco.com/setupguide

The section applies identically to all C9800 WLC deployments like eWLC C9800-SX installed on Catalyst platform, C9800-L, C9800-CL, C9800-40, and C9800-80.

Note: Make sure you have a Cisco DNA Spaces account with necessary licenses. Please check with your Cisco Sales Team or Partners to get account created and activates. Alternatively, check the URL https://dnaspaces.cisco.com/contact-us/ for more details.

Configurations:

To connect the controller to Cisco DNA Spaces, the controller must be able to reach Cisco DNA Spaces cloud over HTTPS.

Import the DigiCert CA Root Certificate into the WLC

If the WLC uses a root certificate not signed by DigiCert CA, one will see the **https: SSL certificate problem: unable to get local issuer certificate** error.

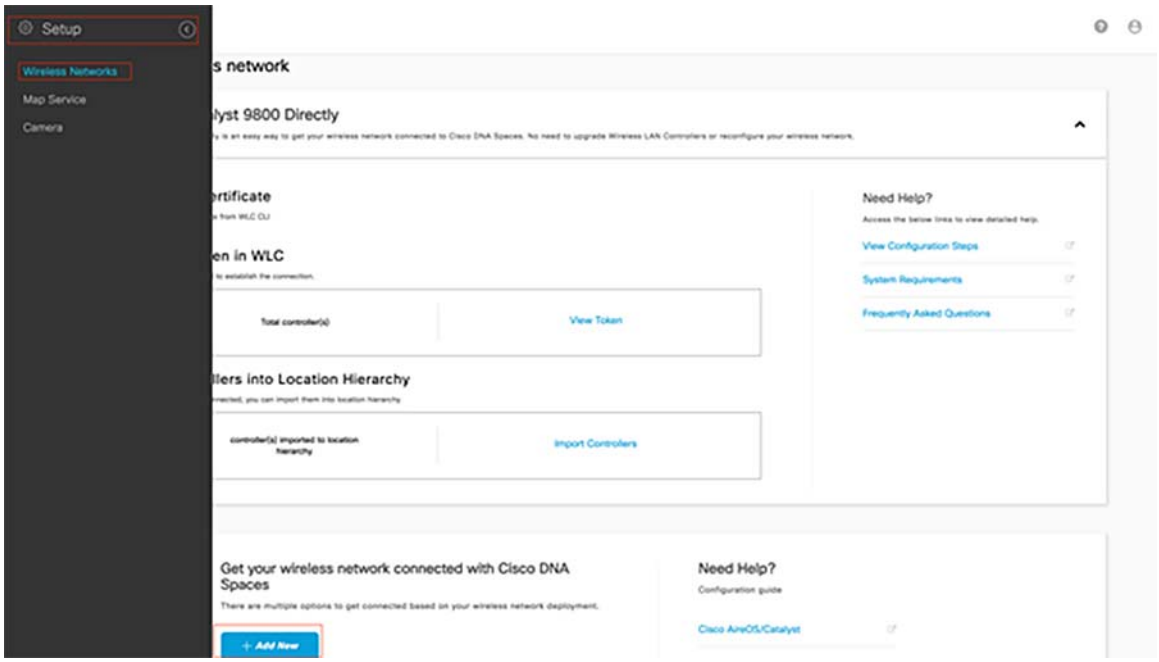
Step 1. Run these commands to configure the DNS server in the 9800 controller and import the certificate:

```
WLC(config)#ip name-server <server-ip>
WLC(config)#ip domain-lookup
WLC#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
Reading file from http://www.cisco.com/security/pki/trs/ios.p7b
Loading http://www.cisco.com/security/pki/trs/ios.p7b !!!
% PEM files import succeeded.
%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS: Trustpool Download is successful
```

Add the WLC to Cisco DNA Spaces:

Step 1: Navigate to https://dnaspaces.io/ to login to the Cisco DNA Spaces dashboard, using your Cisco DNA Spaces account credentials and navigate to **Setup-> Wireless Networks-> + Add New**.

Figure 267 Adding Wireless Network to DNA Spaces



Step 2. Select **Cisco AireOS/Catalyst**.

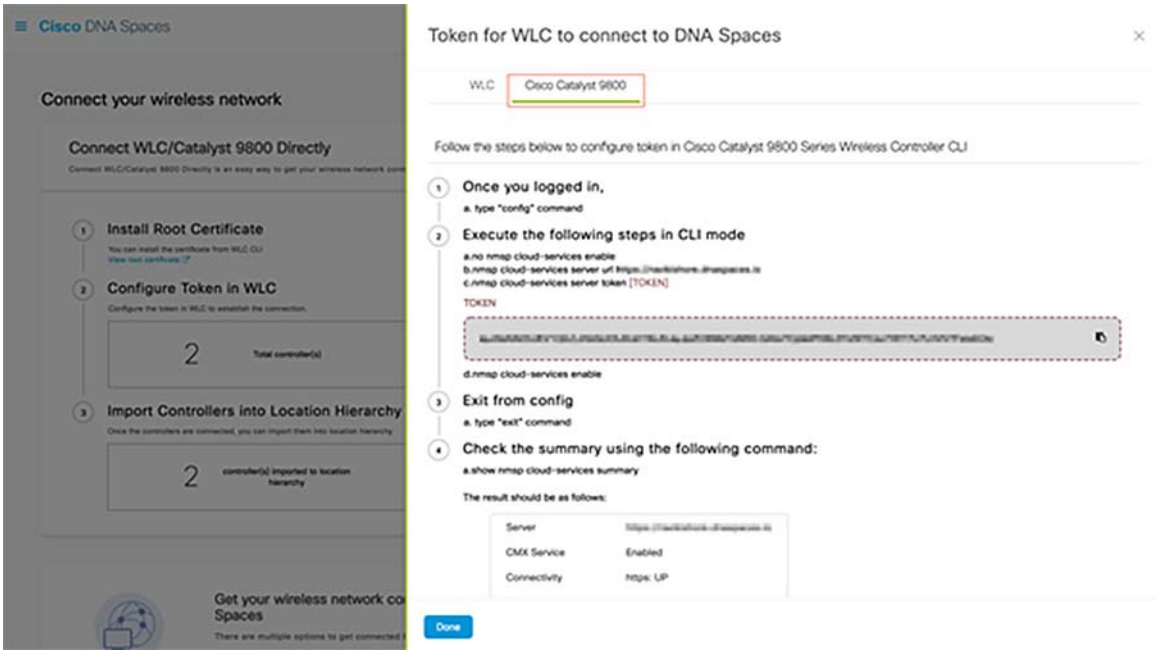
Step 3. Select **Connect WLC directly**.

Step 4. Click on **Customize Setup**.

Step 5. Click on **View Token-> Cisco Catalyst 9800** to get the cloud-services URL and cloud-services server ID Token for the controller.

Step 6. Log in to the controller CLI and run the commands mentioned in tab **View Token-> Cisco Catalyst 9800.**

Figure 268 DNA Spaces Token Id Configuration for WLC




```
WLC(config)#no nmsp cloud-services enable
WLC(config)#nmsp cloud-services server url https://<URL>
WLC(config)#nmsp cloud-services server token <TOKEN>
WLC(config)#nmsp cloud-services enable
```

Note: If the 9800 controller is behind a proxy, configure the proxy information with the nmsp cloud-services http-proxy <proxy ip_addr> <proxy port> command before you enable the NMSP cloud services.

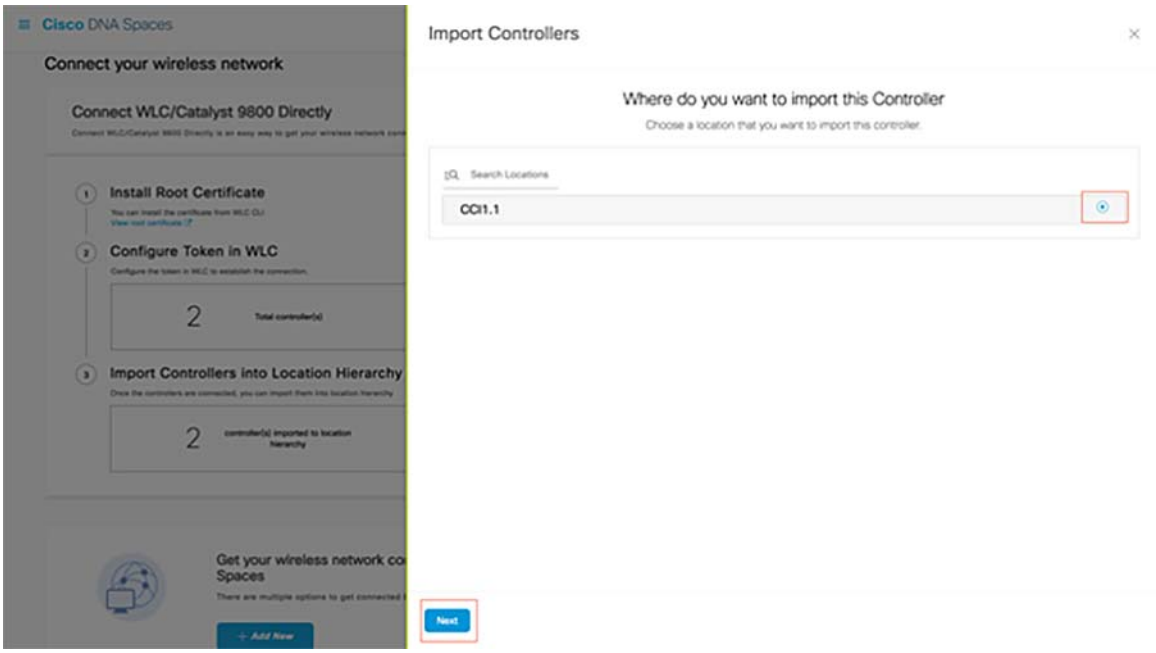
Note: NMSP traffic always uses the Wireless Management interface for communicating with DNA Spaces or CMX. This cannot be changed in the 9800 controller configuration. The interface number would be irrelevant, whichever interface is assigned as a Wireless Management Interface on the 9800 controller will be used.

Import the 9800 Controller to Cisco DNA Spaces:

Step 1. Navigate to **Setup -> Wireless Networks** and click **Import Controllers**.

Step 2. Choose the location where you want to import controllers and click **Next**. If this is the first time you import a controller, you may see the default location, i.e., your Cisco DNA Spaces account Name.

Figure 269 Controller Import on DNA Spaces



Step 3. Check the IP address of the controller you want to add. Then click Next.
Note: For the 9800 controller to be listed on the list, at least one AP needs to be associated with the controller.

Step 4. Select the locations and click Finish.
To confirm the connectivity status between the WLC and Cisco DNA spaces, run the show nmsp cloud-services summary command. The result should be as follows:

```
WLC#show nmsp cloud-services summary
CMX Cloud-Services Status
-------------------------
  Server                  : https://<url>
 CMX Service             : Enabled
  Connectivity            : https: UP
  Service Status          : Active
  Last IP Address         : 52.20.144.155
  Last Request Status     : HTTP/1.1 200 OK
  Heartbeat Status        : OK
```

Technical Reference: https://dnaspaces.cisco.com/why-cisco-dna-spaces/

Cisco DNA Spaces for Wi-Fi Analytics

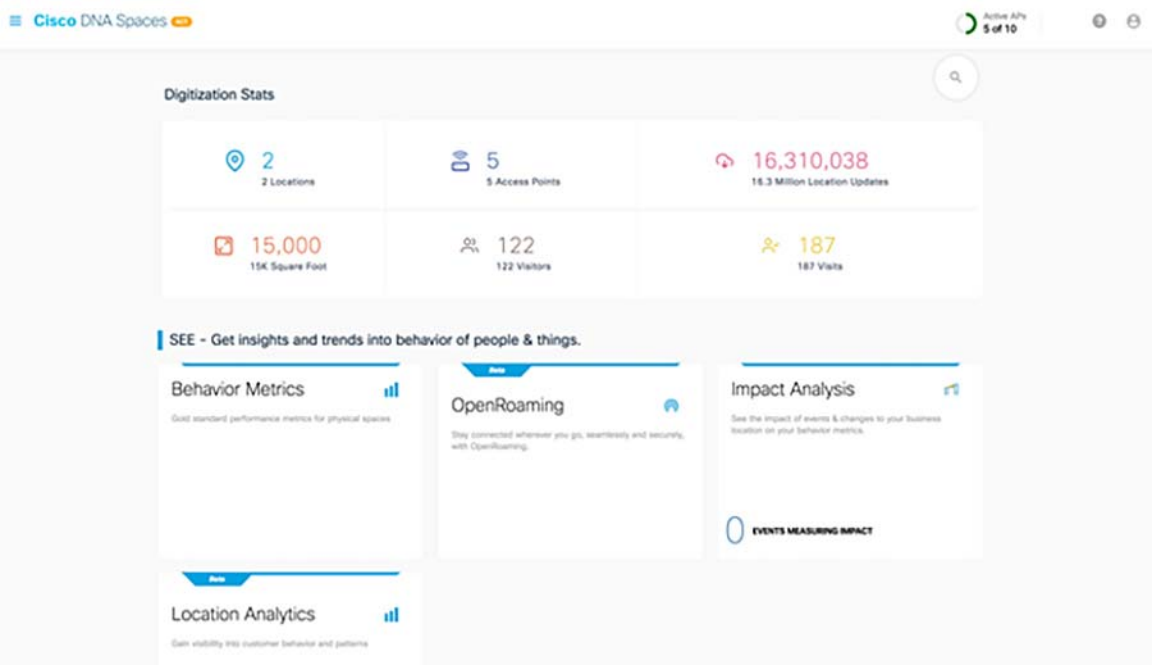
Cisco DNA Spaces aims at digitizing physical spaces, unlocking the physical spaces blind spot. It is the powerful location platform that leverages existing Wi-Fi infrastructure to give you actionable insights and drive business outcomes. It provides customized in-premise mobile guest experiences and seamless Wi-Fi onboarding to users, across locations.

Cisco DNA Spaces enables secure integration of CCI wireless (Wi-Fi) infrastructure across locations with centralized Cisco DNA Spaces platform that seamlessly integrates with our on-premise systems.

For more details about DNA Spaces and user cases, refer to the URL https://dnaspaces.cisco.com/

The Cisco DNA Spaces dashboard offers a single pane of glass for all location-based services. It also provides different views based on types of users and their permissions—such as for executives, property managers, and others.

Figure 270 Cisco DNA Spaces Dashboard



Wi-Fi Analytics Use Case on DNA Spaces

Cisco DNA Spaces takes the wireless network beyond connectivity to drive digitization in three easy steps: See, act, and extend. Now we can see what's happening at our properties, act on this knowledge through digitization toolkits, and extend platform capabilities by leveraging a partner app ecosystem.

Few of the features are covered in this section, for DNA Spaces Configuration guidance refer to the following URL:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide.html

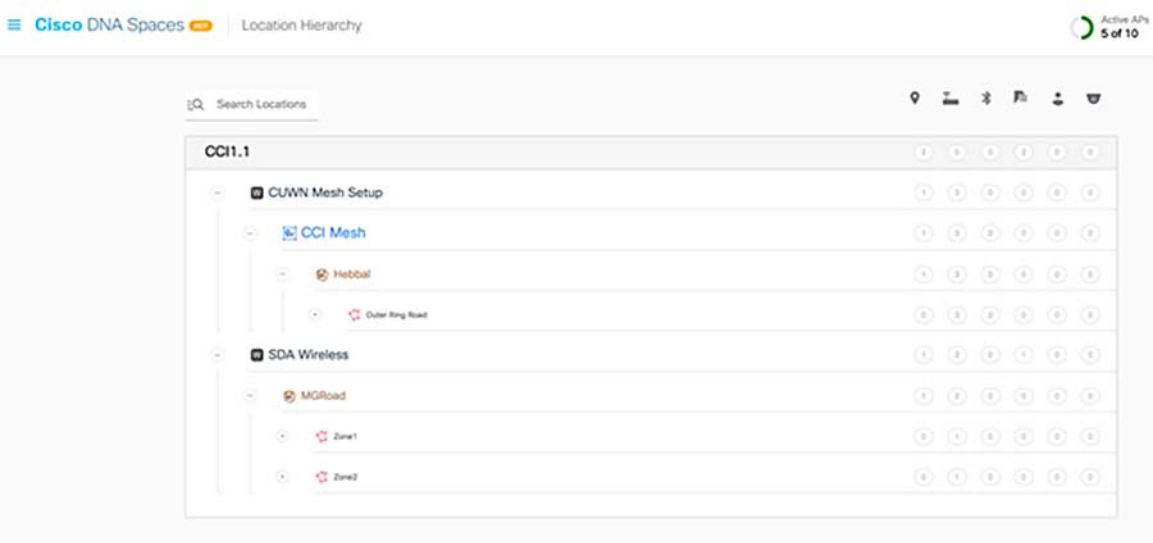
Location Hierarchy

The location-hierarchy capability enables us to manage and group locations based on business taxonomy. What we're doing is translating the IT backbone we already have (our wireless access points) into business context and nomenclature to create a centralized management view across all locations. We can group locations by geography, state, brand, type of store, zone, and more. Grouping enables us to create proximity rules specific to a set of locations.

Configuration Steps:

1. Click the three-line menu icon at the top-left of the Cisco DNA Spaces dashboard.
2. Choose **Location Hierarchy**.
3. In the **Location Hierarchy** window, click **More Actions** at the far right side of each Wireless Network create Groups and Zones in a Hierarchal manner.

Figure 271 Cisco DNA Spaces Location Hierarchy



For details about Location Hierarchy, refer to:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_hierarchy-location.html

Location Analytics

The Location Analytics app enables us to view reports of visits in our locations. The report gets displayed for the filters applied. We can apply the filters only if we are an ACT license user. The SEE license users cannot use the SSID filter. However, they can use the date range filter, and filter the locations except the network, floor and zone locations. In the below screenshots we are displaying the Visitor, Visits Dwell Time and Dwell Time breakout.

To view an Impact Analysis report, In the Cisco DNA Spaces dashboard, choose **Location Analytics**.

Figure 272 Cisco DNA Spaces Location Analytics 1

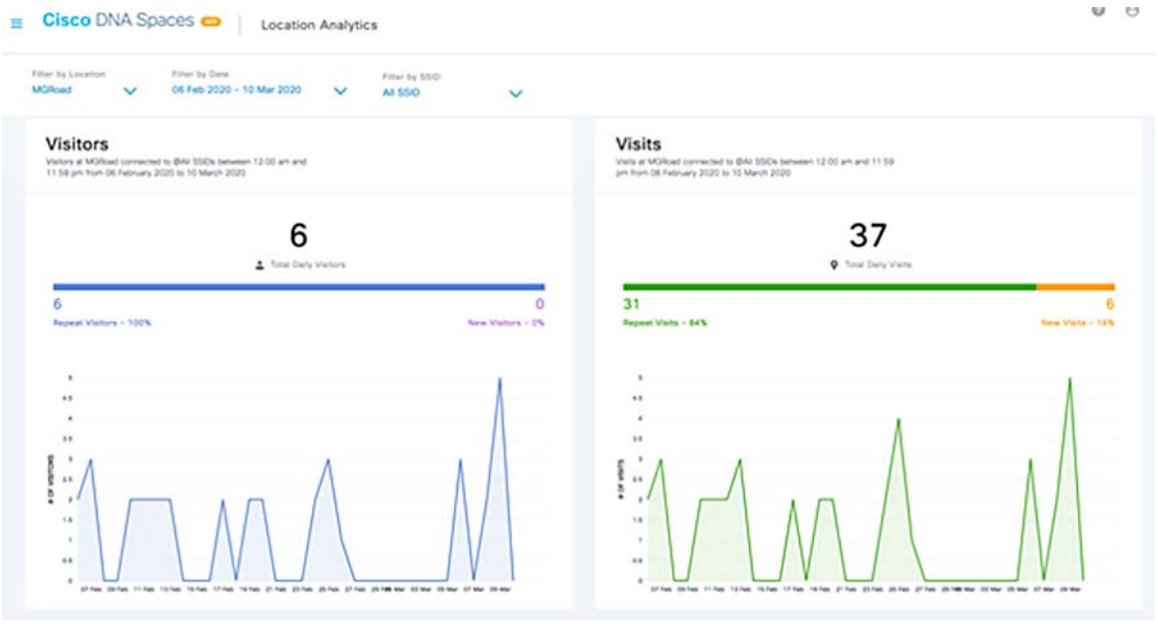
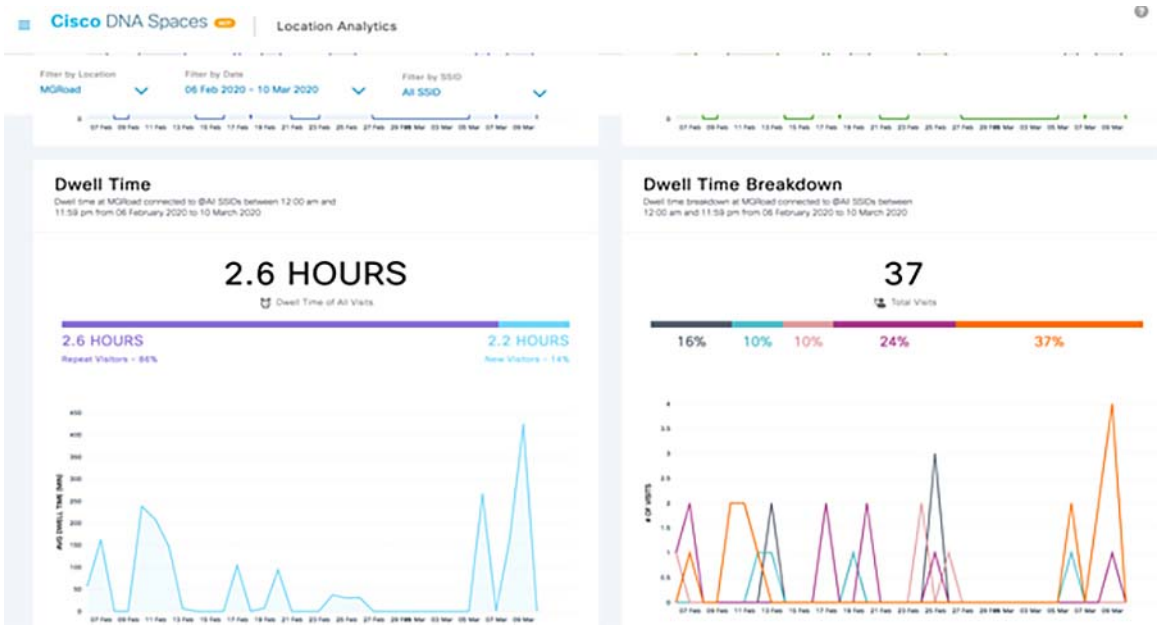


Figure 273 DNA Spaces Location Analytics 2



For more details about Location Analytics Report, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_location-analytics.html

DNA Spaces Captive Portal with 9800 Controller

A Captive portal is the user interface that appears when a Wi-Fi user connects to an SSID. We can create the captive portals using Cisco DNA Spaces, and enhance the portals using the various portal modules provided by Cisco DNA Spaces.

Cisco DNA Spaces also allows us to have your own portals (Enterprise Captive Portals) to onboard end users who connect to Wi-Fi. For more information on Enterprise Captive Portals, see Enterprise Captive Portal at:

- https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/enterprise-captive-portal/b-enterprise-captive-portal.html

This section describes how to configure captive portals using Cisco DNA Spaces with a 9800 controller.

To enable Captive Portal, the controller needs to be connected to DNA Spaces using the WLC Direct Connect.

Configuration on DNA Spaces Dashboard:

Captive Portal Configuration

- SSID Creation (WLAN)
- Portals Creation
- Captive Portal Rules Creation

Configuration on C9800 WLC (Without and With DNA Spaces Radius Server)

- Web-auth Certificate Installation & Configure global Parameter map
- ACL and URL Filter configuration on the 9800 controller:
- Parameter Map Creation
- WLAN (SSID) Creation

Configuration on Embedded Controller on C9800 Switch

- Web-auth Certificate Installation & Configure global Parameter map
- Guest WLAN creation from DNA Center and Provisioning
- Manual Configurations

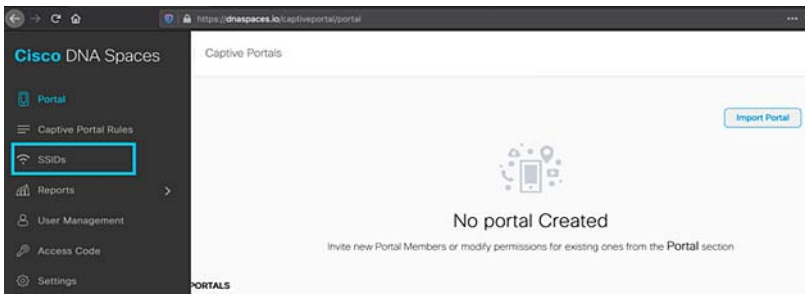
Configuration on DNA Spaces Dashboard:

Step1: Create the SSID on DNA Spaces

a. Click on **Captive Portals** in the dashboard of DNA Spaces:

b. Open the captive portal menu by clicking the three lines icon in the upper left corner of the page and click on **SSIDs:**

Figure 274 SSID Creation on DNA Spaces



c. Click on **Import/Configure SSID**, select **CUWN (CMX/WLC)** as the " Wireless Network" type, and enter the SSID name as shown in Figure 275.

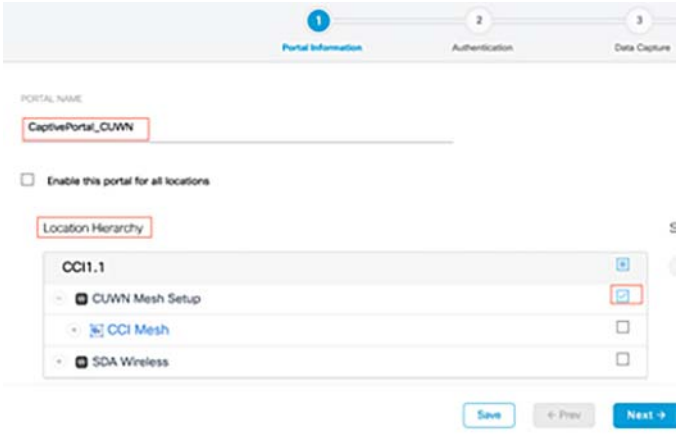
Figure 275 Configure SSID on DNA Spaces

Step 2: Create the portal on DNA Spaces

a. Click on **Captive Portals** in the dashboard of DNA Spaces, Click on **Create New,** enter the portal name and select the locations that can use the portal:

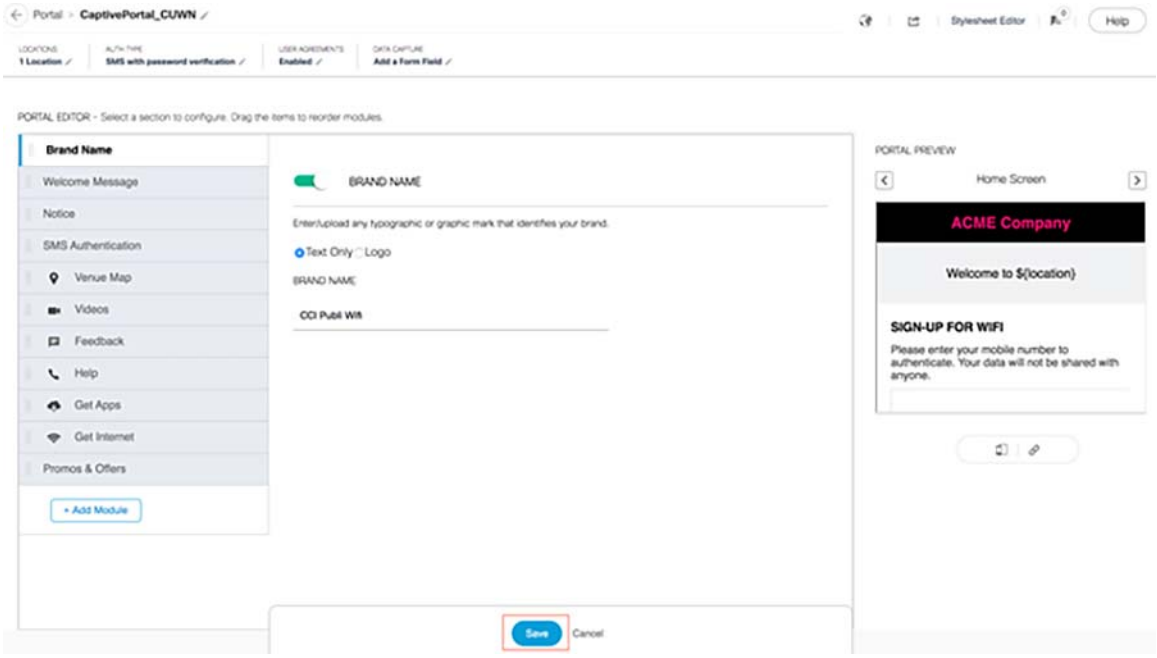
b. Select the authentication type, choose if we want to display data capture and user agreements on the portal home page and if users are allowed to Opt-in to receive a message. Click **Next**:

Figure 276 Captive Portal on DNA Spaces



c. Edit the portal as needed, Click on **Save.**

Figure 277 Captive Portal Editor on DNA Spaces

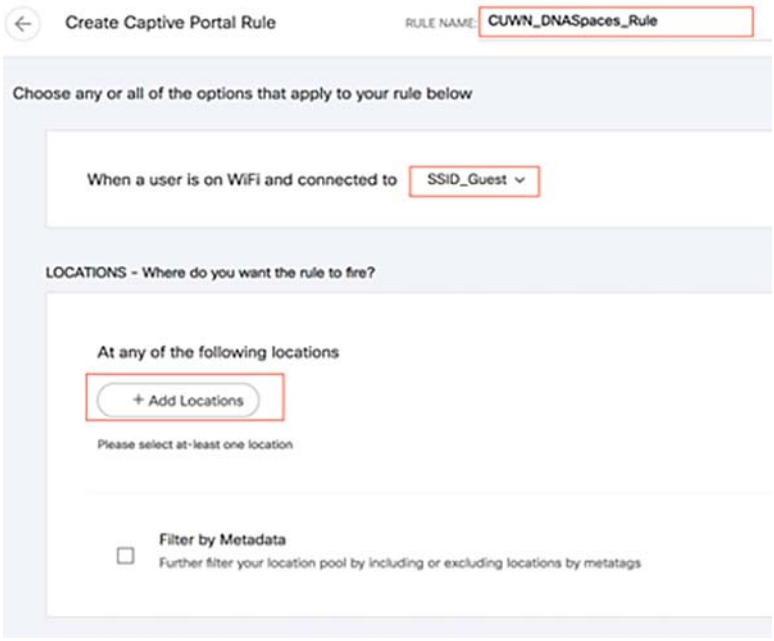


Step 3: Configure the Captive Portal Rules on DNA Spaces

a. Click on **Captive Portals** in the dashboard of DNA Spaces, Open the captive portal menu and click on **Captive Portal Rules:**

b. Click **+ Create New Rule**. Enter the rule name, choose the SSID previously configured.

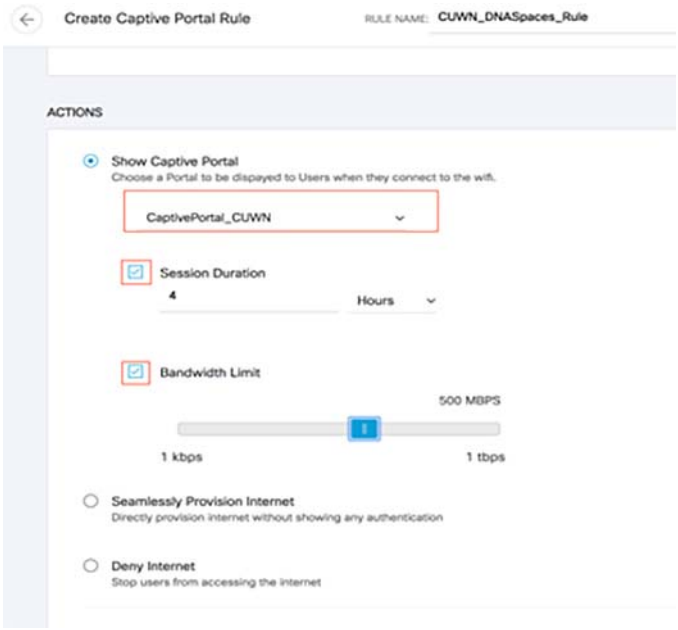
Figure 278 Captive Portal Rule on DNA Spaces



c. Select the locations in which the portal is available. Click **+ Add Locations** in the **LOCATIONS** section. Choose the desired one from the Location Hierarchy.

d. Choose the action of the captive portal. In this case, when the rule is hit, the portal is shown. Click **Save & Publish.**

Figure 279 Captive Portal Rule Actions Tab on DNA Spaces



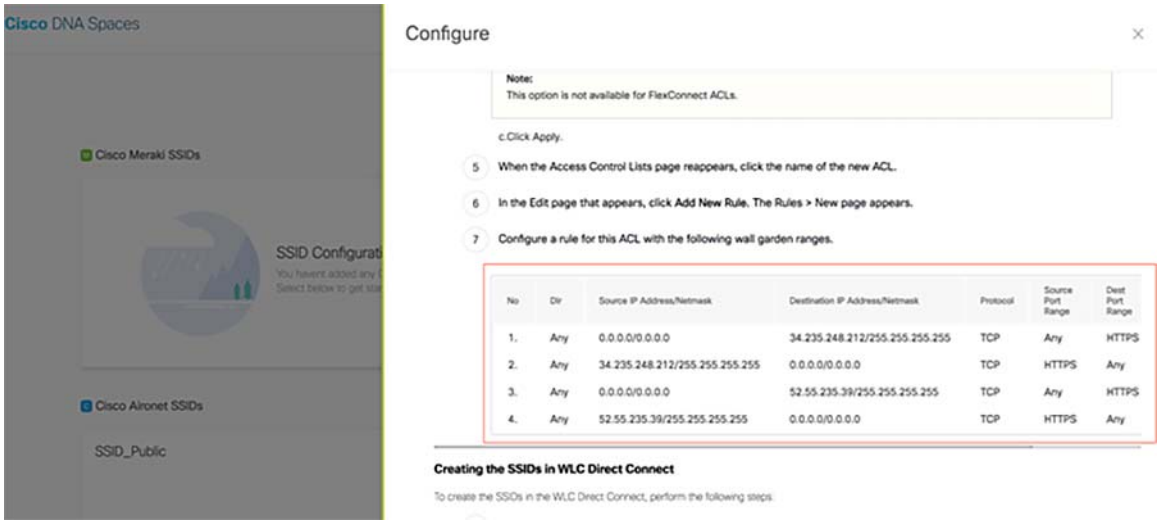
Refer to the following URL for Captive Portal Configurations:

- https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_captive-portals.html

Capture the DNA Spaces IP address, splash portal url , Captive Portal Radius server and shared key details:

Click on **Captive Portals** in the dashboard of DNA Spaces, Open the captive portal menu by clicking the three lines icon in the upper left corner of the page and click on **SSIDs** and click on **Configure Manually.**

Figure 280 DNA Spaces Configuration information



Configuring Cisco Catalyst 9800 Series Wireless Controller for Captive Portals:

Step 1: Web-auth Certificate Installation and Configure global Parameter map

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

Refer to the following URL to generate a Certificate Signing Request (CSR) in order to obtain a third-party certificate and how to download a chained certificate to a Catalyst 9800 Wireless LAN Controller (9800 WLC) and use for webauth and webadmin portal.

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html#anc0

  a. On C9800 WLC GUI, Navigate to **Configuration-> Security-> Web Auth,** Click the Parameter map name, global. On the General tab, from the Type drop-down list, choose webauth. Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field. Check the Web Auth intercept HTTPS check box.

CLI:

```
(config)#parameter-map type webauth global
(config-params-parameter-map)#type webauth
(config-params-parameter-map)#intercept-https-enable
(config-params-parameter-map)#virtual-ip ipv4 <Virtual IP> virtual-host <Virtual Host>
```

  b. Once we purchase the certificate, convert the certificate into pkcs12, the file format will be .p12 and Copy into the tftp server.

Download the certificate from the tftp server using the following steps:

In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

```
(config)#crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

a. To confirm the tftp server IP, enter **yes**.

b. Enter the certificate file name. For example, wildcard.wifi.com.p12. The certificate gets downloaded.

c. To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Web Auth > Certificate.The downloaded certificate appears as the last certificate in the list.

d. To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

```
(config)#parameter-map type webauth global
(config-params-parameter-map)#trustpoint <installed trustpool name>
(config-params-parameter-map)#end
#wr
```

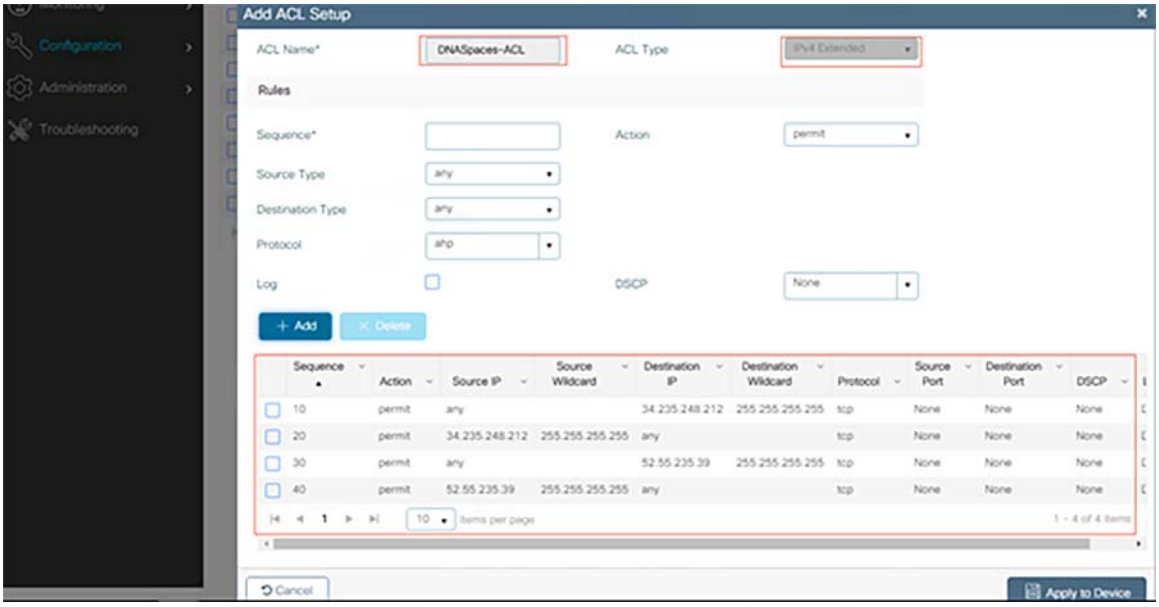
e. Reload Cisco Catalyst 9800 Series Wireless Controller.

Step 2: ACL and URL Filter configuration on the 9800 controller:

A pre-authentication ACL is required as this is a web authentication SSID, and as soon as the wireless device connects to the SSID and receives an IP address, the device's policy manager state moves to the Webauth_Reqd state and the ACL is applied to the client session to restrict the resources the device can reach.

a. Navigate to **Configuration-> Security-> ACL,** click **+Add** and configure the rules to allow communication between the clients and DNA Spaces as follows. Replace the IP addresses with the ones given by DNA Spaces for the account in use:

Figure 281 ACL Filter on C9800 WLC

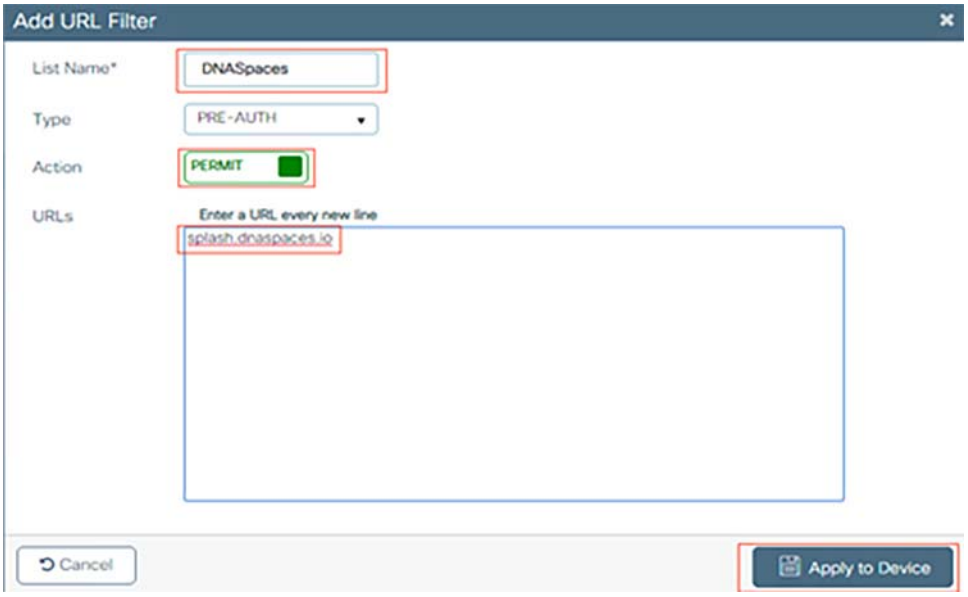


b. Confgure the URL filter to allow the DNA Spaces domain. Navigate to **Configuration-> Security-> URL Filters**, click **+Add** and configure the list name, select **PRE-AUTH** as the type, action as **PERMIT** and the URL **splash.dnaspaces.io**:

Add the following domains, if we want to enable social authentication:

- *.fbcdn.net
- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com
- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

Figure 282 URL Filter on C9800 WLC



Note: The SSID can be configured to use a RADIUS Server or without it. For Seamless Internet Provisioning, Extended session duration, Deny Internet the SSID needs to be configured with a RADIUS Server, otherwise, there is no need to use the RADIUS Server. All kinds of portals on DNA Spaces are supported on both configurations.

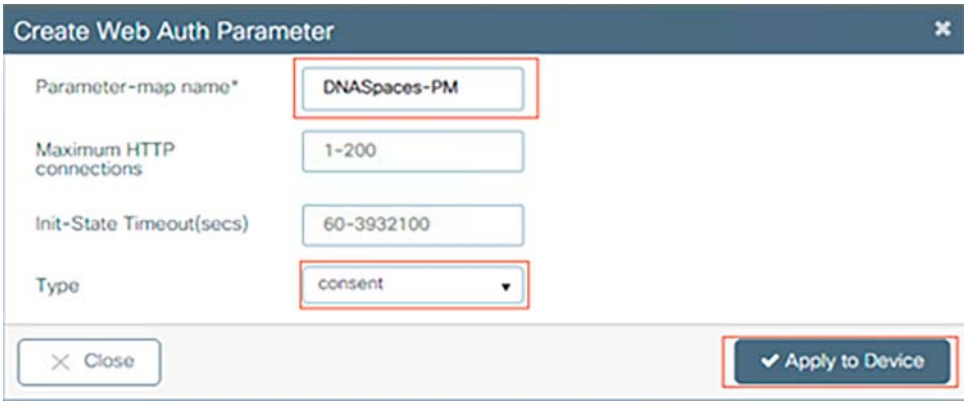
c. Navigate to **Configuration-> Tags & Profiles-> Flex** and click the profiles in use. In the Edit Flex Profile window that appears, click Policy ACL tab, Click Add. From the dropdown, select ACL and Pre-Auth URL Filter. (This step applies only for Flex Mode).

Captive Portal without RADIUS Server on DNA Spaces:

Step3a. Web Auth Parameter Map configuration on the 9800 controller

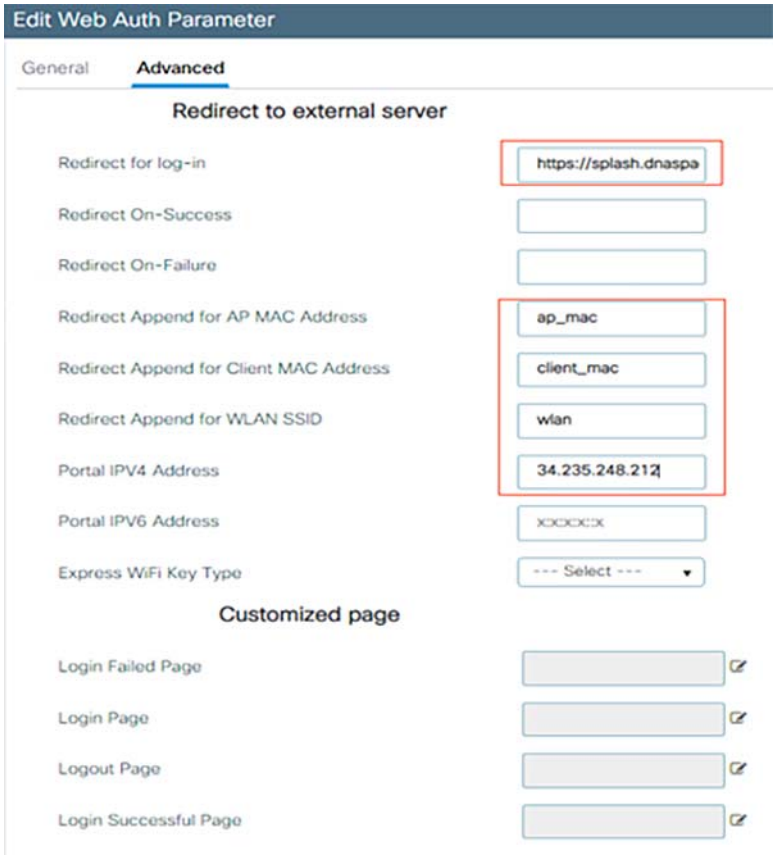
a. Navigate to **Configuration-> Security-> Web Auth**, Click **+Add** to create a new parameter map. In the window that pops-up configure the parameter map name, and select **Consent** as the type:

Figure 283 Parameter Map Creation on C9800 WLC



b. Click on the parameter map configured in the previous step, navigate to the **Advanced** tab, and enter the Redirect for log-in URL, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address as follows. Click **Update & Apply**.

Figure 284 Parameter Map Configuration on C9800 WLC



Note: Cisco DNA Spaces portal can resolve to two IP addresses, but the 9800 controller allows only one IP address to be configured, choose any of those IP addresses and configure it on the parameter map as the Portal IPv4 Address.

Step4a. Create the WLAN (SSID) on the 9800 controller

c. Navigate to **Configuration-> Tags & Profiles-> WLANs**, click **+Add.** Configure the Profile Name, SSID and enable the WLAN. Make sure the SSID name is the same name as the configured in step of section **Create the SSID on DNA Spaces.**

d. Navigate to **Security-> Layer2.** Set the Layer 2 Security Mode to **None,** make sure MAC Filtering is disabled.

e. Navigate to **Security-> Layer3.** Enable Web Policy, configure the web auth parameter map and add the Preauthentication ACL. Click **Apply to Device**

Configure Policy Profile on the 9800 controller:

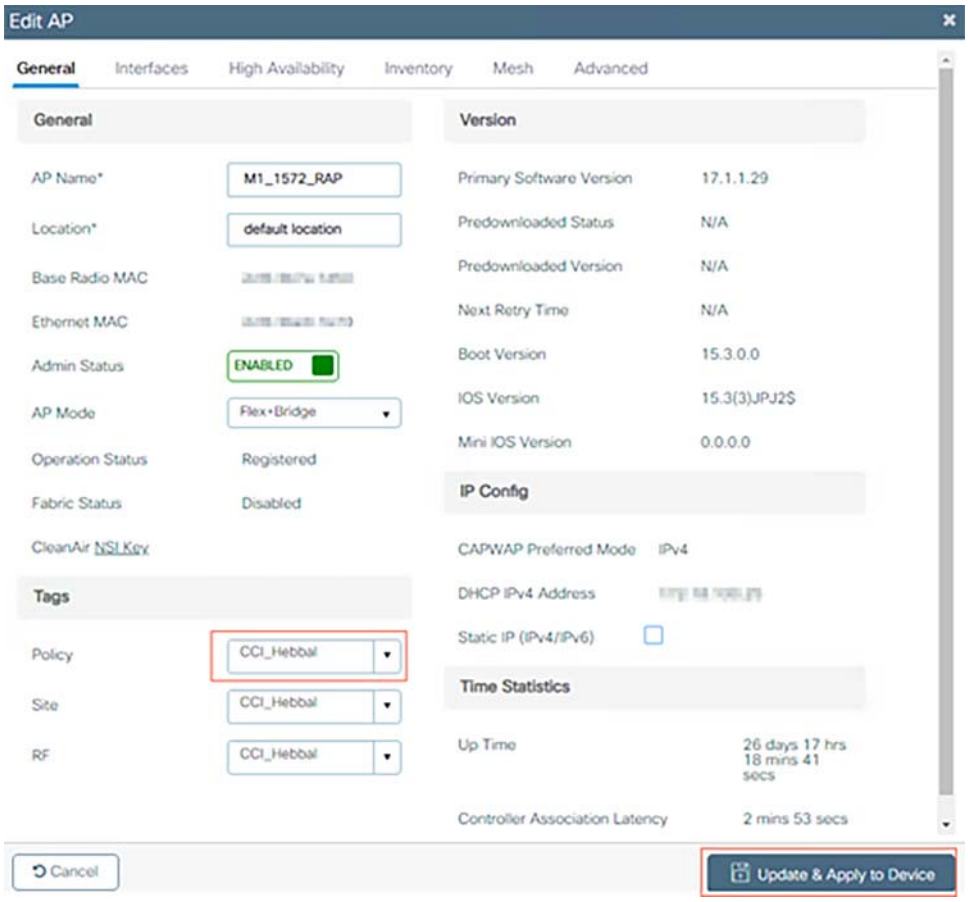
f. Navigate to **Configuration-> Tags & Profiles-> Policy** and create a new Policy Profile or use the default Policy Profile. In the access Policies tab, configure the client VLAN and add the URL filter.

Configure Policy Tag on the 9800 controller:

g. Navigate to **Configuration-> Tags & Profiles-> Tags.** Create a new Policy Tag or use the default policy tag. Map the WLAN to the Policy Profile in the Policy Tag.

h. Apply the Policy Tag to the AP to broadcast the SSID. Navigate to **Configuration-> Wireless-> Access Points,** Select the AP and add the Policy Tag. This will cause the AP to restart its CAPWAP tunnel and join back to the 9800 controller:

Figure 285 Applying Policy Tag to the AP



Captive Portal with RADIUS Server on DNA Spaces

It is recommended to use RADIUS authentication for captive portals. The following features work only if we configure RADIUS authentication.

- Seamless Internet provisioning
- Extended session duration.
- Deny Internet

RADIUS Servers Configuration on the 9800 Controller:

a. Configure the RADIUS servers. Cisco DNA Spaces acts as the RADIUS server for user authentication and it can respond on two IP addresses. Navigate to **Configuration-> Security-> AAA**, click on **+Add** and configure both RADIUS servers:

b. Configure the RADIUS Server Group and add both RADIUS servers. Navigate to **Configuration-> Security-> AAA-> Servers / Groups-> RADIUS-> Server Groups**, click **+add,** configure the Server Group name, MAC-Delimiter as **hyphen,** MAC-Filtering as **mac**, and assign the two RADIUS servers:

c. Configure an Authentication Method list. Navigate to **Configuration-> Security-> AAA-> AAA Method List-> Authentication,** click **+add.** Configure the Method List name, select **login** as the type and assign the Server Group:

d. Configure an Authorization Method list. Navigate to **Configuration-> Security-> AAA-> AAA Method List-> Authorization,** click **+add.** Configure the Method List name, select **network** as the type and assign the Server Group:

e. Configure an Accounting Method list. Navigate to **Configuration-> Security-> AAA-> AAA Method List-> Accounting,** click **+add.** Configure the Method List name, select **Identity** as the type and assign the Server Group.

The below steps covers only the extra configurations or modifications required for using DNA Spaces RADIUS Server.

Step3b: Configuration changes at Web Auth Parameter Map on the 9800 controller

a. Create a web auth parameter map. Navigate to **Configuration-> Security-> Web Auth**, Click **+Add**, and configure the parameter map name, and select **webauth** as the type:

Step4b: Configuration changes needed at WLAN (SSID) on the 9800 controller

a. Select the WLAN and Navigate to **Security-> Layer2.** Set the Layer 2 Security Mode to **None,** enable MAC Filtering and add the Authorization List:

b. Navigate to **Security-> Layer3.** Enable Web Policy, configure the web auth parameter map and the Authentication List. Enable On Mac Filter Failure and add the Preauthentication ACL. Click **Apply to Device**.

c. Navigate to **Configuration-> Tags & Profiles-> Policy,** In the Advanced tab, enable AAA Override and configure the accounting method list:

d. Apply the Policy Tag to the AP to broadcast the SSID. Navigate to **Configuration-> Wireless-> Access Points,** Select the AP in question and add the Policy Tag. This will cause the AP to restart its CAPWAP tunnel and join back to the 9800 controller:

Verification:

To confirm the status of a client connected to the SSID navigate to **Monitoring-> Clients**, click on the MAC address of the device and look for Policy Manager State:

Configuring Embedded Controller (C9800-sw) Running on C9300 for Captive Portals

In our CCI network, for SDA Wireless deployment mode eWLC (C9800-sw) runs as a software component in IOS-XE on the Catalyst 9000 switch. The management of the controller is handled from the DNA Center.

In addition to the configuration made from the DNA Center, few additional manual configurations are required.

Step1. Web-auth Certificate Installation & Configure global Parameter map

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

Refer to the below url to generate a Certificate Signing Request (CSR) in order to obtain a third-party certificate and how to download a chained certificate to a Catalyst 9800 Wireless LAN Controller (9800 WLC) and use for webauth and webadmin portal.

- https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html

Global parameter map Configuration:

```
(config)#parameter-map type webauth global
(config-params-parameter-map)#type webauth
(config-params-parameter-map)#intercept-https-enable
(config-params-parameter-map)#virtual-ip ipv4 <Virtual IP> virtual-host <Virtual Host>
```

a. Once we purchase the certificate, convert the certificate into pkcs12, the file format will be .p12 and Copy into the tftp server.

Download the certificate from the tftp server using the following steps:

1. In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

```
(config)#crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

To confirm the tftp server IP, enter **yes**.

Enter the certificate file name. For example, **wildcard.wifi.com**.p12. The certificate gets downloaded.

To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Web Auth > Certificate.The downloaded certificate appears as the last certificate in the list.

To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

```
(config)#parameter-map type webauth global
(config-params-parameter-map)#trustpoint <installed trustpool name>
(config-params-parameter-map)#end
#wr
```

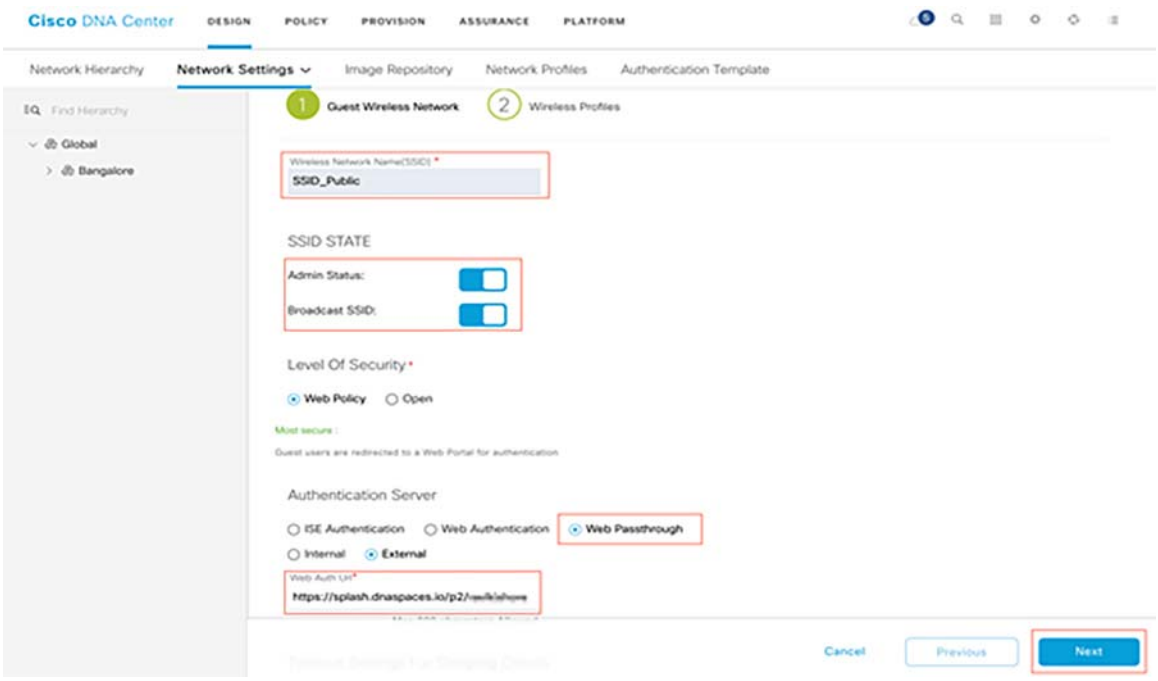
Reload Cisco Catalyst 9800 Series Wireless Controller.

Step2: WLAN (SSID) Creation from DNA Center

a. On the DNA Center GUI, Navigate to **Design-> Network Settings-> Wireless** , Under Global Hierarchy click on **Add for Guest Wireless**.

b. Configure the SSID name, Enable SSID State, Level of Security as 'Web Policy' ,Authentication Server as Web Passthrough and provide External DNASpaces splash portal url and keep the other fields as default and click **Next**.

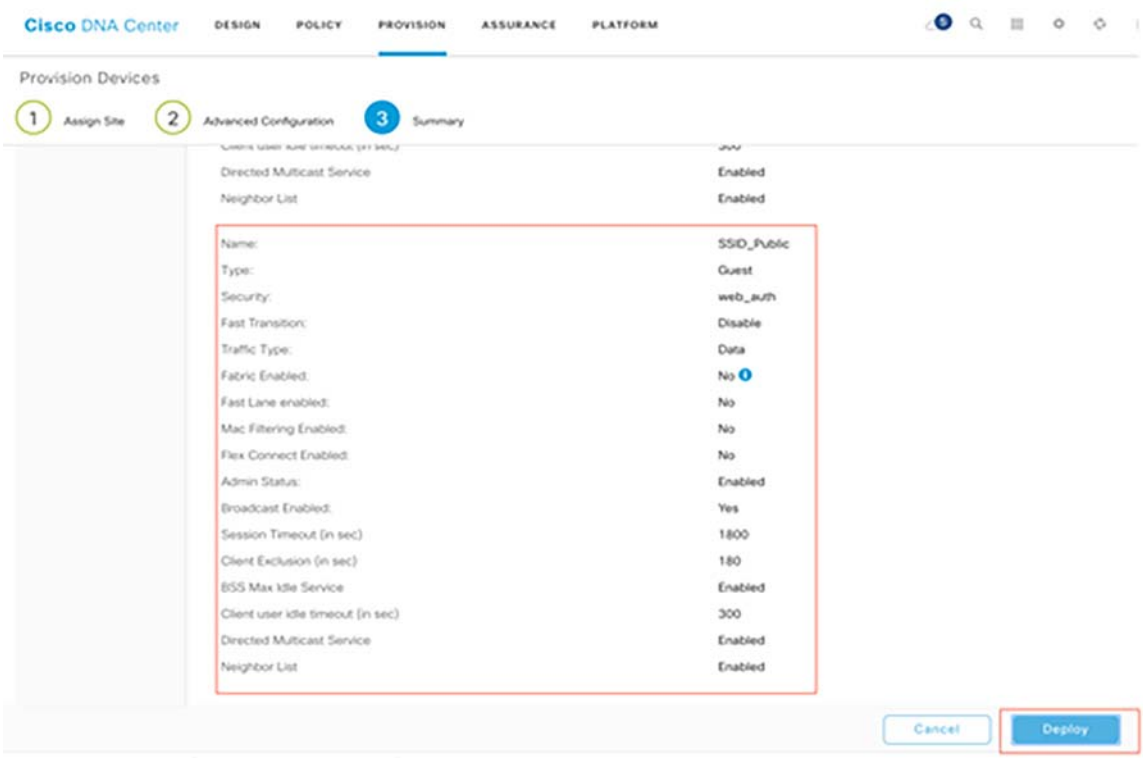
Figure 286 Guest SSID Creation on DNA Center



c. Click on **Add** and associate the Wireless Profile and then click **Finish**.

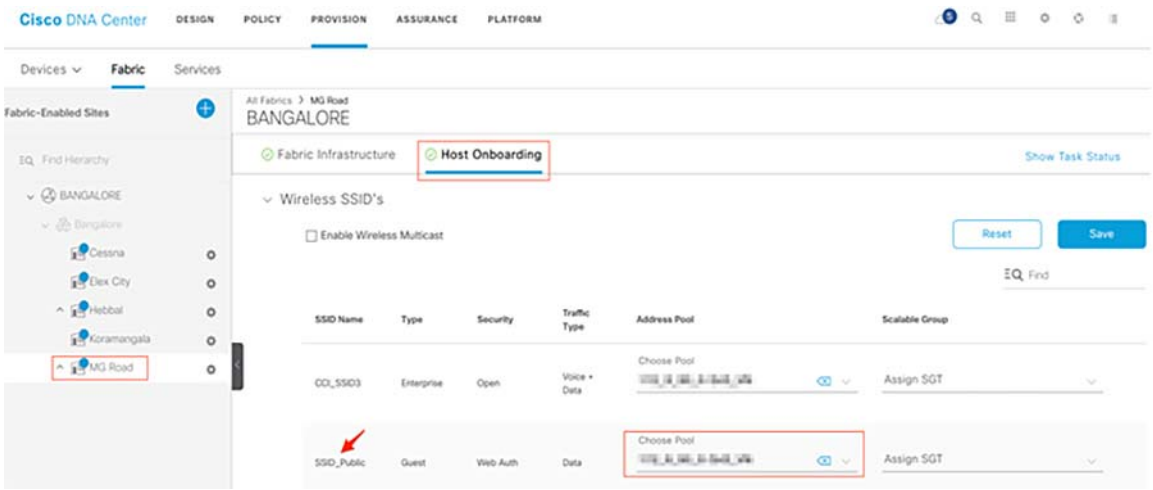
d. Navigate to **Provision -> Devices** and Provision the C9300 switch on which we are running the embedded controller. Make sure our newly created SSID is available in the Summary and click on **Deploy**.

Figure 287 Provisioning eWLC with Guest SSID



e. Navigate to **Provision -> Fabric**, from the Hierarchy select the target Site and click on **Host Onboarding** under Wireless SSIDs and assign an IP address IP pool for the SSID. Click on **Save** and then **Apply** as shown in Figure 288.

Figure 288 Host Onboarding of SSID



Verification:

```
C9300-R-Stack#sh run | inc SSID_Public
wlan SSID_Publi_Global_F_065f81ce 20 SSID_Public

C9300-R-Stack#sh run | sec SSID_Publi_Global_F_065f81ce
```

```
parameter-map type webauth SSID_Publi_Global_F_065f81ce
 type consent
 sleeping-client
 redirect for-login https://splash.dnaspaces.io/p2/<id>
 redirect portal ipv4 52.55.235.39
wireless profile fabric SSID_Publi_Global_F_065f81ce
 client-l2-vnid 8193
 description SSID_Publi_Global_F_065f81ce
wireless profile policy SSID_Publi_Global_F_065f81ce
 aaa-override
 no central dhcp
 no central switching
 description SSID_Publi_Global_F_065f81ce
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric SSID_Publi_Global_F_065f81ce
 http-tlv-caching
 service-policy input silver-up
 service-policy output silver
 no shutdown
 wlan SSID_Publi_Global_F_065f81ce policy SSID_Publi_Global_F_065f81ce
wlan SSID_Publi_Global_F_065f81ce 20 SSID_Public
 ip access-group web EXT_REDIRECT_ACL_52.55.235.39
 no security ft adaptive
 no security wpa
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list dnac-cts-list
 security web-auth parameter-map SSID_Publi_Global_F_065f81ce
 no shutdown
```

a. Configure Redirect Append for AP MAC, Client MAC and WLAN SSID on C9300 switch:

```
C9300-R-Stack(config)#parameter-map type webauth SSID_Publi_Global_F_065f81ce
C9300-R-Stack(config-params-parameter-map)#redirect append ap-mac tag ap_mac
C9300-R-Stack(config-params-parameter-map)#redirect append wlan-ssid tag wlan
C9300-R-Stack(config-params-parameter-map) #redirect append client-mac tag client_mac
```

b. Configure url filter and add to the Policy Profile:

Add the following domains, if we want to enable social authentication:

- *.fbcdn.net
- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com

- ssl.gstatic.com
- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

```
C9300-R-Stack(config)#urlfilter list DNASpaces
C9300-R-Stack(config-urlfilter-params)#action permit
C9300-R-Stack(config-urlfilter-params)#url splash.dnaspaces.io

C9300-R-Stack(config)#wireless profile policy SSID_Publi_Global_F_065f81ce
C9300-R-Stack(config-wireless-policy)#shutdown
C9300-R-Stack(config-wireless-policy)#urlfilter list pre-auth-filter DNASpaces
C9300-R-Stack(config-wireless-policy)#no shutdown
```

Implementing Network Security

Implementing network segments, securing CCI network from external threats, and providing secure communications to network devices and endpoints connecting to CCI network are the key building blocks of the CCI Solution network security design. For more details on CCI solution security design, refer to the *Cisco Connected Communities Infrastructure Solution Design Guide*, which can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html

This chapter includes the following major topics:

Configuring Macro-Segmentation—VN Provisioning

Virtual Networks (VN) provide the isolation of networks by segmenting the overall network into multiple logically separate networks as needed. When configuring a VN for a service in a PoP (fabric) site, a Virtual Routing and Forwarding (VRF) table is automatically created on the border node. This is same as macro-segmentation. This VRF is separate from another VRF and traffic can only pass between them if explicitly configured on the fusion router. Each service will have a separate VN, but the steps to create one are largely the same.

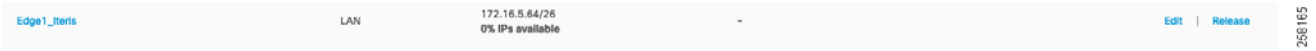
1. A global IP address pool needs to be allocated for the service and this can be configured manually from Cisco DNA Center or automatically from an IP address management platform.

Figure 289 Example of a Global IP Pool

2. A portion of that global pool also needs to be reserved in the fabric site.

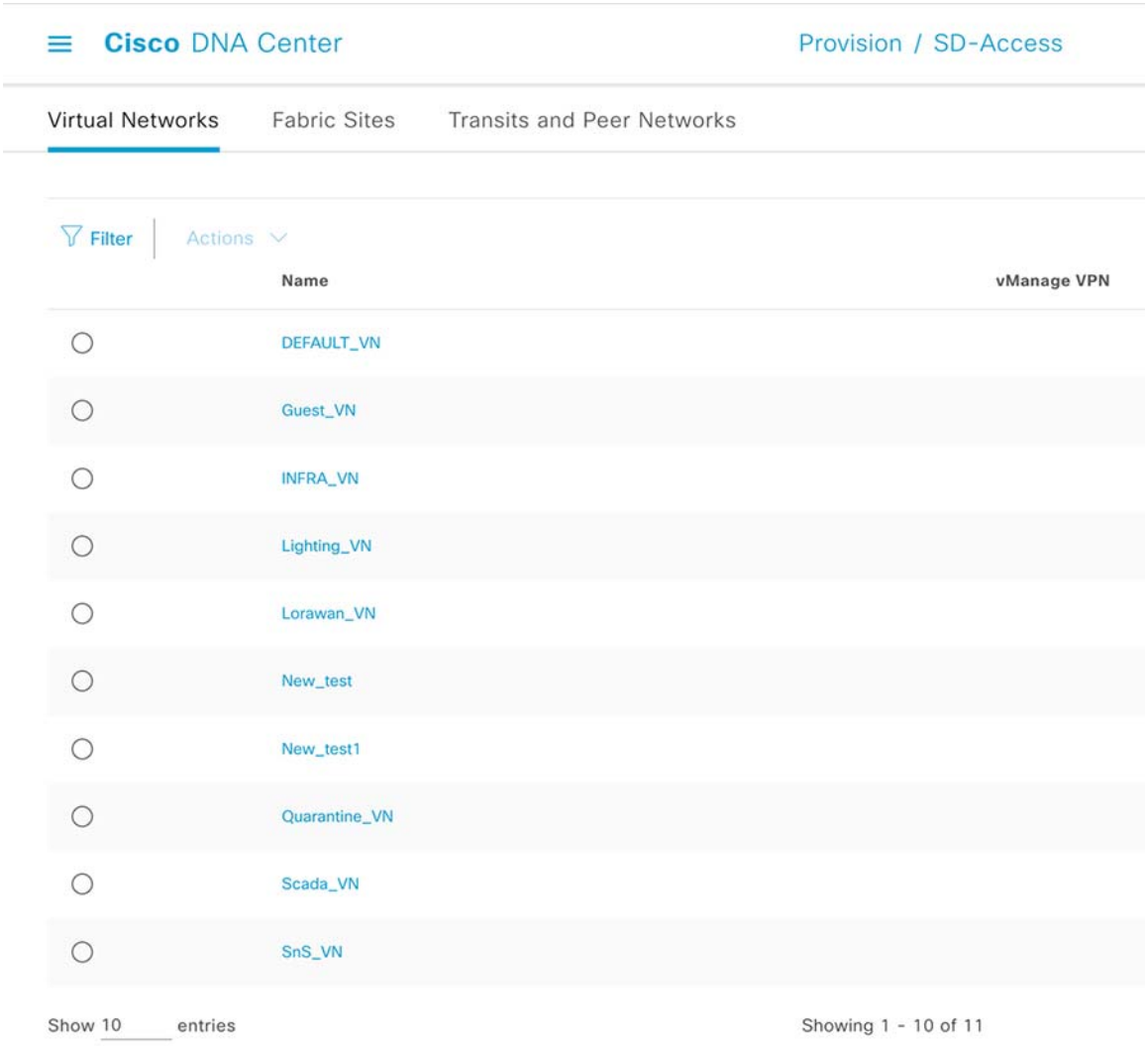
Figure 290 Fabric Data Center IP Pool

Figure 291 Fabric Edge IP Pool



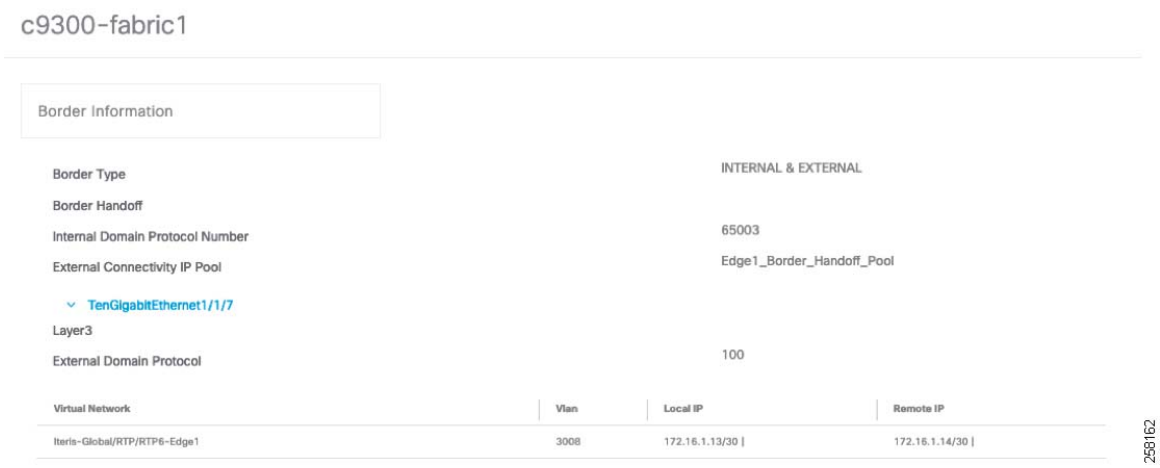
3. The virtual network is created under the **Policy** section and scalable groups can be added if desired.

Figure 292 Virtual Network



4. Next, the VN must be configured on the PoP (fabric) site under **Provision-> SD Access-> <Fabric site>-> Host Onboarding**. When adding the VN to the border node, Cisco DNA Center will automatically push the appropriate configuration to the device(s) that is performing the border function; in the case of a CCI PoP, this is a FiaB. This configuration is found in the MPLS backhaul network section. An example from the Cisco DNA Center Border node information is seen below in Figure 293:

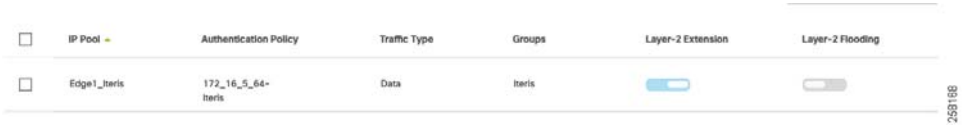
Figure 293 Border Node External Information



5. The VLAN is automatically chosen by Cisco DNA Center and the IP address is chosen from the **External Connectivity IP Pool**.

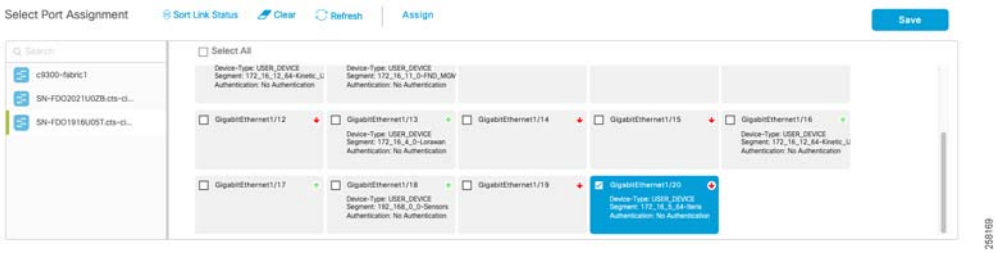
6. The VN is configured for the fabric edge through the **Host Onboarding** section. The VN is selected and then IP pools must be added to it.

Figure 294 Host Onboarding for Virtual Network



7. Once configured, a VLAN will be created for this VN for use by the hosts. If the host will be connected to an extended node, or the fabric edge node, it can be configured in the **Select Port Assignment** section.

Figure 295 Port Assignment for Virtual Network



8. For any hosts connected to non-extended nodes in the PoP (fabric) site, the VLAN will have to be manually added to the non-extended node. The VLANs are configured dynamically so that the fabric border will have to be examined for the correct value.

```
c9300-fabric1#sh ip vrf Iteris
  Name                             Default RD          Interfaces
  Iteris                           1:4100              Vl1022
                                                       Vl3008
                                                       Vl3016
                                                       LI0.4100
```

9. From the command shown above and the fabric border configuration in the Cisco DNA Center web interface, the border is using VLAN 3008 and 3016 to communicate with the IP transit node. This means that VLAN 1022 is used for the Iteris VN. Looking at the VLAN interface configuration will confirm this:

```
c9300-fabric1#show run interface vlan 1022
Building configuration...
Current configuration: 313 bytes
!
interface Vlan1022
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45d
 vrf forwarding Iteris
 ip address 172.16.5.65 255.255.255.192
 ip helper-address 100.0.0.100
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 172_16_5_64-Iteris-IPV4
end
```

10. Since the edge fabric site implementation presumes a REP ring of non-extended nodes, the VLAN must be allowed on every REP trunk port to ensure connectivity around the ring. Every port that is part of this VN must also be configured with the correct access VLAN.

11. After the edge ports are configured and the border configs are in place between all the fabric sites, a host in the VN should have connectivity to any other host in the VN.

Repeat this process for the other VNs to enable all necessary services.

Network Devices and Endpoints Security Implementation

This section covers the implementation of secure network connectivity for the network devices and endpoints (Hosts) in the CCI network. Network devices and endpoints/host AAA leveraging Cisco ISE are discussed.

Network Devices Security Implementation

A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted (for example, switches, routers, and so on). The network device definition enables the Cisco Identity Services Engine (Cisco ISE) to interact with the network devices that are configured. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

Network devices are authenticated by Cisco ISE server automatically when we integrate the Cisco ISE with Cisco DNA Center. Following are the steps to ensure successful network devices authentication using Cisco ISE as AAA server in the CCI network:

Note: Cisco ISE uses the shared secret password to authenticate the device, the SSH user, and shared secret is configured when integrating the Cisco ISE with Cisco DNA Center.

Endpoints Security Using 802.1X and MAC Authentication Bypass

Secure connectivity for the wired endpoints or hosts connecting to CCI network can be implemented using 802.1X authentication mechanism for the endpoints supporting 802.1X protocols. For the endpoints that do not support 802.1X protocol, MAC Authentication Bypass (MAB) can be implemented to authenticate and authorize the endpoints or hosts connecting to CCI network.

Cisco DNA Center SD-Access supports closed authentication for the endpoints/hosts connecting to FiaB Edge. However, the extended nodes or non-extended nodes in the Ethernet access ring are not provisioned for " Closed Authentication" using Cisco DNA Center. Therefore, secure onboarding of a host connecting to extended and non-extended nodes must be done manually, or configuration should be automated using Cisco DNA Center configuration templates.

Note: It is recommended to use secure onboarding of wired endpoints connecting to CCI network using 802.1X or MAB methods, as discussed in this section, for the endpoints' authorization and security of the network.

An example implementation of 802.1X and MAB validated in this CVD for the wired clients (example: IP Camera) is covered in this section. Complete the following steps to successfully implement 802.1X or MAB for wired endpoints connecting to the Ethernet access ring.

Note: Make sure all the IE switches in the access ring are provisioned in the PoP (fabric) site by the Cisco DNA Center, which configures the IE switches for AAA authentication and RADIUS authorization CLI commands. It is required for successful implementation of 802.1X and MAB

1. Create Authentication and Authorization Policies in Cisco ISE

   In this implementation, a wired endpoint/client is authenticated and authorized by Cisco ISE using the wired dot1x or wired MAB authorization policy. By default, 802.1X and MAB authentication polices are available in Cisco ISE as part of Cisco ISE installation. It is recommended to leverage default authentication policies in ISE for the wired client's authentication.

   Following are the steps to create an authorization policy in Cisco ISE:

   a. Log in to Cisco ISE, navigate to **Administration-> Identities Management-> Identities**.

   b. Create a user profile for the wired client (example: **Cisco IP Camera user**).

   c. Click **Groups** in the **Identities Management** tab, create a user group, and associate the username created in **Identities** to the group.

   d. Navigate to **Policy-> Policy elements-> Authorization-> Authorization profile**.

   e. Create an Authorization profile for wired clients, select the access type as **Accept**, and authorize the profile based on VLAN.

   f. Optionally, you should assign a Scalable Group Tag (SGT) for the authorized client in the network in the authorization profile.

   g. From **Policy-> Policy Sets-> Authorization Policy**, create an Authorization policy for dot1x and MAB.

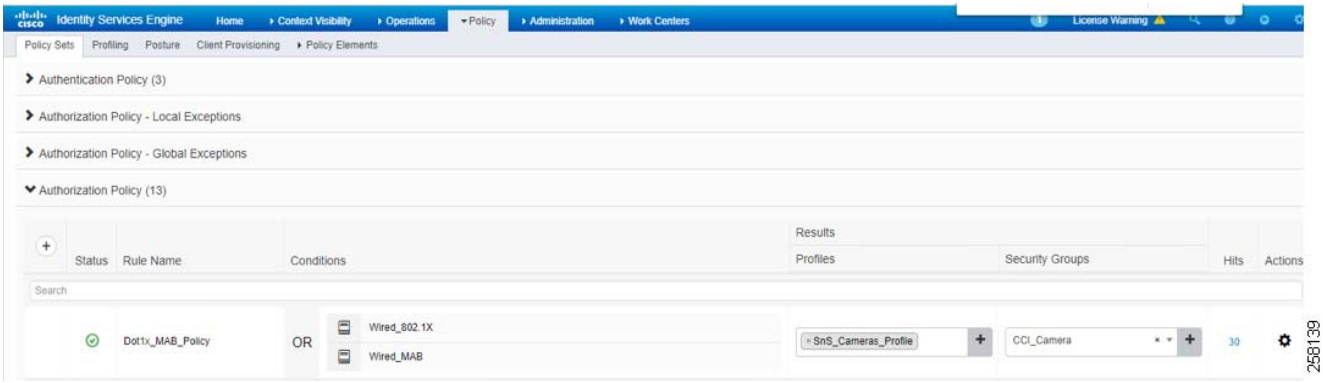
   h. Associate the **Authorization profile** to the **Authorization Policy** and click **Save**.

   For detailed step-by-step instructions for creating Authorization Policies in Cisco ISE, refer to the chapter " Configure and Manager Policies" in the *Cisco Identity Services Engine Administrator Guide, Release 2*.4.

   Note: Endpoint data traffic VLAN ID provisioned by Cisco DNA Center on Extended Nodes (EN) in the PoP site ring is used in the ISE authorization policy result set for that endpoint's access to CCI network. Therefore, check the VLAN ID for that PoP site's VN subnet (endpoint's data traffic subnet) from the Cisco DNA Center GUI Fabric Border configuration.

   Figure 296 shows an example 802.1X or MAB authorization policy created for wired clients (example: **Cisco IP Camera**) in the CCI network:

Figure 296 Cisco ISE Dot1x or MAB Authorization Policy View



2. Configure and apply dot1x or MAB Policies in Extended and Non-Extended Nodes

   Once Cisco ISE authentication and authorization policies are created, the IE switches (extended and non-extended nodes) in the ring must be configured for 802.1X or MAB access policies and apply the policy on each switch port where the wired endpoint/client would be connected.

   Identity control policies are configured on IE switches to define policy actions that use Identity-Based Networking services in response to specified conditions and subscriber events.

   For more details on Identity-Based Networking Services and control policies, refer to the chapters "Identity-Based Networking Services Overview" and "Configuring Identity Control Policies" in the *Identity-Based Networking Services Configuration Guide*, which can be found at the following URL:

   – https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-e/ibns-15-e-book/ibns-cntrl-pol.html

   An example 802.1X or MAB access policy configuration on IE switches used in this implementation is given below:

   a. Create the Class maps control type to match the result criteria. For example, the following 802.1X class-maps are configured as global configuration on IE switches in the ring to match the 802.1X result action:

```
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
```

   b. Create the policy maps control type to match the event and resultant action criteria. Class maps are associated for each policy map to trigger the action based on class map match criteria. For example, following 802.1X or MAB policy-maps are configured as global configuration on IE switches in the ring to trigger the 802.1X or MAB event priority and failure action:

```
policy-map type control subscriber Dot1xOrMAB
event session-started match-all
 10 class always do-until-failure
  10 authenticate using dot1x priority 10
event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  30 authentication-restart 60
 10 class DOT1X_NO_RESP do-until-failure
```

```
    10 terminate dot1x
    20 authenticate using mab priority 20
    40 class always do-until-failure
    10 terminate dot1x
    20 terminate mab
    30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
    10 terminate mab
    20 authenticate using dot1x priority 10
```

c. Apply the configured control policy on all IE switch ports or specific switchports where access control is required. The following example shows an access policy configured on an IE switchport for 802.1X or MAB authentication:

```
interface GigabitEthernet1/10
 switchport mode access
 ip device tracking maximum 10
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 mab
  dot1x pae authenticator
  service-policy type control subscriber Dot1xOrMAB
end
```

The above example policy-map for access policy configured on IE switches and associated to switchports triggers 802.1X authentication event for the wired endpoint/client connected to the switchport.

Upon successful 802.1X authentication of the endpoint (example: Cisco IP Camera) by ISE, the authorization policy (as shown in Figure 296) is matched to apply the result set (VLAN, SGT, etc.) on the switch port by ISE. It also provides the endpoint access (based on authorization policy configuration) to CCI network.

If 802.1X authentication of the endpoint (example: Cisco IP Camera) by ISE fails, MAB authentication event is triggered for the wired endpoint. The authorization policy (as shown in Figure 296) is matched to apply the result set (VLAN, SGT, etc.) on the switchport by ISE, if MAB is successful. It also provides the endpoint access (based on authorization policy configuration) to CCI network.

Implementing Firewall Using Firepower for CCI Network

Cisco Firepower is an integrated suite of network security and traffic management products that is deployed either on purpose-built platforms or as a software solution. In the CCI solution, the Firepower model used is the 2140 series. In this implementation, the Firepower device is being managed by the Firepower Management Center (FMC).

A FMC is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for your Firepower System deployment. FMC controls the network management features on your devices: switching, routing, NAT, VPN, and so on.

In CCI solution, FMC has been deployed as a virtual machine. It has to be configured in the same network as the management ports of Firepower. For more details on FMC and the configuration steps for management of Firepower, refer to:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/introduction_to_the_cisco_firepower_system.html

Firepower Installation and HA Configuration

In the CCI solution, Firepower is being used to provide network security between the zones and Internet connectivity to the internal devices. Firepower has been configured with high availability to provide redundancy in the setup. A high availability pair results in a single logical system for policy application, system updates, and registration. With device high availability, the system can fail over either manually or automatically.

Before starting with the other configurations on the Firepower, it must be brought up in routed mode and configured for management via FMC.

1. Configure Routed Mode

   Routed mode for Firepower must be chosen at the very beginning as a part of the initial configuration when the device boots up for the first time. If mode has not been set to routed in the beginning, the following steps should be followed to configure the right mode.

   At the Firepower CLI, the following commands are issued in sequence to configure it for routed mode:

   ```
   configure firewall routed
   ```

   For example:

   ```
   > configure firewall routed
   This will destroy the current interface configurations, are you sure that you want to
   proceed? [y/N] y
   The firewall mode was changed successfully.
   ```

   Alternatively, the mode can be also be changed from FMC by following the steps in the following URL:

   – https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/interface_overview_for_firepower_threat_defense.html

2. Configure Management via FMC

   Follow the steps listed in the Quick Start Guide to perform the initial configuration of the Firepower Threat Defense (FTD) and configure the management of the FTD via FMC:

   – https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/ftd-fdm-2100-qsg.html

Configuring Firepower for CCI Solution Use Cases

To configure the Firepower in the CCI network as a Firewall, a sequence of steps must be done as shown in Figure 297:

Figure 297 Cisco Firepower Configuration Flow Using FMC

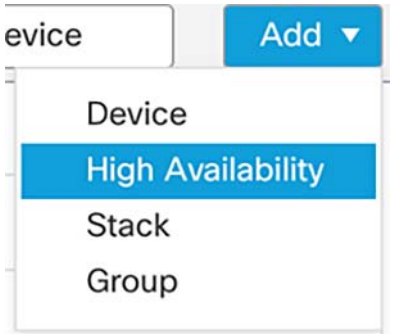
1. Configure High Availability (HA):

   After adding both devices to the Firepower Management Center, the following steps must be followed to configure HA:

   a. Choose **Devices-> Device Management**.

   b. From the **Add** drop-down list, choose **High Availability**, as shown in Figure 298:

Figure 298 Adding Device in HA



c. Enter a display name for the high availability pair.

d. Under **Device Type**, choose **Firepower Threat Defense**.

e. Choose the **Primary Peer device** for the high availability pair.

f. Choose the **Secondary Peer device** for the high availability pair.

g. Click **Continue**.

h. Under **LAN Failover Link**, choose an interface with enough bandwidth to reserve for failover communications.

Note: Only interfaces that do not have a logical name and do not belong to a security zone will be listed in the **Interface** drop-down list in the **Add High Availability Pair** dialog box.

i. Type any identifying Logical Name.

j. Type a Primary IP address for the failover link on the active unit. This address should be on an unused subnet.

Note: 169.254.0.0/16 and fd00:0:0:*::/64 are Firepower internally-used subnets and cannot be used for the failover or state links.

k. Click **OK**. This process takes a few minutes as the process synchronizes system data.

For more details on how to configure HA, complete the steps listed at:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/high_availability_for_firepower_threat_defense.html

2. Configure Interfaces:

   To configure the interfaces, the following steps must be completed:

   a. Choose **Devices-> Device Management** and edit the HA pair. Click the **Interfaces** tab.

   b. Select the **Edit** icon next to the interface and fill in the details for the interfaces, as shown in Figure 299:

Figure 299 Configuring Interfaces

Similarly, bring up all the interfaces as per topology by enabling them and assigning IP addresses and names to the interfaces following the above steps.

3. Configure Static and Dynamic Routing:

   Firepower acts as the Internet edge device in the network. Therefore, a static default route must be configured on the Firepower for all the devices to reach the Internet.

   The following lists the steps to configure static route for CCI network Internet reachability via Firepower:

   a. Choose **Devices-> Device Management** and edit the HA pair. Click the **Routing** tab.

   b. Select **Static Route** from the table of contents.

   c. Click **Add Routes**.

   d. Click the **IPv4** radio button.

   e. Choose the **Interface** to which this static route applies.

   f. In the **Available Network** list, choose the **destination network**.

   g. Following the above method, add the **static route** for the VN networks via the fusion router.

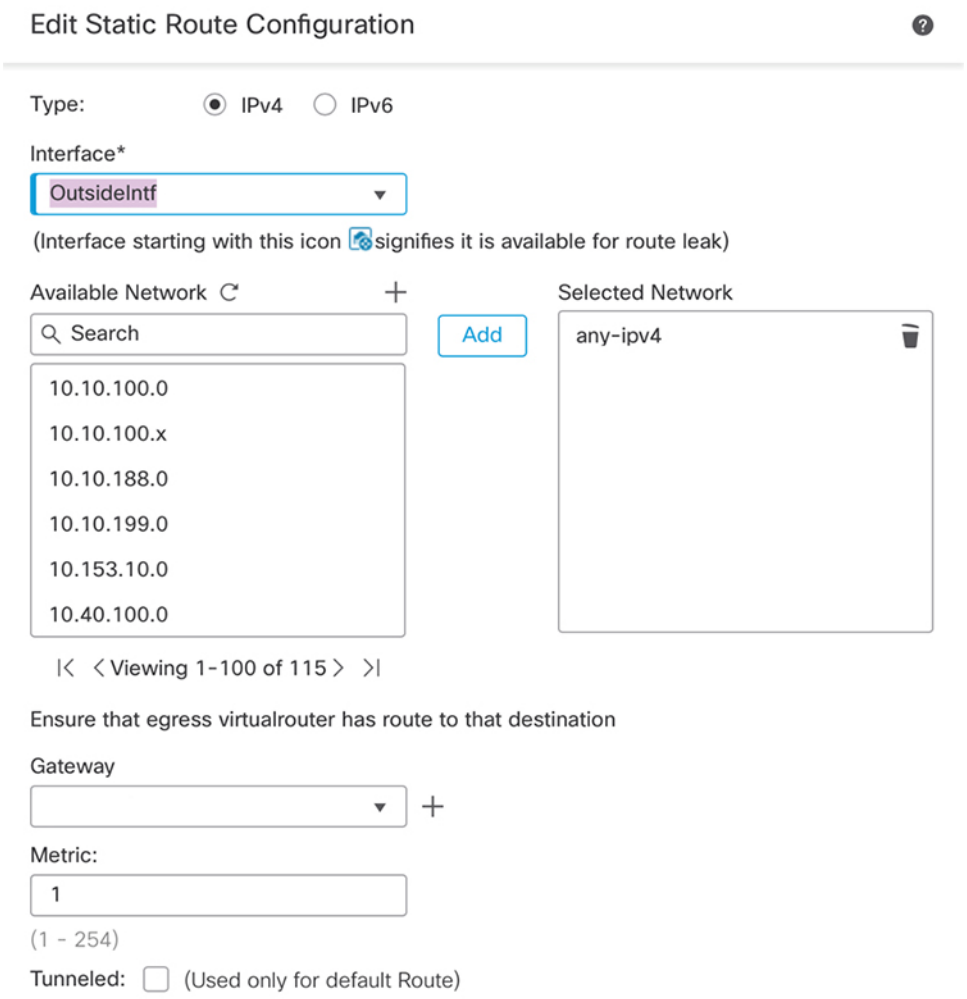
Static and Default Routes for Firepower Threat Defense

To define a default route, create an object with the address 0.0.0.0/0 and select it here.

a. In the **Gateway** or **IPv6 Gateway** field, enter or choose the gateway router, which is the next hop for this route. You can provide an **IP address** or a **Networks/Hosts object**.

b. In the **Metric** field, enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is **1**, as shown in Figure 300:

Figure 300 Example to Add a Static Default Route



Similarly, add the IPv6 static routes by choosing the **IPv6** radio button and entering the value in fields to enable the IPv6 communication.

The routes display in an example configuration, as shown in Figure 301:

Figure 301 An Example View of IPv4 and IPv6 Routes Configured on Firepower

IPv4 Routes				
10.153.10.0	InsideIntf	10.40.100.100	false	1
IPv4-Private-10.0.0.0-8	InsideIntf	10.40.100.100	false	1
172NW	ToSDAccessCSR	10.10.204.2	false	1
any-ipv4	OutsideIntf	[redacted]	false	1
IPv6 Routes				
SCADA	InsideIntf	2001:db8:16:107::1	false	1
FNDNetwork	ToSDAccessCSR	2001:db8:16:109::2	false	1
SLCNetwork	InsideIntf	2001:db8:16:107::1	false	1

For more detailed step-by-step instructions, refer to the following URL:

- https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/static_and_default_routes_for_firepower_threat_defense.html

Configuring Dynamic Routing Protocol

For dynamic exchange of routes between Firepower, the HER, and the fusion router, complete the steps described below. In this implementation, EIGRP routing protocol is used on the Firepower using FlexConfig.

a. Go to **Devices-> FlexConfig**.

b. Create a new policy by adding name and description and selecting the **FTD HA** pair from available devices. Then click **Save**.

c. Select **Eigrp_configure** from the list of system-defined FlexConfig.

d. Create a copy of this config and rename it.

e. In the created copy, edit the variables **$eigrpAS** and **$eigroNetworks** to hold values of the autonomous system in use for topology and the networks to be advertised. This can be done by editing the variable from **Objects-> Object Management->FlexConfig-> Text Object**.

The Object should appear as shown in Figure 302:

Figure 302 Configuring EIGRP on Firepower

f. Append the FlexConfig created in the Step 5, click **Save**, and then click **Deploy**.

g. To verify the formed EIGRP neighborship, issue the following on CLI:

```
> show eigrp neighbors
EIGRP-IPv4 Neighbors for AS(2000)
H   Address                 Interface       Hold Uptime   SRTT   RTO   Q  Seq
                                            (sec)         (ms)       Cnt Num
2   10.10.204.3             ToSDAccessCSR    12      1w1d 1      200  0    50

1   10.10.204.2             ToSDAccessCSR    14      1w3d 2      200  0   202

0   10.40.100.101           InsideIntf       11      1w4d 1      200  0    90
```

h. Similarly, verify the routing table for the received routes via EIGRP:

```
> show route eigrp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is <Gateway> to network 0.0.0.0

D        10.10.100.0 255.255.255.0
           [90/28416] via 10.10.204.3, 1w1d, ToSDAccessCSR
```

Note: The above output is only a sample output and large section of output may have been omitted.

Note: As a best practice, when a change needs to be made in the FlexConfig , the **Eigrp_unconfigure** function should be called so as to avoid any errors (similar to the no <config> of the CLI.)

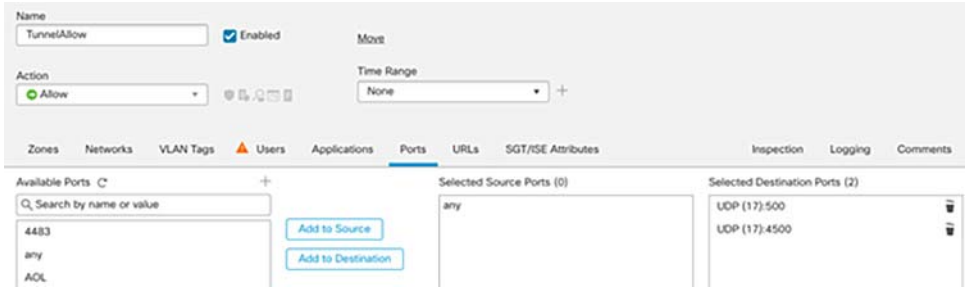
4. Configure Access Control Policy:

Access control policy will allow or disallow communication between the different zones.

a. In order to configure the **Access Control Policy**, click **Policies -> Access Control -> New Policy**.

b. Enter the details as shown in Figure 303:

Figure 303 Adding a New Policy

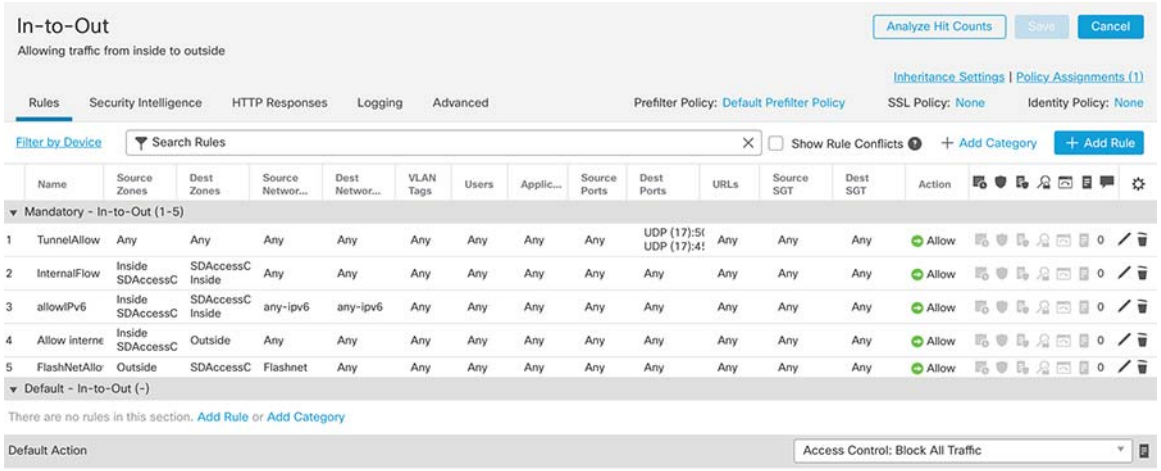


c. Click **Edit policy -> Add Rule** and then add the source and destination zone for allowing communication between the fusion router and HER, and vice versa.

d. Add another rule to Enable the UDP port 500 and 4500 to allow the tunnel establishment between the CGR and the HER and also between the CIMCON LG cloud service router end and the HER. Also, include the rule to allow the communication from source IP of FlashNet Application server (in cloud) to the CCI network for FlashNet LoRaWAN Use case. Work with FlashNet support to obtain the source IP of FlashNet Application server.

The rules will appear as shown in the example in Figure 304:

Figure 304 Rules Configured Under Access Control Policy



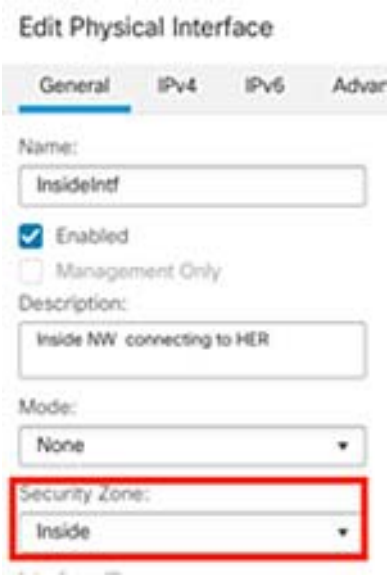
5. Configure NAT policy:

   For the devices to reach the Internet via the Firepower, a NAT policy is configured. Dynamic and static NATs are configured in CCI solution. When devices need to be accessible from outside, a static NAT is implemented; otherwise dynamic NAT is implemented. For example, for internet access of internal devices dynamic NAT policy is deployed, whereas for building a tunnel to the HER and for Flashnet use case a static NAT is implemented.

   Following are the steps listed for the same:

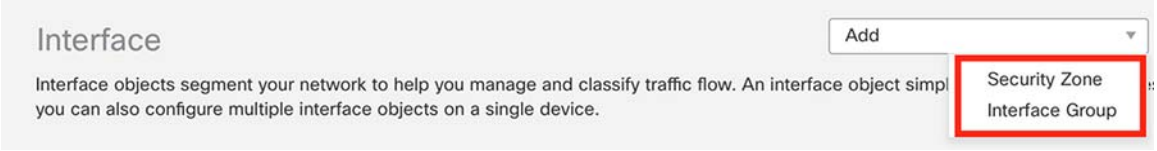
   a. Assign interfaces to Security Zones, if not already assigned in the **Creating Interfaces** section, as shown in Figure 305.

Figure 305 Editing Interface



   b. You can create/edit **Interface Groups** and **Security Zones** from the **Objects -> Object Management> Interface** page, as shown in Figure 306.

Figure 306 Adding a Security Zone



c. Configure NAT on FTD by creating a NAT policy. Navigate to **Devices -> NAT** and create a NAT Policy.

d. Select **New Policy -> Threat Defense NAT**, as shown in the image.

e. Specify the policy name and assign it to the HA pair.

f. To add a static and a dynamic NAT rule to the policy, click **Add Rule**.

g. Specify these as per task requirements, as shown in Figure 307 and Figure 308.

Figure 307 Configuring a NAT Policy

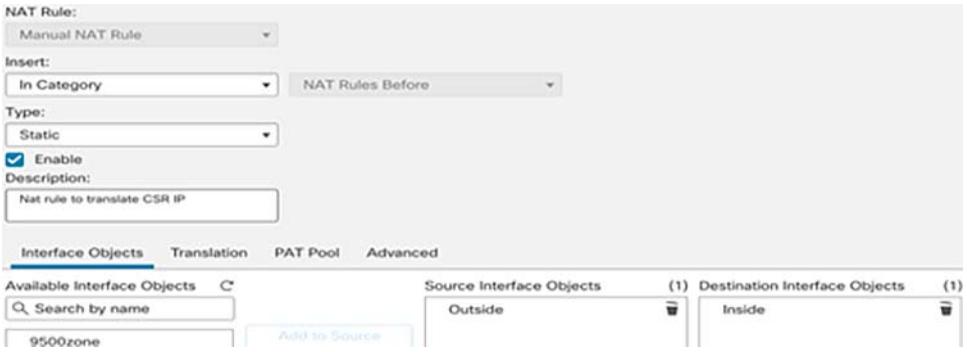
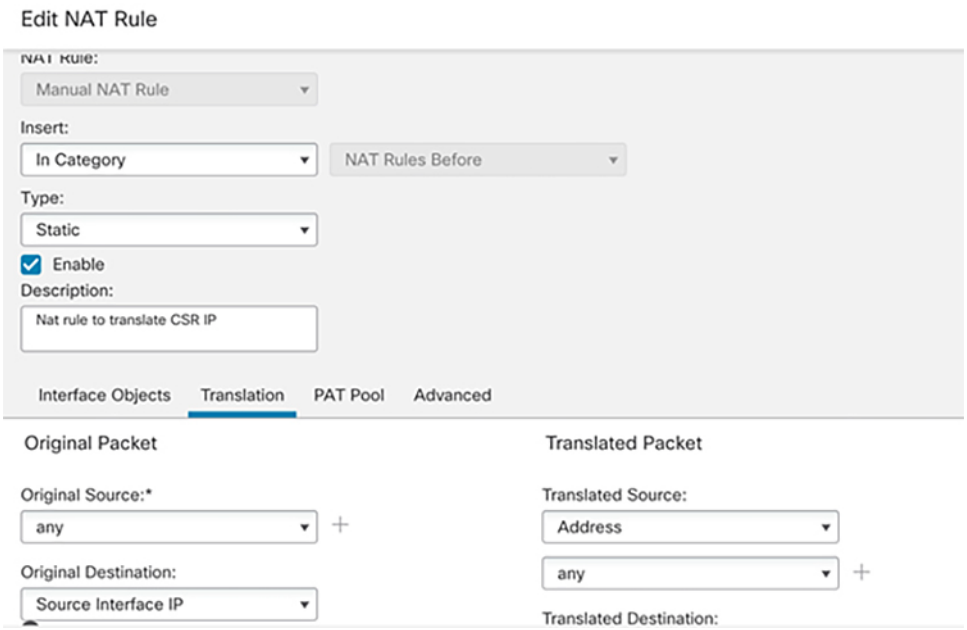


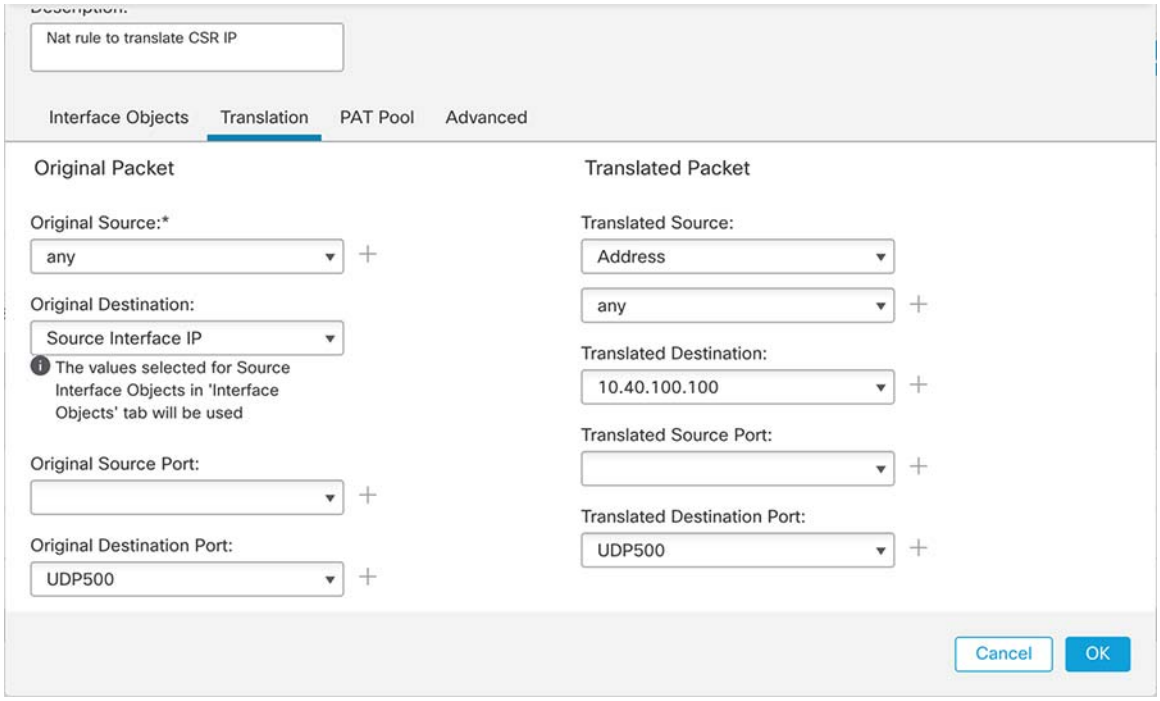
Figure 308 Editing a NAT Policy



h. Similarly, create a static policy for UDP port 4500 as shown in Figure 309.

Figure 309 NAT Policy for Tunnel Establishment–1

Figure 310 NAT Policy for Tunnel Establishment–2



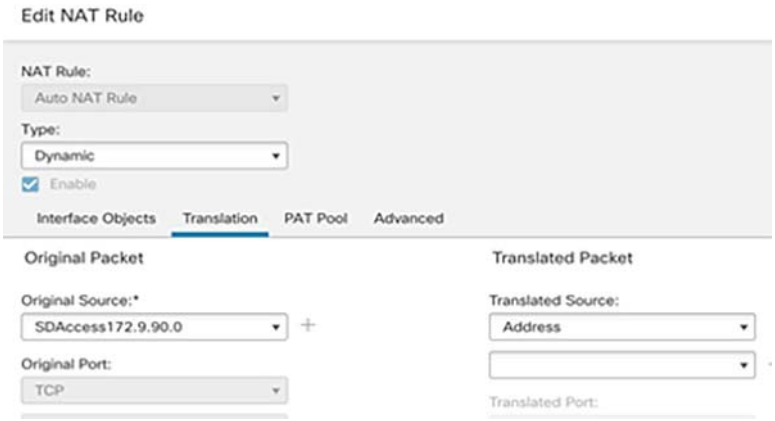
Follow the above steps to create a static NAT for the HER to gain Internet access for FlexVPN tunnel establishment to a remote site.

i. Similarily, configure static NAT for Flashnet Application Server to be able to reach TPE. Here, the public IP used by the Flashnet Application server (obtained from Flashnet support) is to be configured as source address as shown in Figure 311.

Figure 311 Creating a Static NAT Policy for Flashnet Use Case

j. Now create a dynamic NAT rule for all the networks that need Internet access and are connected on the fusion router following the similar steps and choosing dynamic instead of static, as shown in Figure 312:

Figure 312 Editing a Dynamic NAT Policy



k. Verify the configuration. From CLI:

```
Connect ftd
show running-config nat
nat (OutsideIntf,InsideIntf) source static CimconCSR CimconCSR destination static interface
10.40.100.0 service SVC_21474841183 SVC_21474841183 description Nat rule to translate CSR IP
nat (OutsideIntf,InsideIntf) source static CimconCSR CimconCSR destination static interface
10.40.100.0 service SVC_21474841184 SVC_21474841184
!
object network SDAccess172.9.90.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess172.10.90.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess172.20.90.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess172.15.70.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess172.16.70.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess172.17.70.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDaccess192.100.80.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.100.90.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.0
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.4
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.8
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.12
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.16
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.168.70.20
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.0.50.11
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface
object network SDAccess192.0.50.12
 nat (ToSDAccessCSR,OutsideIntf) dynamic pat-pool interface:

> show nat
Manual NAT Policies (Section 1)
```

```
1 (OutsideIntf) to (InsideIntf) source static CimconCSR CimconCSR  destination static interface
10.40.100.0 service SVC_21474841183 SVC_21474841183 description Nat rule to translate CSR IP
    translate_hits = 51, untranslate_hits = 51
2 (OutsideIntf) to (InsideIntf) source static CimconCSR CimconCSR  destination static interface
10.40.100.0 service SVC_21474841184 SVC_21474841184
    translate_hits = 1, untranslate_hits = 214

Auto NAT Policies (Section 2)
1 (ToSDAccessCSR) to (OutsideIntf) source dynamic SDAccess192.0.50.11 pat-pool interface
    translate_hits = 2, untranslate_hits = 12
2 (ToSDAccessCSR) to (OutsideIntf) source dynamic SDAccess192.0.50.12 pat-pool interface
    translate_hits = 2, untranslate_hits = 12
> show xlate
4 in use, 51 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
UDP PAT from OutsideIntf: <CIMCON LG cloudservice router's public IP> 0 to InsideIntf: <CIMCON LG
cloudservice router's public IP> 0
    flags srIT idle 18:25:29 timeout 0:00:00
UDP PAT from InsideIntf:10.40.100.0/24 500-500 to OutsideIntf:<Cisco headend public IP> 500-500
    flags srT idle 18:25:29 timeout 0:00:00
UDP PAT from OutsideIntf: <CIMCON LG cloudservice router's public IP> 0 to InsideIntf: <CIMCON LG
cloudservice router's public IP> 0
    flags srIT idle 359:24:59 timeout 0:00:00
UDP PAT from InsideIntf:10.40.100.0/24 4500-4500 to OutsideIntf:<Cisco headend public IP>
4500-4500
    flags srT idle 284:45:51 timeout 0:00:00
```

Note: The above output is only a sample output and large section of output may have been omitted.

For more details on configuring NAT policy, refer to the following URL:

- https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

Configuring Micro-Segmentation Using Scalable Groups and SGACLs

The SD-Access solution has the capability to define security rights from Cisco DNA Center, which will leverage the Identity Services Engine (ISE) to enforce policies that will secure our network. SD-Access provide segmentation that enables an organization to implement security between different user groups and devices in the network. This is very similar to what industry has been doing for many years based on the IPs with ACLs, whereas in SD-Access the same can be achieved based on the user identity profile (in ISE) and regardless of IP (subnet).

Segmentation in SD-Access takes place at both a macro and a micro level through VNs, as discussed in previous sections (Macro Segmentation) and Scalable Groups (Micro Segmentation), respectively. VNs provide routing isolation between the different entity and SGT provides isolation within the routing entity, i.e., within VRF.

Scalable groups comprise a grouping of users, end point devices, or resources that share the same access control requirements. These groups (known in Cisco ISE as security groups or SGs) are defined in Cisco ISE. Scalable Group Tags (SGT) will provide micro-segmentation within the VN (within routing visibility or partition). That is, IP reachability is available within subnets of the VN or hosts within the VN, However, based on the user's identity profile, the traffic flow needs to be controlled between different groups using permit/deny SGACLs.

For more details on the CCI Security Policy design with Segmentation, refer to the *CCI Solution Design Guide*, which can be found at the following URL:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html

In this implementation, an example configuration of Scalable Groups and Scalable Group-based Access Control Policy (SGACL) validated in this CVD is provided as a reference/guideline to implement micro-segmentation in the CCI network.

Note: Example micro-segmentation policies with Scalable Groups and SGACLs covered in this section are reference configuration only. Depending on your network deployment and CCI vertical use cases security requirements, you should choose to create your new Scalable Groups or SGACLs to implement the micro-segmentation in the CCI network.

In the following example, micro-segmentation policies within SnS_VN are created to achieve the policy enforcement, as shown in Table 28. Policy deployment has a default permit policy (blocked list policy model deployment). The deny policy enforcement would happen at the egress node side where the destination SGT resides; in our case, the Catalyst 9300 switch stack (FiaB) in SD-Access is the policy enforcement point as per the CCI solution design.

Table 28 Example IP Addressing Prefixes and Convention Followed

Destination / Source	SNS_Servers	SnS_Traffic_Servers	SnS_SGT	SnS_Traffic
SnS_SGT	Permit	Deny	Permit	Deny
SnS_Traffic	Deny	Permit	Deny	Permit
SnS_Servers	Permit	Deny	Permit	Deny
SnS_Traffic_Servers	Deny	Permit	Deny	Permit

Note: Make sure that Cisco DNA Center with ISE are successfully integrated and that your Fabric Edge nodes are successfully registered on ISE before implementing micro-segmentation in the CCI network.

Prerequisites for SGACL Configuration

Before we look into the pre-checks required before pushing SGACLs from Cisco DNA Center, let's understand what is Protected Access Credential (PAC) and its significance. PAC is the Protected Access Credential generated by the server and provided to the client. It consists of:

- PAC key (random secret value, used to derive TLS primary and session keys)
- PAC opaque (PAC key + user identity, all encrypted by the EAP-FAST server primary key)
- PAC info (server identity, TTL timers)

The server, ISE in this case issuing the PAC will encrypt the PAC key and identity using the EAP-FAST server primary key, (that is, the PAC opaque) and sends the whole PAC to the client (Catalyst 9300 FiaB devices, in this case). The server does not keep or store any other information, except the primary key, which is the same for all PACs. Once the PAC opaque is received, it is decrypted using the EAP-FAST server primary key and validated. The PAC key is used to derive the TLS primary and session keys for an abbreviated TLS tunnel. New EAP-FAST server primary keys are generated when the previous primary keys expire. In some cases, a primary key can be revoked.

Following are some checks that can be completed to make sure your network devices and ISE have been successfully integrated before we start to configure policy enforcement using SGTs:

- Make sure the PACs are provisioned on the network switches by Cisco DNA Center:

```
Edge_Device#show cts pacs
AID: E74D665D34C206E451B00F66D2209918
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: E74D665D34C206E451B00F66D2209918
  I-ID: FCW2304G0VH
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 13:07:09 UTC Wed Oct 30 2019
PAC-Opaque:
000200B800030001000400010E74D665D34C206E451B00F66D22099180006009C0003010053E42932DA5A892B8000AF04EB<
output-snipped>
```

```
Refresh timer is set for 12w2d
```

- Check the configuration on the network switches for ISE communication over RADIUS. These configurations are pushed automatically by DNA Center while provisioning:

```
aaa group server radius Cisco DNA Center-client-radius-group
 server name Cisco DNA Center-radius_X.X.X.X
 ip radius source-interface Loopback0
aaa group server radius Cisco DNA Center-network-radius-group
 server name Cisco DNA Center-radius_X.X.X.X
 ip radius source-interface Loopback0
aaa authentication login default local
aaa authentication login VTY_authen group Cisco DNA Center-network-radius-group local
aaa authentication dot1x default group Cisco DNA Center-client-radius-group
aaa authorization exec default local
aaa authorization exec VTY_author group Cisco DNA Center-network-radius-group local
if-authenticated
aaa authorization network default group Cisco DNA Center-client-radius-group
aaa authorization network Cisco DNA Center-cts-list group Cisco DNA Center-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group Cisco DNA Center-client-radius-group
aaa accounting exec default start-stop group Cisco DNA Center-network-radius-group
aaa server radius dynamic-author
 client X.X.X.X server-key 7 143453180F0B7B7977
pac key 7 072C605F4D06485744
```

Procedure of SGACL Configuration

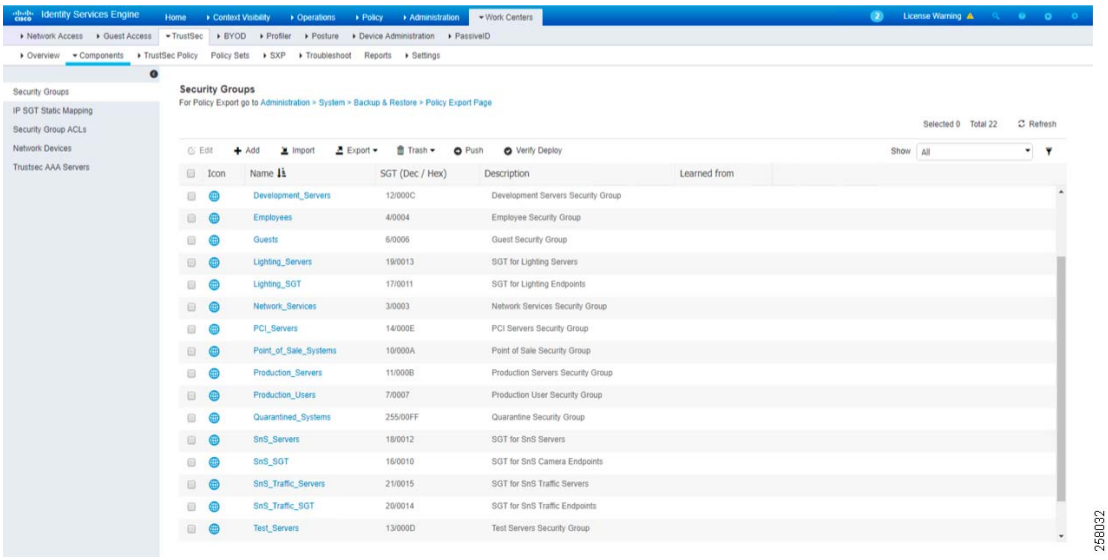
Complete the following steps to configure SGACLs in the CCI network for an example implementation shown in Figure 313:

1. Creating SGTs on ISE

   SGTs can be assigned statically for a resource on Cisco DNA Center or ISE. This value is inserted into the **Reserved** field of the VXLAN header in SD-Access.

   - On ISE, navigate to **Work center-> Trustsec-> Components-> Security Groups-> Add**. Each SGT gets assigned a number, as shown in Figure 313:

Figure 313 Cisco ISE Scalable Groups List

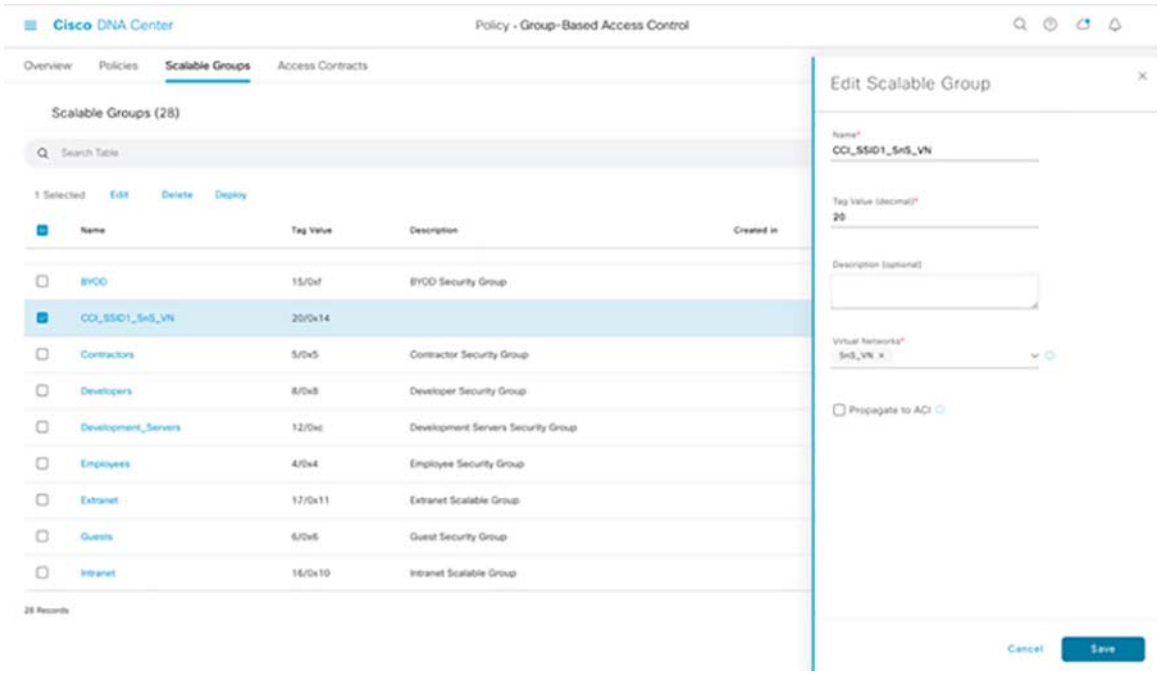


2. Mapping SGTs to Virtual Network on Cisco DNA Center

   SGTs that were created on ISE are seen on Cisco DNA Center and those Scalable Groups have to be mapped to the respective VNs.

   – On Cisco DNA Center GUI, select the VN from **Policy-> Group-Based Access Control > Scalable Groups** and select the scalable groups from the available list to **Edit**, as shown in Figure 314, and then click **Save**.

Figure 314 Cisco DNA Center Scalable Groups Mapping to a VN



Confirm that the environment data (SGTs) are being successfully downloaded by the switch from ISE on the Fabric edge devices (i.e., FiaB). Also, notice that each SGT name is mapped to a number. This mapping is critical since in packet captures, you will only see the numbers, not the names of the SGTs.

```
C9300-HQ-Stack#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
  Server: X.X.X.X, port 1812, A-ID E74D665D34C206E451B00F66D2209918
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
    3-00:Network_Services
    4-00:Employees
    5-00:Contractors
    6-00:Guests
    7-00:Production_Users
    8-00:Developers
    9-00:Auditors
    10-00:Point_of_Sale_Systems
    11-00:Production_Servers
    12-00:Development_Servers
    13-00:Test_Servers
    14-00:PCI_Servers
    15-00:BYOD
    16-00:SnS_SGT
    17-00:Lighting_SGT
    18-00:SnS_Servers
    19-00:Lighting_Servers
```

```
    20-00:SnS_Traffic_SGT
    21-00:SnS_Traffic_Servers
    255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 13:07:22 UTC Sun Aug 4 2019
Env-data expires in   0:08:10:57 (dd:hr:mm:sec)
Env-data refreshes in 0:08:10:57 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

3. Creating Policy and Contracts on Cisco DNA Center

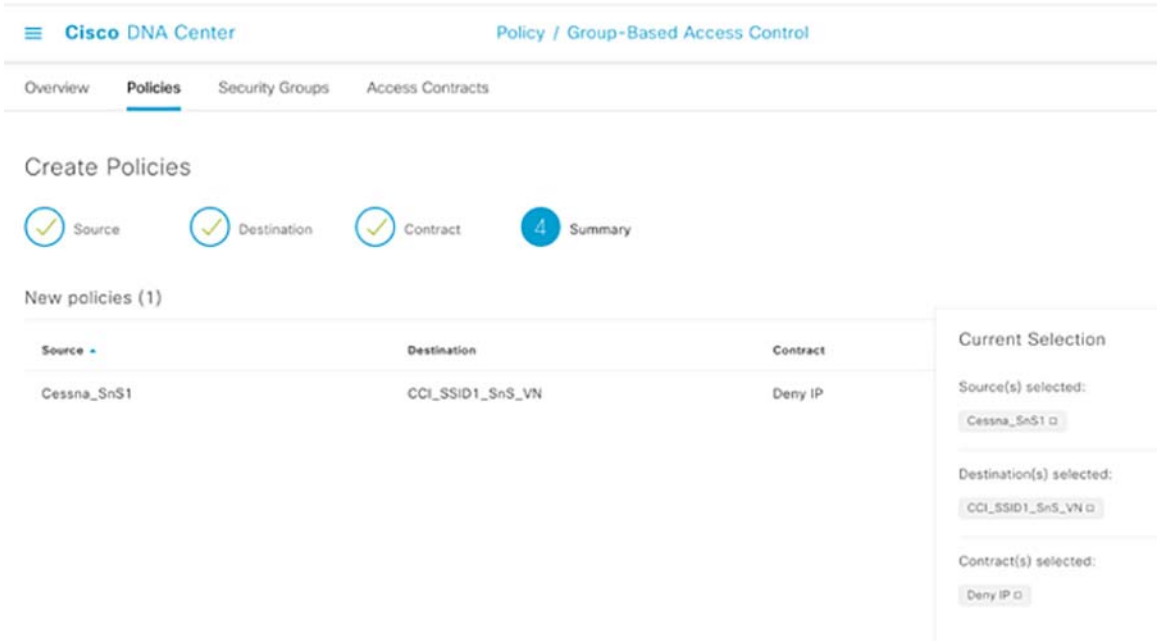
   Cisco ISE PxGrid Policy deployment has default permit policy (blocked list policy model deployment). All the SGTs are allowed to communicate with each other within VN. If an SGT has to be access restricted to the rest of the SGTs then 1: N access policy has to be created.

   In order to limit what type of traffic will be able to traverse the network, create an access contract. You can create a contract that will contain the ports and protocols that are allowed or prohibited to communicate between different groups or by default "deny" and "permit" contracts are present in Cisco DNA Center which you can leverage.

   In this example, we have SGTs within a VN and create a deny policy between them, as shown in Figure 315.

   a. On Cisco DNA Center, navigate to **Policy-> Group-Based Access Control Policies**, click **Create Policies** and then select source and destination SGT Groups and select **Contract**. Then choose deny contract rule between the SGTs, as shown in Figure 315:

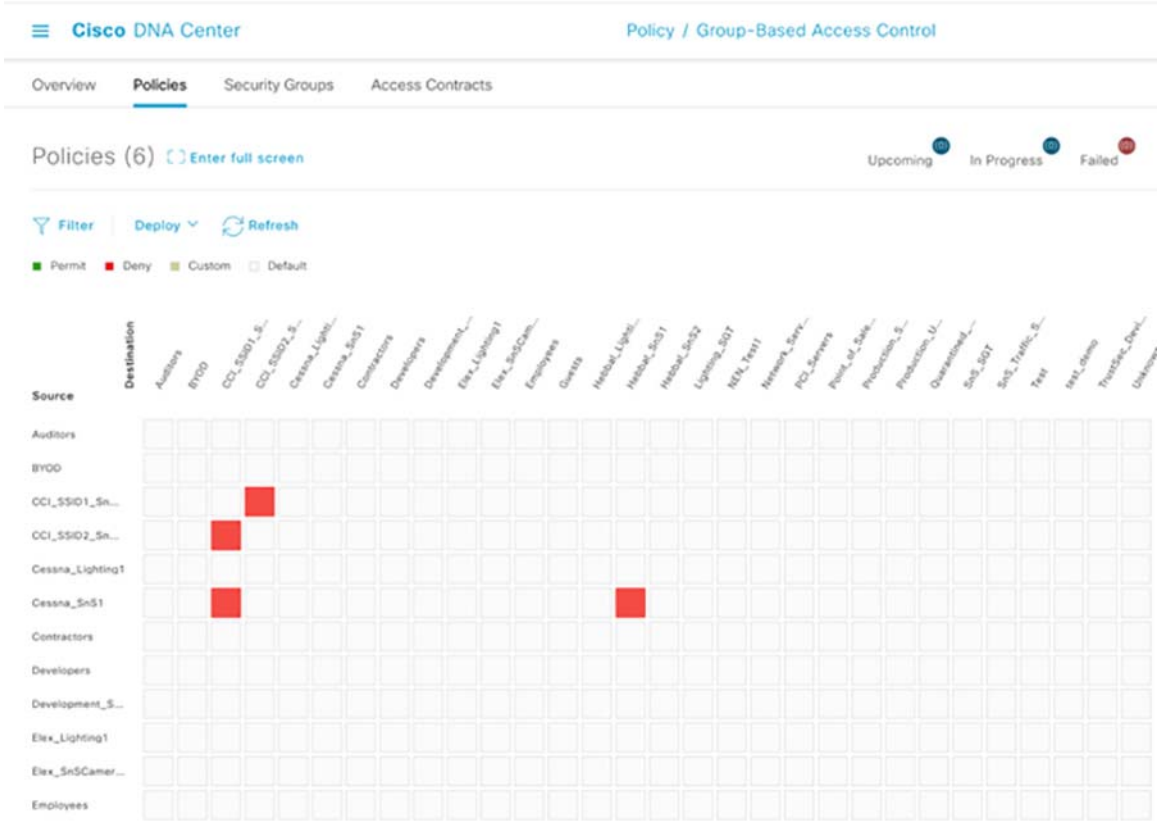
Figure 315 Cisco DNA Center Scalable Groups-based Policy Creation View



The Cisco TrustSec (CTS) matrix is where policies are defined initially in ISE. It contains two axis (the source axis and destination axis). You will see the deny policy between the SGTs as per our bi-directional policy enforcement. This matrix will be controlled by the Cisco DNA Center controller and all the policy changes can be done on the Cisco DNA Center.

b. The applied policy with the deny contract can be seen on Cisco ISE GUI in matrix format. Navigate to **Work Centers-> TrustSec Policy-> Egress Policy-> Matrix**. Figure 316 shows a sample policy matrix defined as per the configuration:

Figure 316 Cisco DNA Center Scalable Groups-based Policy Matrix View



4. Verify the SGACL configuration on the FiaB (Fabric edge).

The SGACL configuration is downloded to the FiaB device can be verified as below:

```
C9300-HQ-Stack#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 16:SnS_SGT to group 20:SnS_Traffic_SGT:
        Deny IP-00
IPv4 Role-based permissions from group 18:SnS_Servers to group 20:SnS_Traffic_SGT:
        Deny IP-00
RBACL Monitor All for Dynamic Policies: FALSE
RBACL Monitor All for Configured Policies : FALSE
```

In this example, we have created SGACLs using Cisco DNA Center between the SGT groups within the VN and the configuration has been pushed to the devices from the ISE. Now the traffic filtering can be validated with role-based counters command:

```
Edge_Device#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          5          14075822   0          0
16      20      0          120        0          0          0          0
18      20      0          0          0          0          0          0
```

Implementing Cisco Cyber Vision Network Sensors

Cisco Cyber Vision Center and Sensors Deployment

This section describes the deployment of Cisco Cyber Vision Center (CVC) in Shared Services and the deployment of network sensors on IE3400 and IE3300-X Series switches in CCI PoPs and IR1101 gateway in RPoPs.

Cisco Cyber Vision Center Installation

The Cyber Vision Center can be deployed as a virtual machine (VM) or as a hardware appliance. In this deployment, the standalone Cyber Vision Center (standalone) is deployed as a VMs on a Cisco Unified Computing System (UCS) in the CCI Shared Services network.

For step-by-step instructions on installation and resource recommendations of CVD, refer to the Cisco Cyber Vision Center VM Installation Guide at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_4_0_0.pdf

It is recommended to install the Cyber Vision Center application in the CCI Shared Services network with dual interfaces;: one for management and the other for sensor communication. Following is an example of the IP addressing schema used in CVC installation.

■Admin Interface (eth0): 10.104.206.225 (Routable IP address for CVC UI access)

■Collection interface (eth1): 10.10.100.33 (shared services network IP)

■Collection network gateway: 10.10.100.1 (shared services gateway)

■NTP: 10.10.100.1

Refer to the section “Cisco Cyber Vision Operational Technology (OT) Flow and Device Visibility Design” in the CCI General Solution Design Guide for the detailed design and deployment considerations for CVC, Network Sensors on IE3400 and IE3300-X series switches, and the IR1101 for RPoP in a CCI deployment here:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html

Sensor Installation

There are two types of Cyber Vision Sensor: hardware and network. The hardware Sensor is the Cyber Vision IOx application installed on an Industrial Compute Gateway 3000 (IC3000) appliance. The network Sensor is the Cyber Vision IOx application installed on the supported switches and routers. In the CCI solution, only network sensors on IE switches and IR router are used, as described in the design.

For Network Sensors, there are three methods of installation: switch CLI, switch web interface, and Cyber Vision Center Extension. This guide discusses the network sensor installation using the Cyber Vision Center Extension feature. Refer to the Cyber Vision documentation for guidance on manual installations here, if needed:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf

Prior to any installation, the following prerequisite configurations must be done on the IE switches in CCI PoPs:

1. Verify that Extended Node (IE3300 10G aka IE3300-X) and PEN (IE3400) switches in the ring are onboarded into the fabric with switches images running from switch flash instead of sdflash and the IE switch boot variable “ENABLE_FLASH_PRIMARY_BOOT” is set to “yes”.

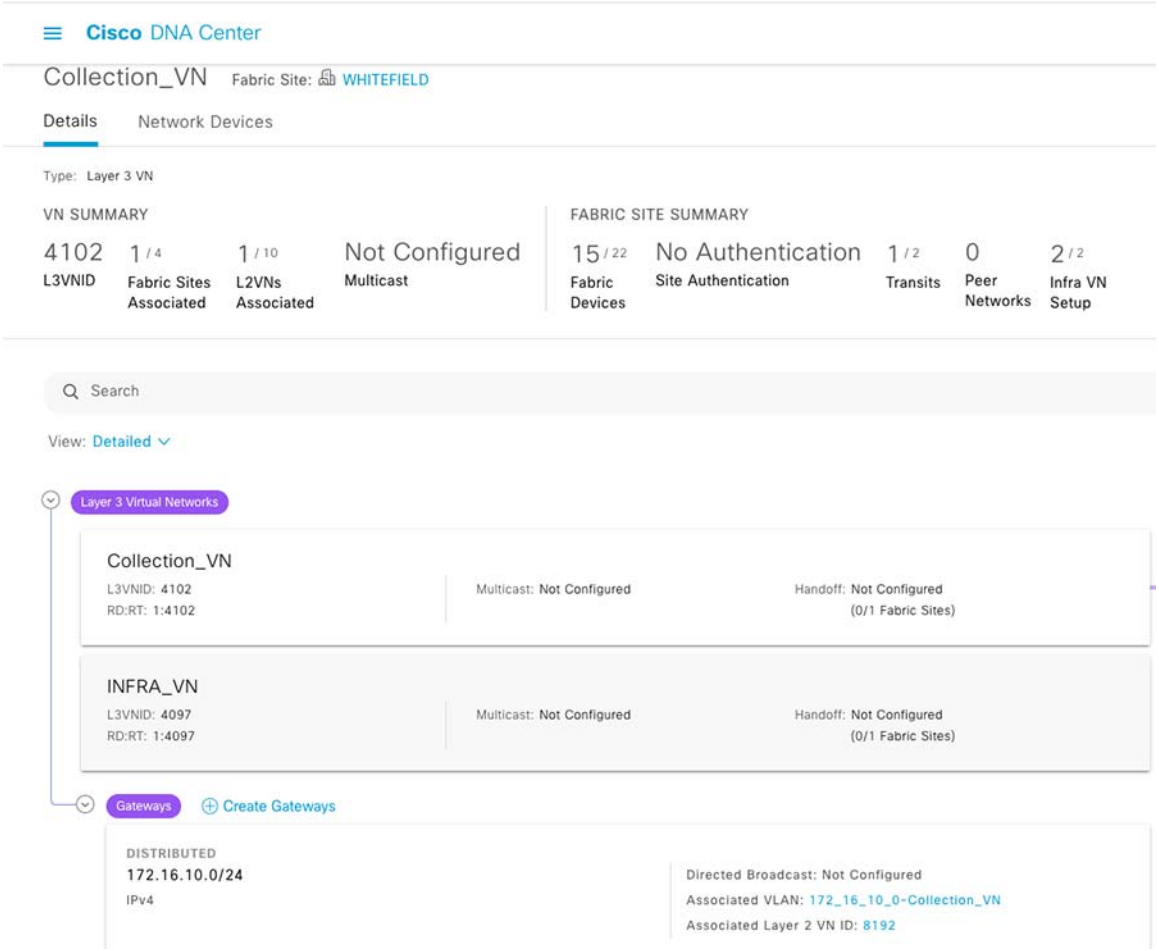
   ```
   On a IE3300 10G or IE3400 switch in a CCI PoP:
   SN-FCW24110H0T#show boot
   Current Boot Variables:
   BOOT variable = flash:ie3x00-universalk9.1761a.SPA.bin;
   Boot Variables on next reload:
   BOOT variable = flash:ie3x00-universalk9.1761a.SPA.bin;
   Config file = flash:/nvram_config
   ENABLE_FLASH_PRIMARY_BOOT = yes
   <snipped>
   ```

   Note: You must boot the IE switch image from switch flash memory because the sdflash drive on the switch is formatted with the ext4 file system and the sensor application is installed and running from the sdflash memory of the switch.

2. Ensure network reachability between the Cyber Vision Center and the IE Switches in the PoPs. A separate collection Virtual Network (VN) is configured along with an IP subnet pool for Sensors on IE switches using the Cisco DNA Center at CCI PoP sites. Figure 1The figure below shows an example configuration of a Collection_VN and IP pool for Sensor communication with CVC. (For example, 172.16.10.x/24 at Whitefiled PoP fabric site) communication with CVC.

   Note: An IE switch in CCI PoP may have been configured with VLANs in multiples VNs by the Cisco DNA Center for switch management, CV sensor communication, and one or more VLANs for IT/OT data traffic. (For example, Extended node VLAN in INFRA_VN) CV sensor communication (VLAN in collection VN), and one or more VLANs for IT/OT data traffic (VLAN in SnS_VN for endpoints).

Figure 317 CCI Collection VN configuration with IP Pool Binding



3. Ensure that the FiaB switch and the IE switches in the CCI PoPs are configured with collection network VLAN.

On FiaB switch at a PoP site:

```
Akash-C9300-Whitefield#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
<snipped>
1023 SnS_VN                           active    L2LI0:8190, Gi1/0/13
1024 Scada_VN                         active    L2LI0:8191,
1025 172_16_10_0-Collection_VN        active    L2LI0:8192,
<snipped>
Akash-C9300-Whitefield#show run interface Vlan 1025
interface Vlan1025
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f818
 vrf forwarding Collection_VN
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 10.10.100.42
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
```

```
 lisp mobility 172_16_10_0-Collection_VN-IPV4
 no autostate
end
```

On IE3300-A switch at the PoP site ring:

```
SN-FCW24110H0T#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
<snipped>
1023 SnS_VN                           active    Gi1/7
1024 Scada_VN                         active
1025 172_16_10_0-Collection_VN        active
```

4. Configure an SVI in the collection network VLAN on the IE switch where the CV sensor is to be installed. EAn example SVI configuration on Collection VLAN in IE3300-A 10Gig switch is:

```
SN-FCW24110H0T#show run interface Vlan 1025
!
interface Vlan1025
 ip address 172.16.10.250 255.255.255.0
end
```

5. Verify that the IE switch can reach the CVC Collection Interface IP at the shared services network in the CCI HQ site.

On the IE switch in a PoP, ping CVC collection network interface:

```
SN-FCW24110H0T#ping 10.10.100.33 source vlan 1025
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.33, timeout is 2 seconds:
Packet sent with a source address 172.16.10.250
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Note: the IP 10.10.100.33 in the above example configuration is the IP address of Cyber Vision Center collection network interface configured during the installation of CVC. Also note that, CVC would need appropriate network route and gateway configurations to ensure network connectivity to the sensor network on IE switches.

This ensures network connectivity between CVC (For example, 10.10. 100.x subnet in CCI shared services network) and IE switches (172.16.10.x collection network for sensors).

Configuring the Sensor on IE3400/IE3300 10G Switches

The following configurations must be done on the switch before installing a CV sensor in it:

- SSH
- IOx and storage formatting
- Data export using Encapsulated Remote Switched Port Analyzer (ERSPAN)
- Port configuration

Use the following IP address schema to bring up the CVS application on IE3400/IE3300 10G and integrate it to the CVC.

CVC

Admin Interface (eth0): 10.104.206.225

Collection interface (eth1): 10.10.100.33

Collection network gateway: 10.10.100.1

NTP: 10.10.100.1

IE3300 10G Switch

Admin IP address: 192.100.2.39

Subnet mask: 255.255.255.0

Management port: 443

Admin username: admin

Admin password: sentryo69!

CVS

Capture IP address: 169.254.1.2

Capture subnet mask: 30

Capture VLAN number: 2508

Collection IP address: 172.16.10.249

Collection subnet mask: 24

Collection gateway: 172.16.10.1

Collection VLAN number: 1025

A prerequisite is the sensor application installation on the IE3400/IE3300 10G is to configure the switch for access to the CLI (ssh or console port).

Configuration prerequisites needed on IE3400/IE3300 10G before installing the Sensor:

- configure access to ssh
- configure basic parameters

The steps below show the necessary configuration needed on IE3300 10G or IE3400 switches for the sensor installation to then register it with the CVC.

```
Format sdflash and enable IOx on the IE switch
format sdflash: ext4
!
#show sdflash: filesys
Filesystem: sdflash
Filesystem Path: /flash11
Filesystem Type: ext4
Mounted: Read/Write
!
configure terminal

iox
end
!
#show iox

#sh iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
```

```
IOx service (HA)                : Not Supported
IOx service (IOxman)            : Running
IOx service (Sec storage)       : Running
Libvirtd 5.5.0                  : Running
Dockerd 18.03.0                 : Running
```

6. Configure SVI in the Collection network VLAN for enabling sensor communication to CVC.

```
interface Vlan1025 //VLAN 1025 is a Collection subnet VLAN
 ip address 172.16.10.252 255.255.255.0
end
```

7. To receive traffic inside an IOx application, you should make ensure that sure the AppGigabitEthernet port for communications can reach the IOx virtual application using the following commands.

   – Configure a VLAN for traffic mirroring:

```
configure terminal
vtp mode off
vlan 2508
remote-span
end
!
interface AppGigabitEthernet 1/1
 switchport mode trunk
exit
```

8. Configure the SPAN session and add to the session the interfaces to monitor:

```
monitor session 1 source interface Gi1/3 - 5 , Gi1/7 - 10
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
```

   Note: The source of the monitor session in this configuration, is a range of access ports for endpoints to be monitored.

9. **Save** the configuration.

```
wr mem
```

Refer to the sensor installation “Initial Configuration” steps in the following Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf

After the switch has all necessary configurations, the sensor can be deployed using the Cyber Vision Center extension. First, install the extension by completing the steps below:

1. Download the extension (.ext file) from cisco.com.
2. In Cyber Vision Center, navigate to **Admin > Extensions**.
3. Click the **Import Extension File** button and then browse to the extension file.

After the extension has been installed, install a sensor by completing the steps below:

1. In Cyber Vision Center, navigate to **Admin > Sensors > Sensors**.
2. Click the **Deploy Cisco Device** button:

a. In the IP address field, enter the IP address of the switch.

b. In the Port field, enter 443 for a network sensor.

c. In the User field, enter the user name to log in to the switch.

d. In the Password field, enter the password associated with the user account on the switch.

e. In the Center IP field, you may enter the IP address of the Center that the sensors will use for communication. For dual interface Center deployments, it is recommended to entering the eth1 IP address is recommended.

f. Under Capture mode, you may choose from the various options to change what data the sensor will process. In this validation, the Optimal (default) option was selected.

g. Click **Deploy**.

h. More configuration fields display. In the **Capture IP** address field, enter the ERSPAN destination IP address for the sensor.

i. In the Capture prefix length field, enter the prefix associated with the ERSPAN IP address.

j. In the Capture VLAN number field, enter the monitoring session destination VLAN

k. In the Collection IP address field, enter the IP address of the eth0 interface of the sensor. This is the IP address that will be used for communication with the Center.

l. In the Collection prefix length field, enter the prefix associated with the sensor IP address.

m. In the Collection gateway field, enter the IP address of the gateway that the sensor will use for communicating through the network.

n. In the Collection VLAN number, enter the VLAN of the sensor IP address.

o. Under Application type, click the radio button of the type of sensor you wish to deploy. For the Passive and Active Discovery option, additional information is required:

– In the IP address field, enter an IP address for the sensor to use in Active Discovery. Note that this IP address needs to be from the same subnet as the end devices you wish to discover. If active discovery is necessary on the same subnet as the sensor itself, you can click the USE COLLECTION button.

– In the Prefix length field, enter the prefix associated with the IP address.

– In the VLAN field, enter the VLAN for the subnet.

– (Optional) Click the ADD ONE button to configure another Active Discovery interface. This secondary interface should be configured for doing active discovery on a different subnet than what was specified for the first interface.

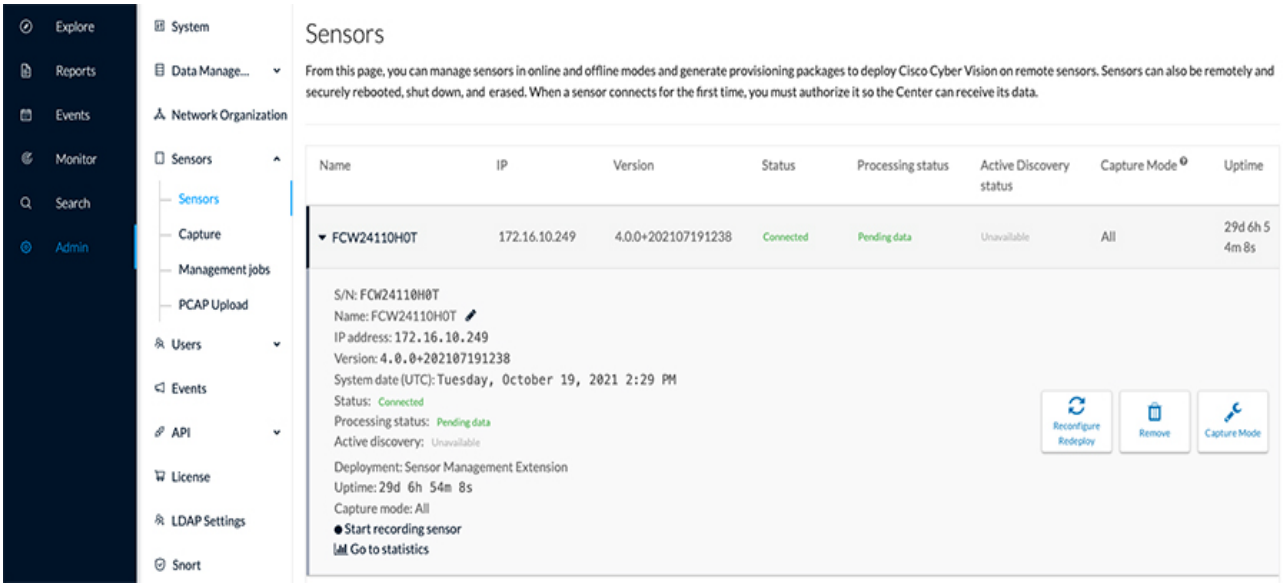
3. Click **Deploy**.

Refer to the “Procedure with the Cyber Vision sensor management extension” section for the detailed step-by-step instructions of CV sensor installation on IE3400 and IE3300 10G Series switches, in the following guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300_4_0_0.pdf

The figure below shows the sensor status on the Cyber Vision Center dashboard after it has successfully installed on an IE switch. Navigate to **Admin -> Sensors** on the CVC dashboard.

Figure 318 IE switch CV Sensor Status on CVC Dashboard



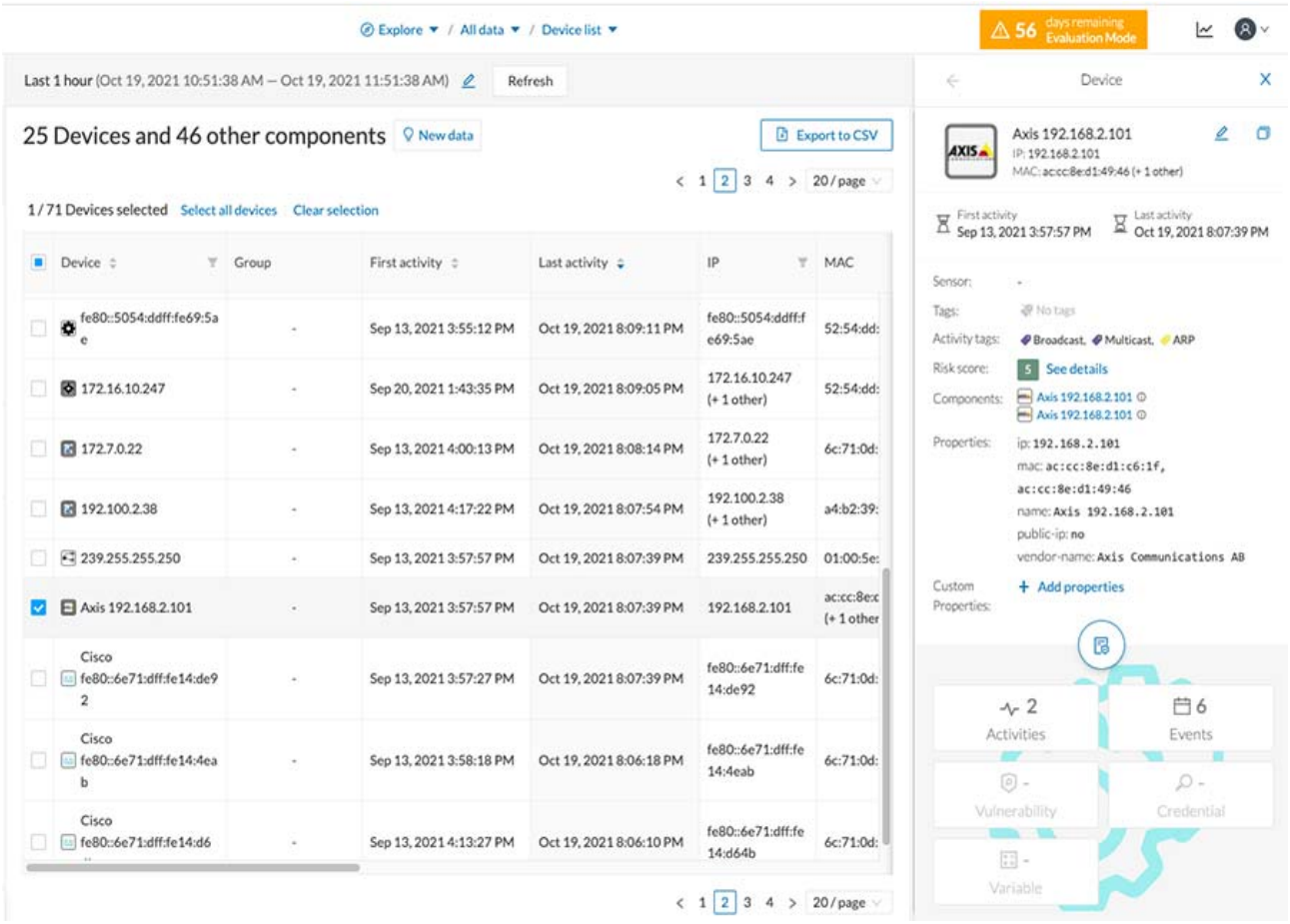
Cyber Vision OT Device Detection Example

After the sensor is running on the IE switch, you can view the data collected from the sensor on the CVC dashboard. For example, a CCTV Axis Camera device connected to the IE switch can be detected by Cyber Vision by monitoring the camera port traffic on the IE switch by the CV sensor.

The figure below shows an Axis Camera device in CVC dashboard. To see sensor data, complete the steps below:

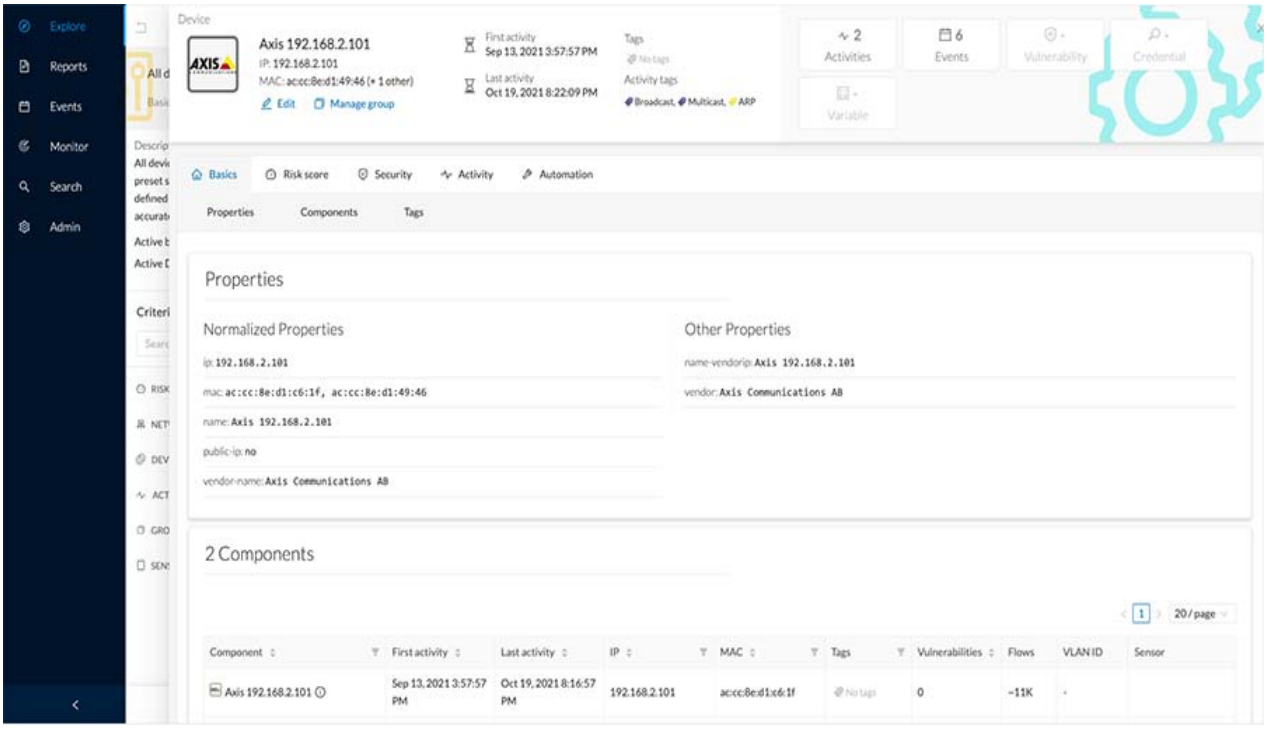
1. On CVC dashboard, navigate to **Explore -> All data**.
2. Click on **Devices**.
3. Select the device in the list to get more details on the device, as shown in the figure below.

Figure 319 CVC Dashboard Device View



4. Click on the Device and Basics tab to see more details on the device, as shown in the figure below.

Figure 320 CVC Dashboard Device Basics



Activities – These are the communication flows between components. From the **Activities** button on the Preset Dashboard, you can view these communications based on the time reference selected.

Similarly, traffic flows detected by CV sensor are displayed in CVC dashboard by navigating to **Explore -> All data -> Activity** list.

Refer to the following URL for MODBUS and DNP3 OT assets visibility.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/IG/DA-GS-IG/DA-GS-IG.html#pgfId-482904

Configuring Sensor on RPoP IR1101

This section focuses on the components listed below discussing the interactions between the Cisco Cyber Vision Sensor application hosted on the IR1101 and the Cisco Cyber Vision Center used for managing the sensor application to provide OT traffic visibility in CCI RPoP.

■RPoP Cisco IR1101 Integrated Services Router Rugged

■Cisco Cyber Vision Sensor (CVS) application

■Cisco Cyber Vision Center (CVC)

Cisco Cyber Vision Sensor application can be hosted as an Edge compute in IOX. Regular IOS perform the operation of routing the SCADA traffic. Sensor applications installed on IOX are passive sensors. The sensor application hosted on the IR1101 needs two interfaces, one to connect the sensor to the collection network interface of the Cyber Vision Center and one to monitor the traffic on local IOS interfaces.

Cisco IR1101 IOx uses VirtualPortGroup as means to communicate between IOS and the IOx application. A logical mapping of VirtualPortGroup and the IOx Application is shown in the CCI2.1 General Design Guide. Refer to the following URL for more details of the Cyber Vison sensor design on CCI RPoP.

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html

This guide proposes using the Encapsulated Remote Switched Port Analyzer (ERSPAN) to monitor traffic on one or more routed ports or routed Switch Virtual Interfaces (SVI).

The ERSPAN source sessions copy traffic from the source routed ports or SVIs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session, which is the Cisco Cyber Vision Sensor application in this solution. Similarly, the application uses a separate interface to send the processed traffic to the collection network interface.

To enable reachability of the collection network interface of the Center for the sensor, it is recommended to enable NAT on the VirtualPortGroup and overload using the IR1101 WAN facing interface. This section describes how to perform a clean installation of the sensor application (CVS) on the Cisco IR1101. As a prerequisite it is recommended to have the Cisco Cyber Vision Center installed and running.

The following IP address schema has been used in this guide to bring up the CVS application on IR1101 and integrate it to the CVC as highlighted in the above figure above.

CVC

- Admin Interface (eth0): 10.104.206.225
- Collection interface (eth1): 10.10.100.33
- Collection network gateway: 10.10.100.1
- NTP: 10.10.100.1

IR1101

- Management IP address: 192.168.100.80
- Subnet mask: 255.255.255.0
- Management port: 443
- Admin username: admin
- Admin password: sentryo69!

CVS

- Capture IP address: 169.254.1.1
- Capture subnet mask: 30
- Collection IP address: 192.168.9.2
- Collection subnet mask: 30
- Collection gateway: 192.168.9.1

For the sensor application install on the IR1101, the prerequisite is to first configure the router for access to the CLI (ssh or console port).

Below are the configuration prerequisites needed on IR1101 before installing the Sensor:

■Configure access to ssh on a CCI RPoP router

■Configure basic parameters.

To bring up the IR1101 with sensor application (CVS) and have it registered with the CVC with the IP address schema mentioned earlier, follow steps 8.1 to 8.3 in Section 8 “Procedure with the Cyber Vision Sensor Management Extension” in the Cisco Cyber Vision IR1101 installation guide here:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IR1101_4_0_0.pdf

The steps below show the necessary configuration needed on the IR1101 for the deployed sensor application to register with the CVC.

1. Setup ERSPAN (Encapsulated Remote Switched Port ANalyzer). To receive traffic inside an IOx application, you should make sure the app is connected to a VirtualPortGroup, and has the correct IP address by issuing the following commands.

```
interface VirtualPortGroup0
 description App ERSPAN
 ip address 169.254.1.1 255.255.255.252
end
```

Create the monitor session:

```
monitor session 1 type erspan-source
 source interface Tu10
 destination
  erspan-id 1
  mtu 1464
  ip address 169.254.1.2
  origin ip address 169.254.1.1
```

2. Setup NAT

   Add NAT rules so that the container can ping the outside. This will be on a different virtual port group than the ERSPAN to separate the traffic.

On the Cellular interface:

```
interface Cellular0/1/0 :
 mtu 1430
 ip address negotiated
 ip nat outside
 ip tcp adjust-mss 1313
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
end
```

On the Tunnel/Loopback interface:

```
 interface Tunnel10
 ip unnumbered Loopback10
 ip mtu 1400
 ip nat outside
 ip tcp adjust-mss 1283
 tunnel source Cellular0/1/0
 tunnel destination <Tunnel_Destination_Public_IP>
 tunnel protection ipsec profile default_No_cert
end
```

```
interface Loopback10
 ip address 192.168.100.80 255.255.255.255
 ip nat outside
end
```

On VirtualPortGroup1,

```
interface VirtualPortGroup1
 ip address 192.168.9.1 255.255.255.252
 ip nat inside
 ip tcp adjust-mss 1330
end
```

Configure the Access list for the VirtualPortGroup1 to reach outside the container via tunnel interface.:

```
ip access-list standard NAT_ACL
 10 permit 192.168.9.0 0.0.0.3
ip nat inside source list NAT_ACL interface Loopback10 overload
```

3. Save the configuration.

```
Exit
write mem
```

After a few minutes the sensor displays as connected in Cisco Cyber vision after following any one of three ways to install the sensor on Cisco IR1101 as described in the “Cisco Cybervision IR1101 Installation Guide”.

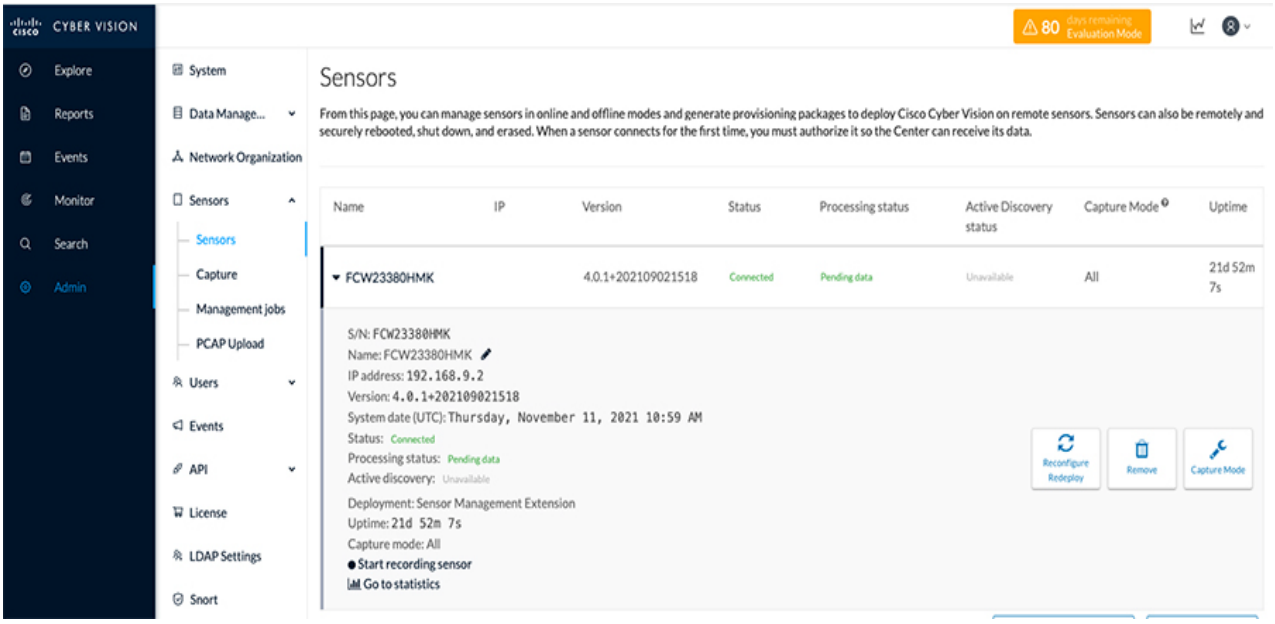
After the prerequisites are met (section 6 and section 8.1 to 8.3), there are three ways to install the Cyber Vision Sensor on IR1101:

- Via Local Manager – Follow Section 7.1 to 7.5 in above guide
- Via CLI – Follow section 9.1 to 9.3
- Via Cisco Cyber Vision Center Extension – Follow section 8.1 to 8.3

Note: When the IR1101 IoX sensor is deployed via Cyber Vision Extension Feature, make sure to configure “ip tcp adjust-mss 1330” on VirtualPortGroup1 of IR1101 and Virtual-template interface on Head End Router (in DMZ) where IR1101 Tunnel interface is connected.

After the sensor is installed and connected to CVC successfully, you see the Sensor status on CVC, as shown in the figure below.

Figure 321 IR1101 CV Sensor Status on Cyber Vision Center



Implementing CCI Network Quality of Service

This chapter provides the detailed implementation of CCI network QoS for the CCI Solution CVD, Release 2.1QoS design considerations, as discussed in the Cisco CCI General Solution Design Guide. Implementing QoS in CCI network ensures efficient use of CCI network resources and provide preferential of differential treatment to business critical and other classes of traffic in the network.

This chapter includes the following major topics:

Configuring QoS on Fabric and Backhaul Network Devices Using SD-Access

Cisco DNA Center SD-Access provides the Application Policy feature, which includes various classes of predefined applications, application sets, and traffic queuing profile. This Application Policy feature is leveraged to implement the QoS on CCI network devices like FiaB in PoP sites and other non-fabric/intermediate and backhaul network devices in the CCI network to deploy end-to-end QoS policy.

This section covers QoS deployment on fabric/non-fabric devices (excluding extended in the access ring), with an example configuration of QoS application policies using Cisco DNA Center. For detailed step-by-step instructions for configuring QoS application policies, refer to the section “Application Policies” under the chapter “Configure Policies” in the *Cisco Digital Network Architecture Center User Guide, Release 2.2.3* at the following URL:

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01100.html#id_51875

Note: QoS Application Polices configured using Cisco DNA Center for non-fabric devices is applicable only for Cisco DNA Center-supported switches/routers hardware models. This is because the QoS features support and/or hardware queuing differs from device to device.

1. Creating a Queuing Profile:

   A Queuing profile, as per the QoS design consideration for different classes of traffic, must be created in Cisco DNA Center to allocate the percent of network interface bandwidth. The bandwidth percentage values are chosen based on design guidelines available at the link below in the section “CCI Network QoS Design”:

   – https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg.html

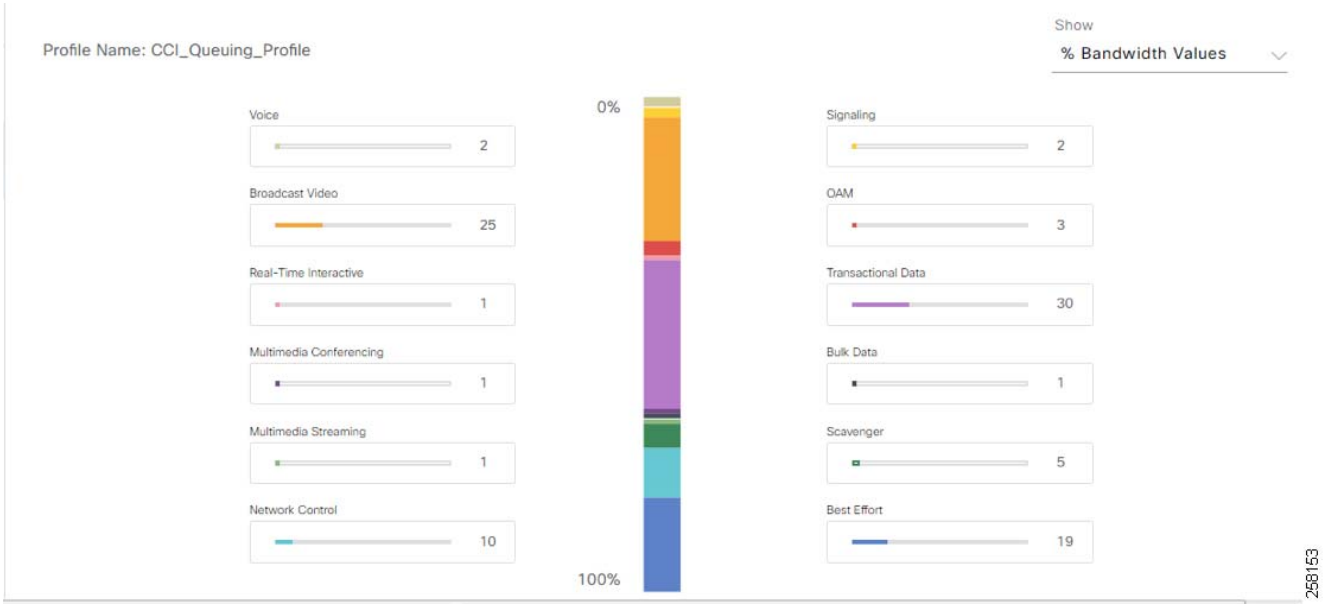
   a. On Cisco DNA Center GUI, navigate to **Policy -> Application QoS -> Queuing Profiles**.

   b. Click **+Add Profile** to add a new Queuing Profile (example: CCI_Queuing_Profile).

   c. Allocate the **Bandwidth percentage** for all applications and save the profile.

Figure 322 shows an example queuing profile created for the CCI network in Cisco DNA Center.

Figure 322 Cisco DNA Center Application Policy Queuing Profile Example



2. Creating a QoS Application Policy:

   An application policy must be created and attached to the queuing profile and sites to deploy the policy in network device in each PoP site and intermediate and/or backhaul network devices (i.e., non-fabric network devices) in the CCI network.

   a. Navigate to **Policy -> Application QoS -> Application Policies**.

   b. Click **+ Add Policy** and name the policy (example: CCI_QoS_Policy).

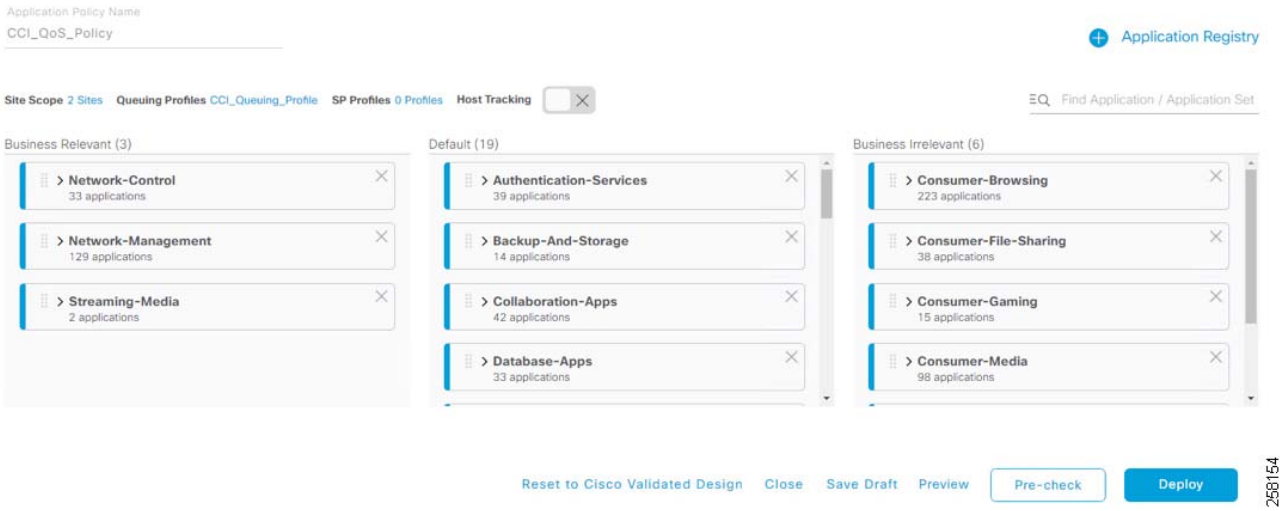
   c. Select the **Queuing profile** and add the Queuing profile created in the previous step (example: CCI_Queuing_Profile), as shown in Figure 323.

   d. Select the **Sites** to which the policy has to be applied.

   e. While adding Sites, select **Site settings**, exclude the devices which are not needed, and then click **Save**.

   f. Then associate the application sets to **Business Relevant**, **Default**, and **Business Irrelevant**, as shown in Figure 323.

Figure 323 Cisco DNA Center Application Policy Creation for QoS Deployment



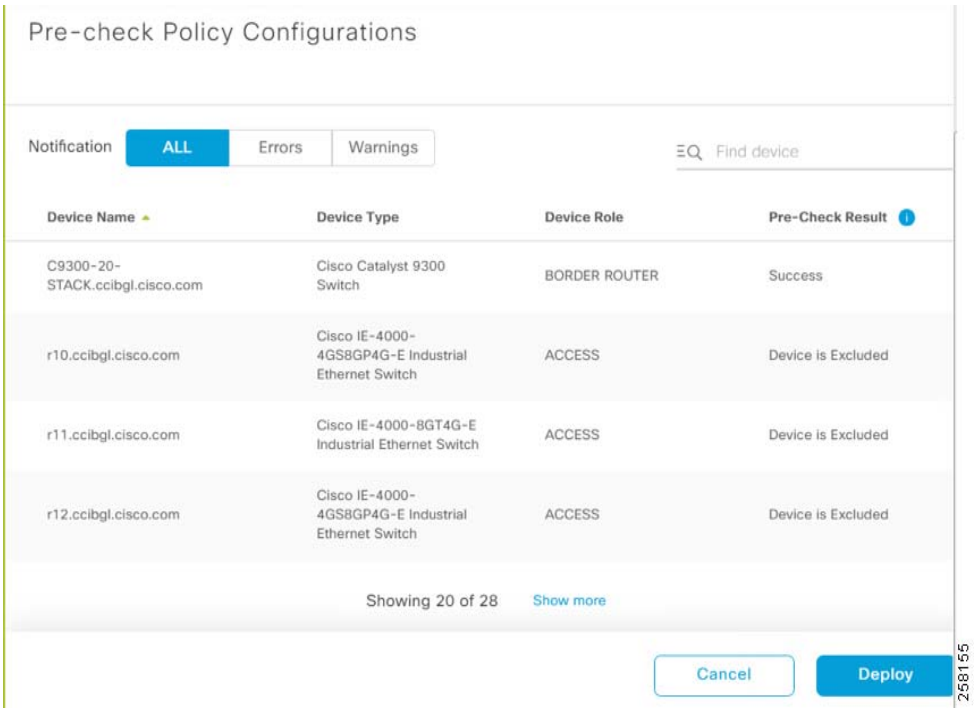
3. Pre-check and deploy the QoS policy:

   Before deploying the QoS configuration on network devices, you should preview the QoS configuration to be applied on the device using the **Preview** option:

   a. Preview the configuration changes on the devices before deployment by selecting the **Preview** option and generating the configuration to view the changes.

   b. Then, click **Pre-check** to make sure there are no errors and warnings before deployment, as shown in Figure 324.

Figure 324 Cisco DNA Center QoS Policy Pre-Check



c. If the Pre-check is successful, click **Deploy** to apply the policy to all the devices included in deployment.

An example QoS configuration that will be deployed on the devices for the **Queuing Profile and Application Policy** is as follows:

```
C9300-20-STACK#show run class-map      #Class-map applied from QoS Policy
class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA
 match dscp cs1
 match dscp af12
 match dscp af13
 match dscp af11
class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
 match dscp cs3
 match dscp cs2
 match dscp cs7
 match dscp cs6
class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
 match dscp af43
 match dscp af41
 match dscp af42
class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
 match dscp cs5
 match dscp cs4
class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
 match dscp ef
class-map match-any DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
 match dscp af23
 match dscp af21
 match dscp af22
class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
 match dscp af32
 match dscp af33
 match dscp af31
end

C9300-20-STACK#show run policy-map#Policy map applied from QoS Policy
```

```
policy-map DNA-dscp#APIC_QOS_Q_OUT
 class DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
  priority level 1
  police rate percent 2
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
  priority level 2
  police rate percent 26
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
  bandwidth remaining percent 21
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
  bandwidth remaining percent 1
  queue-buffers ratio 10
  queue-limit dscp af41 percent 100
  queue-limit dscp af42 percent 90
  queue-limit dscp af43 percent 80
 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
  bandwidth remaining percent 1
  queue-buffers ratio 10
  queue-limit dscp af32 percent 90
  queue-limit dscp af33 percent 80
 class DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
  bandwidth remaining percent 42
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 18 percent 80 100
  random-detect dscp 20 percent 70 100
  random-detect dscp 22 percent 60 100
 class DNA-EZQOS_2P6Q3T_9K#BULK-DATA
  bandwidth remaining percent 8
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 60 100
  random-detect dscp 10 percent 80 100
  random-detect dscp 12 percent 70 100
  random-detect dscp 14 percent 60 100
 class class-default
  bandwidth remaining percent 27
  queue-buffers ratio 25
  random-detect dscp-based
  random-detect dscp 0 percent 80 100
end
```

Then the policy is attached to all the selected interfaces on the device as shown below:

```
interface TenGigabitEthernet 1/1/1
  service-policy output DNA-dscp#APIC_QOS_Q_OUT
```

Note: This example shows an egress service policy (egress traffic) created as a unidirectional QoS policy based on the FiaB device role in Cisco DNA Center.

This completes the QoS deployment on all fabric and non-fabric devices in the CCI network.

Configuring QoS on Ethernet Access Ring

QoS configuration, as per the design, is to be configured manually and using Application QoS in Cisco DNA Center on the Ethernet access ring consisting of IE switches (extended and policy extended nodes non-extended nodes) in each PoP site. However, the QoS configurations on legacy IE switches (IE4000/IE5000/IE3300) discussed in this section can also be automated and provisioned on all IE switches leveraging the Cisco DNA Center Configuration Templates feature.

Configuring QoS on IE4000/IE5000 Series Switches

This section covers the high-level steps to configure QoS with an example configuration on IE4000/IE5000 switches in the access ring of a PoP site.

Refer to the chapter " Configuring Quality of Service (QoS)" in the *Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide*, for detailed step-by-step instructions on QoS configuration.

Complete the following steps to configure QoS on IE4000/IE5000 Series switches in the access ring:

1. Create Access Lists to match Incoming Traffic

   Create an access list to match incoming Operational Technology (OT) traffic and Quarantine traffic in CCI network in global configuration mode. In this example configuration, 172.20.x.x and 172.99.x.x are used as the source network, which identifies OT and Quarantine traffic, respectively.

```
access-list 101 permit ip 172.10.0.0 0.0.255.255 any
access-list 102 permit ip 172.20.0.0 0.0.255.255 any
```

2. Create Class-map to Classify Traffic

   QoS policy class-maps must be created on IE switches to classify and mark the incoming traffic for preferential QoS treatment. The following configuration shows different class-map created to match incoming traffic based on access list (video and OT traffic) and DSCP values for other classes of traffic like network control, signaling, management, voice, and scavenger in the network:

```
class-map match-any VOICE_VIDEO_PQ_OUT1
 match ip dscp cs5
Match ip dscp cs4
Match ip dscp ef
Class-map match-any NW_CONTROL
Match ip dscp cs6 cs7
Class-map match-any SIGNALING
Match ip dscp cs3
Class-map match-any MM_CONF_STREAM_OAM_OT
Match ip dscp af41 af42 af43 af31 af32 af33 cs2 af21 af22 af23
class-map match-any SCAVENGER_QUARANTINE
 match ip dscp cs1

Class-map match-any BULK_DATA
 match ip dscp af11  af12  af13
Class-map match-any SCAVENGER_BULK_DATA_TRAFFIC1
match ip dscp cs1
 match ip dscp af11  af12  af13
class-map match-any NW_CONTROL_SIG_OAM_OUT1
 match ip dscp cs2
 match ip dscp cs3
 match ip dscp cs6
match ip dscp cs7
 match ip dscp af41  af42  af43
Match ip dscp af21 af22 af23
Match ip af31 af32 af33

Class-map QUARANTINE_TRAFFIC
  Match access-group 103

class-map match-any CCI_OT_TRAFFIC
 match access-group 102
```

3. Create a policy-maps for the input and output service policies to perform policy actions like priority queuing and policing of the traffic as per the QoS design. Following are the example policy-map configurations applied on IE4000 and IE5000 series switches in the access ring:

```
policy-map CCI_IE_QoS_Output_Policy    #QoS Output Policy
 class VOICE_VIDEO_PQ_OUT
  priority
  police cir 300000000
 class NW_CONTROL_SIG_OAM_OUT
  bandwidth percent 15
  queue-limit 272 packets
  queue-limit dscp cs3 128 packets
  queue-limit dscp cs2 48 packets
 class CCI_OT_TRAFFIC_OUT
  bandwidth percent 30
 class class-default
  bandwidth percent 25

policy-map CCI_IE_QoS_Input_Policy  #QoS Input Policy
 class VIDEO-PQ
  set qos-group 1
  set ip dscp cs5
 class VOICE-PQ
  set qos-group 1
  set ip dscp ef
 class NW_CONTROL_SIG_OAM_TRAFFIC
  set qos-group 2
 class CCI_OT_TRAFFIC
  set qos-group 3
  set ip dscp af21
!
```

4. Associate the Input and Output QoS service policies on all IE switch ports. Example on an IE switch port (GigabitEthernet1/1) in the following configuration is added:

```
interface GigabitEthernet 1/1
 service-policy input CCI_IE_QoS_Input_Policy
 service-policy output CCI_IE_QoS_Output_Policy
```

5. Repeat the above steps for all the IE4000 and IE5000 series switches in the PoP site access ring.

Alternatively, the above QoS configuration can be automated to configure on all IE switches in the ring using the Cisco DNA Center configuration template feature.

Configuring QoS on IE3300 Switches using DNAC Templates

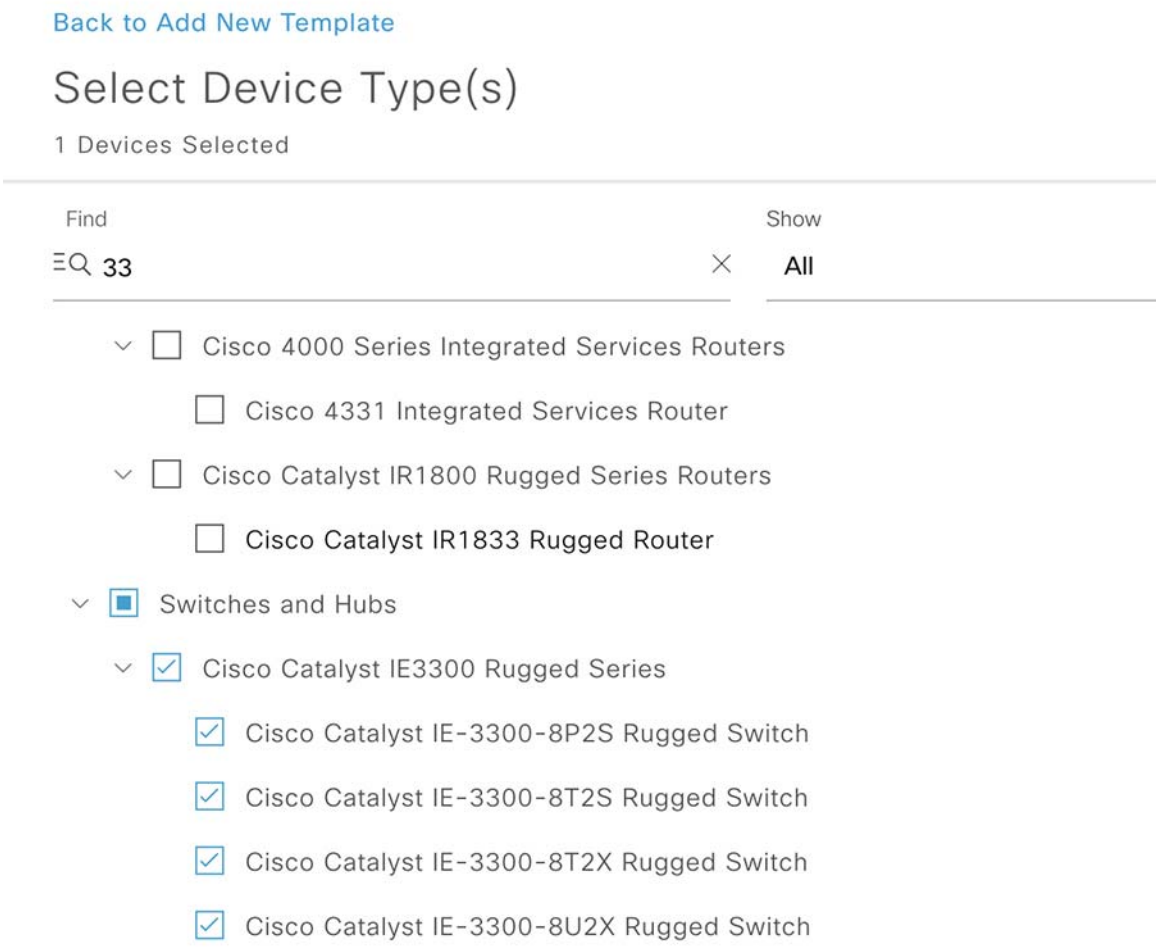
The Cisco DNA Center provides an interactive editor called Template Editor to author CLI templates. Templates can be easily designed with a predefined configuration by using parameterized elements or variables. After creating a template, the template can be used on the devices in one or more sites. For information on how to use templates refer to the **Create Templates to Automate Device Configuration Changes of Cisco DNA Center** section of the User Guide, Release 2.2.3 at https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01100.html#id_51875

To configure QoS on the IE3300 switches following complete the following steps:

1. Create a template by navigating to **Tools->Template Editor**.
2. Create a project, then create the template by clicking on the **+** symbol and selecting the corresponding option.
3. Select template type as **regular** and language as **Velocity**.
4. Enter the name of the template and select the project you created in step 2 from the drop-down menu.

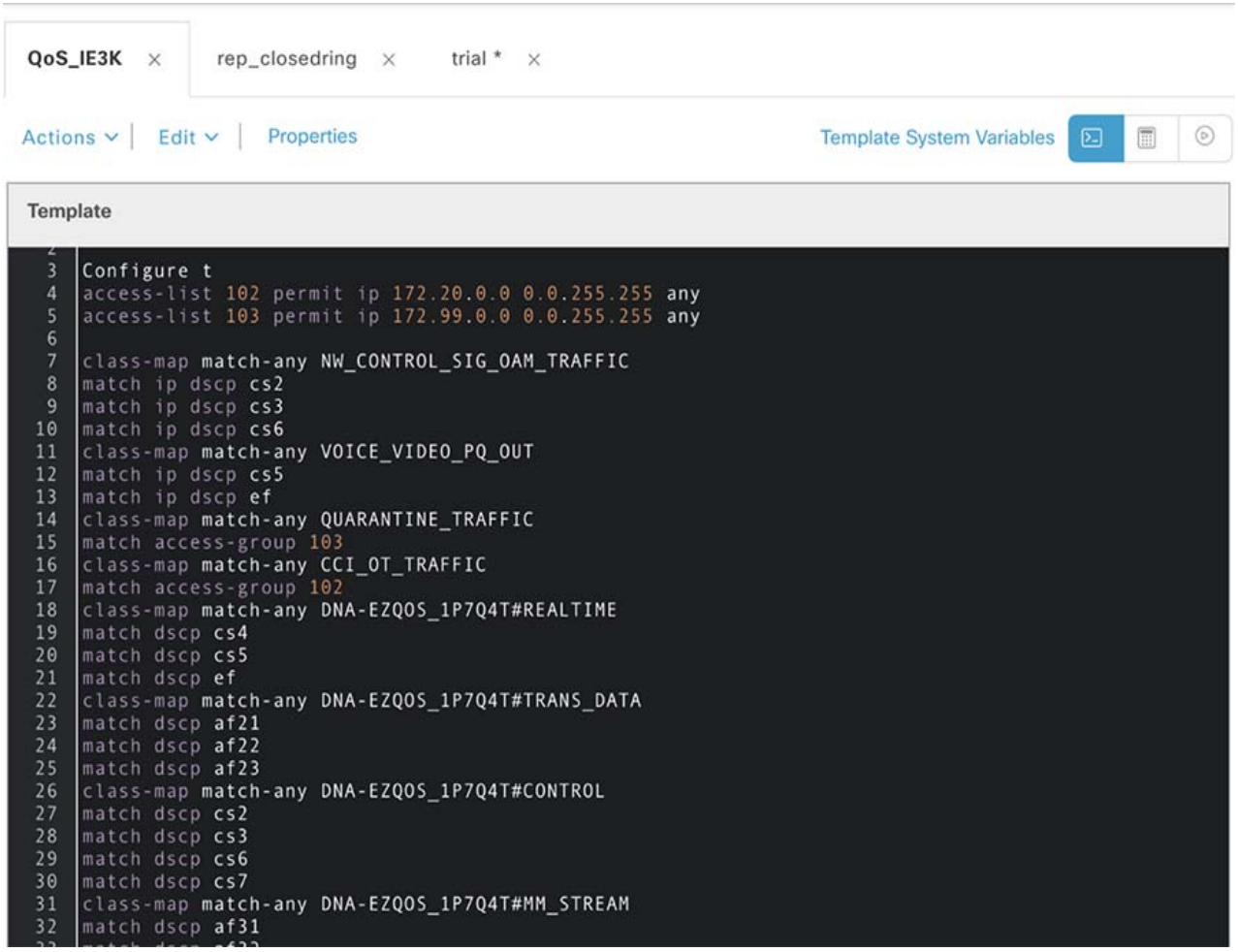
5. Select the device type IE3300 from the list of drop downs as shown in the figure below.

Figure 325 Adding a Template for QoS configuration



6. Select the software type.
7. Click **Add**.
8. In the template window enter the set of QoS configs for IE3300 as shown in figure below

Figure 326 Configuring QoS using DNAC Templates



The following is a sample config for the template :

```
Configure t
access-list 102 permit ip 172.20.0.0 0.0.255.255 any
access-list 103 permit ip 172.99.0.0 0.0.255.255 any

class-map match-any NW_CONTROL_SIG_OAM_TRAFFIC
match ip dscp cs2
match ip dscp cs3
match ip dscp cs6
class-map match-any VOICE_VIDEO_PQ_OUT
match ip dscp cs5
match ip dscp ef
class-map match-any QUARANTINE_TRAFFIC
match access-group 103
class-map match-any CCI_OT_TRAFFIC
match access-group 102
class-map match-any DNA-EZQOS_1P7Q4T#REALTIME
match dscp cs4
match dscp cs5
match dscp ef
class-map match-any DNA-EZQOS_1P7Q4T#TRANS_DATA
match dscp af21
```

```
match dscp af22
match dscp af23
class-map match-any DNA-EZQOS_1P7Q4T#CONTROL
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map match-any DNA-EZQOS_1P7Q4T#MM_STREAM
match dscp af31
match dscp af32
match dscp af33
class-map match-any DNA-EZQOS_1P7Q4T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map match-any DNA-EZQOS_1P7Q4T#SCAVENGER
match dscp cs1
class-map match-any DNA-EZQOS_1P7Q4T#MM_CONF
match dscp af41
match dscp af42
match dscp af43
class-map match-any VOICE-PQ
match ip dscp ef
class-map match-any VIDEO-PQ
match ip dscp cs5
exit


policy-map CCI_IE_QoS_Output_Policy
class DNA-EZQOS_1P7Q4T#REALTIME
bandwidth percent 30
class DNA-EZQOS_1P7Q4T#CONTROL
bandwidth percent 10
queue-limit 272 packets
queue-limit dscp cs2 128 packets
queue-limit dscp cs3 128 packets
class DNA-EZQOS_1P7Q4T#MM_CONF
bandwidth percent 10
class DNA-EZQOS_1P7Q4T#MM_STREAM
bandwidth percent 1
class DNA-EZQOS_1P7Q4T#TRANS_DATA
bandwidth percent 30
class DNA-EZQOS_1P7Q4T#BULK_DATA
bandwidth percent 3
class DNA-EZQOS_1P7Q4T#SCAVENGER
bandwidth percent 1
class class-default
!
policy-map CCI_IE_QoS_Input_Policy
class VIDEO-PQ
set ip dscp cs5
class VOICE-PQ
set ip dscp ef
class NW_CONTROL_SIG_OAM_TRAFFIC
set ip dscp cs6
class CCI_OT_TRAFFIC
set ip dscp af21
class QUARANTINE_TRAFFIC
set ip dscp cs1
!
end


Configure t
interface range GigabitEthernet 1/1-10
```

```
service-policy input CCI_IE_QoS_Input_Policy
service-policy output CCI_IE_QoS_Output_Policy
```

9. Click **Save** and then click **Commit**.
10. Associate the created Template to a profile and associate the profile to the site where the device is added.
11. Provision the device by going to **Provision-> Inventory**->Device->Actions->Provision->Provision Device and then following the screen till **Deploy**.
12. After the Template is successfully deployed, verify that the above configs have been pushed on the device

```
SN-FOC2351V05A#show policy-map

   Policy Map CCI_IE_QoS_Output_Policy
    Class DNA-EZQOS_1P7Q4T#REALTIME
      bandwidth 30 (%)
    Class DNA-EZQOS_1P7Q4T#CONTROL
      bandwidth 10 (%)
      queue-limit 272 packets
      queue-limit dscp cs2 128 packets
      queue-limit dscp cs3 128 packets
    Class DNA-EZQOS_1P7Q4T#MM_CONF
      bandwidth 10 (%)
    Class DNA-EZQOS_1P7Q4T#MM_STREAM
      bandwidth 1 (%)
    Class DNA-EZQOS_1P7Q4T#TRANS_DATA
      bandwidth 30 (%)
    Class DNA-EZQOS_1P7Q4T#BULK_DATA
      bandwidth 3 (%)
    Class DNA-EZQOS_1P7Q4T#SCAVENGER
      bandwidth 1 (%)
    Class class-default

   Policy Map CCI_IE_QoS_Input_Policy
    Class VIDEO-PQ
      set ip dscp cs5
    Class VOICE-PQ
      set ip dscp ef
    Class NW_CONTROL_SIG_OAM_TRAFFIC
      set ip dscp cs6
    Class CCI_OT_TRAFFIC
      set ip dscp af21
    Class QUARANTINE_TRAFFIC
      set ip dscp cs1
```

-----some output has been omitted-----

This completes the provisioning of QoS on IE3300 using the templates.

Configuring QoS on IE3300/IE3400 Series Switches using Application QoS

QoS can be configured on the IE3400 and IE3300 using the Application QoS configured via DNAC.

For detailed information, refer to Application Policies section under chapter Configure Policies of Cisco DNA Center User Guide, Release 2.2.3 at*:*

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01100.html#id_51875

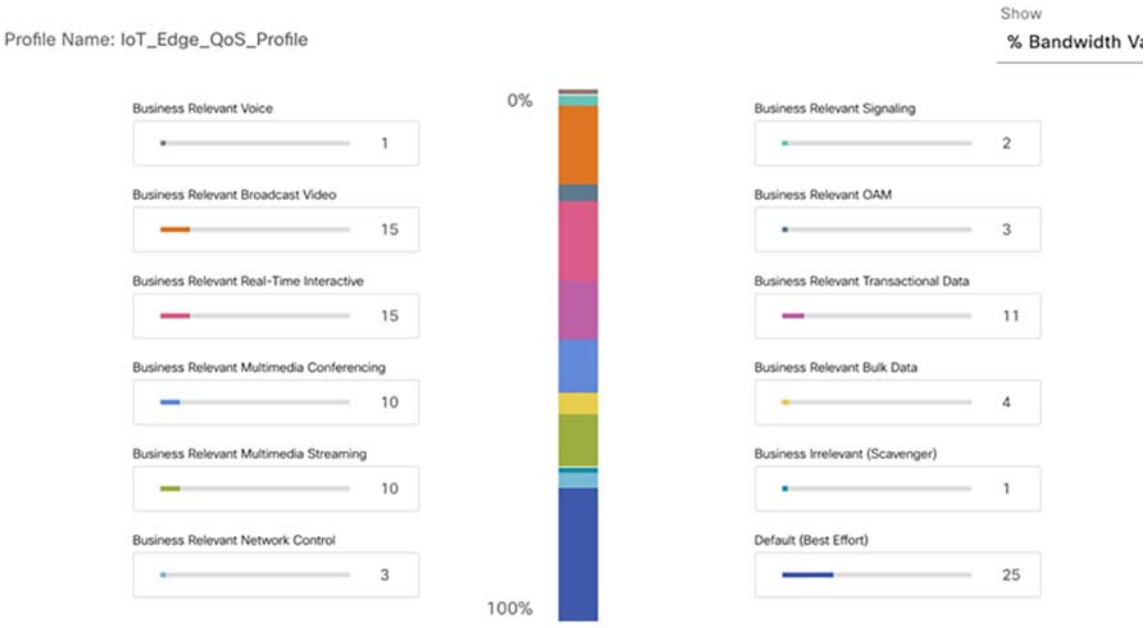
Following are the steps to configure QoS on the switches via Application QoS :

1. Create a Queuing profile as shown in figure below by first navigating to **Policy-> Application QoS->Queuing Profiles** as shown in the figure below.

   Following diagram values derived as per design guide at the following URL:

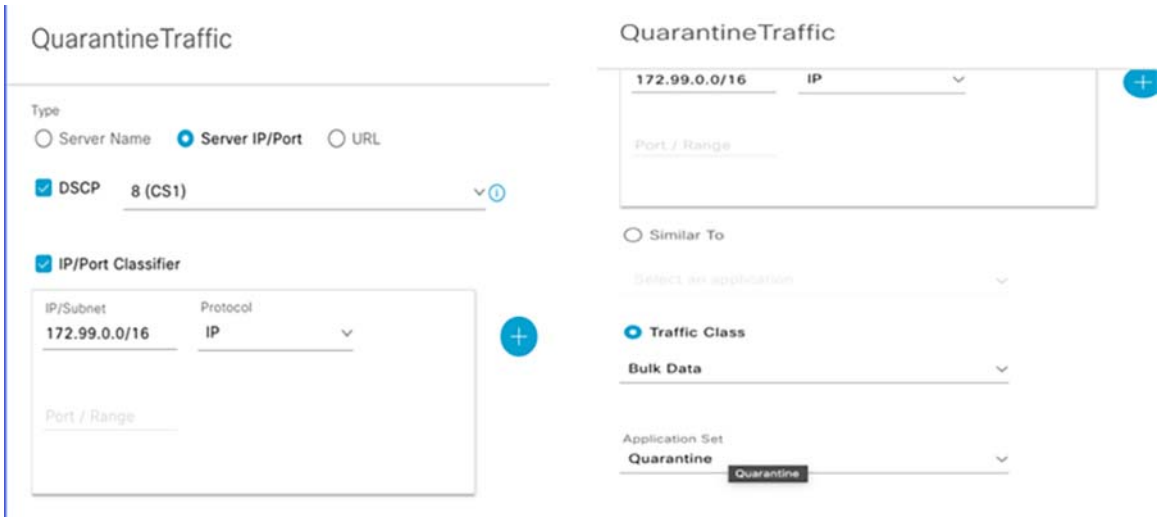
   https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/General/cci-dg/cci-dg.html#pgfId-457899

Figure 327 Queuing Profile for IE3300 and IE3400



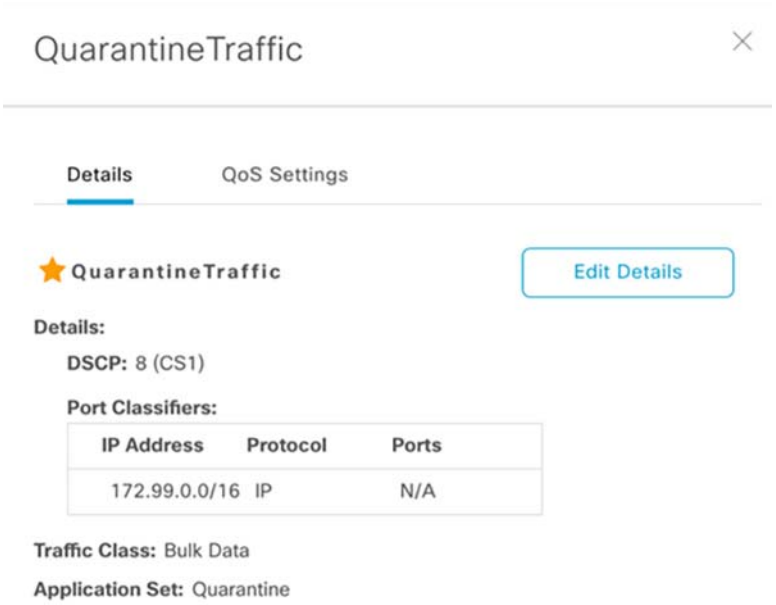
2. Under Application Policy click on **Add Policy** on the right.
3. Assign a name to the policy, select the site scope, and the above created Queuing profile created in step 1.
4. Under **Application Registry**, add the custom applications and application set.
5. To create the Application set click on **Add Application** set, assign a name and setting for the Default Business relevance as Business Relevant. Then click **Save**.
6. Add an Application as shown in figures below.

Figure 328 Creating custom Application



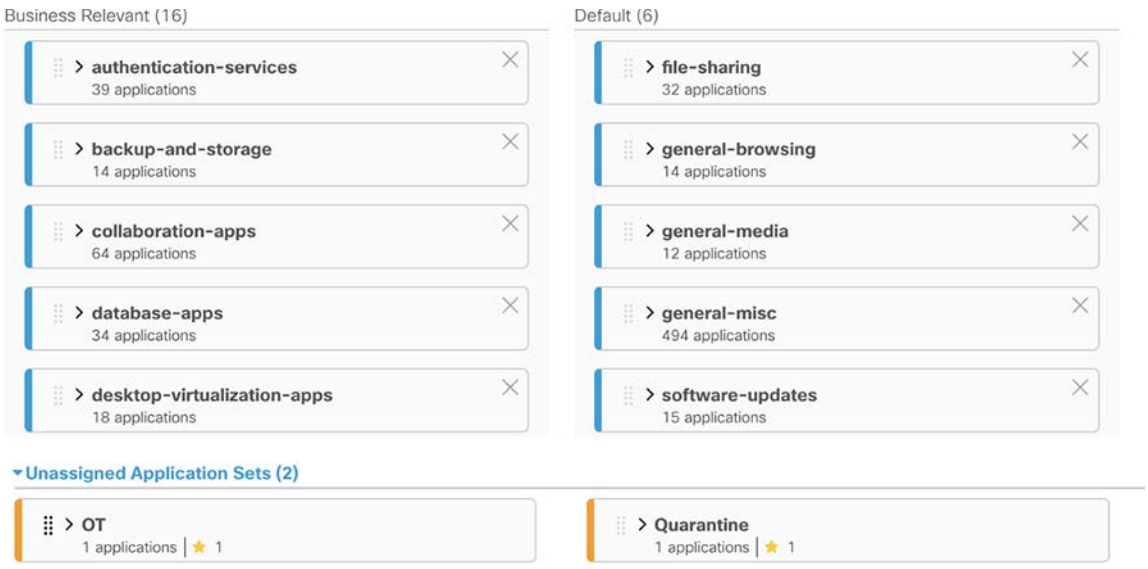
7. The new custom Application will appear as shown below:

Figure 329 Custom QoS Application



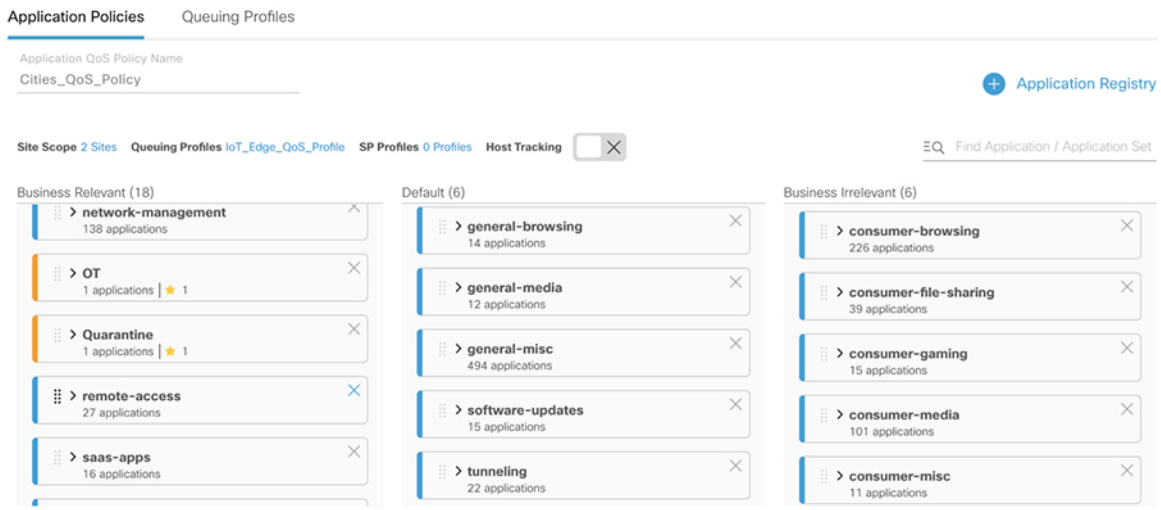
8. The custom application set will appear under **Unassigned** for the Application Policy as shown in the figure below:

Figure 330 Assigning the Custom Application set to Business Relevant



9. Drag and drop the Application sets to the Business Relevant group. The Application sets will nowthen appear as shown in the figure below:

Figure 331 Creating custom Application



10. Click **Deploy**.

11. Verify the policy created on the switch by issuing **show policy-map** and **sh run interface**.

```
SN-FCW2442P3TL # show run int gi 1/6
      Building configuration...

      Current configuration : 164 bytes
      !
      interface GigabitEthernet1/6
       device-tracking attach-policy IPDT_POLICY
       service-policy input DNA-APIC_QOS_IN
```

```
               service-policy output DNA-dscp#APIC_QOS_Q_OUT
end

SN-FCW2442P3TL#show policy-map

    Policy Map DNA-APIC_QOS_IN
    Class DNA-APIC_QOS_IN#REALTIME
      set dscp cs4
    Class DNA-APIC_QOS_IN#CONTROL
      set dscp cs6
    Class DNA-APIC_QOS_IN#MM_CONF
      set dscp af41
    Class DNA-APIC_QOS_IN#MM_STREAM
      set dscp af31
    Class DNA-APIC_QOS_IN#TRANS_DATA
      set dscp af21
    Class DNA-APIC_QOS_IN#BULK_DATA
      set dscp af11
    Class DNA-APIC_QOS_IN#SCAVENGER
      set dscp cs1
    Class class-default
      set dscp default
   Policy Map DNA-dscp#APIC_QOS_Q_OUT
    Class DNA-EZQOS_5P7Q4T#REALTIME
      priority 31 (%)
    Class DNA-EZQOS_5P7Q4T#MM_CONF
      bandwidth remaining 14 (%)
    Class DNA-EZQOS_5P7Q4T#MM_STREAM
      bandwidth remaining 14 (%)
    Class DNA-EZQOS_5P7Q4T#CONTROL
      bandwidth remaining 12 (%)
    Class DNA-EZQOS_5P7Q4T#TRANS_DATA
      bandwidth remaining 16 (%)
    Class DNA-EZQOS_5P7Q4T#BULK_DATA
      bandwidth remaining 6 (%)
    Class DNA-EZQOS_5P7Q4T#SCAVENGER
      bandwidth remaining 1 (%)
    Class class-default
      bandwidth remaining 37 (%)
```

-----some output has been omitted-----

This completes the QoS configuration on IE3300 & IE3400 using Application QoS.

Implementing CCI Network Multicast

Multicast is a useful technology that allows communication to a group of devices in an efficient manner. Whereas unicast is used in one-to-one communication and broadcast is one-to-all communication, multicast is one-to-many or many-to-many communication. This is well suited to video streaming or other streaming type services where many receivers subscribe to a server to receive the same stream. In a unicast only environment, the traffic would increase linearly with each new client receiving the stream until the slowest link is saturated. With broadcast, every client in a network would receive the stream and then have to discard it if not subscribed, creating a large amount of network traffic and system churn. In a multicast environment, the source sends the traffic stream once and only interested receivers subscribe to it. Intermediate routers and switches that perform multicast routing increase the efficiency by only replicating the traffic to those hosts that subscribe to a stream. In this scenario a source does not even have to know when there is a receiver or how many receivers there may be. With a unicast stream, the source would have to maintain a connection to each receiver which could quickly drain its resources with a large number of receivers.

In the context of SDA, multicast takes on another dimension because it can be supported in the underlay or the overlay. When multicast is configured on the underlay, this is known as native multicast from the Cisco DNA Center workflow. When configured in the overlay, it is known as head-end replication. Native multicast is beneficial when the source and receivers are co-located in a PoP site and the receivers are spread out over a number of fabric edge nodes. As the name suggests, head-end replication requires the head-end router, usually the border node, to create multiple unicast copies of the multicast traffic and send them to all the fabric edge nodes where receivers are located. With native multicast, the overlay multicast groups are mapped to an SSM group in the underlay and the underlay devices participate in the replication of the multicast traffic to the other fabric edge devices. The downside to the native multicast implementation is that manual configuration is required on all fabric devices. Also, if the source is outside the fabric, the efficiencies of native multicast may not be fully realized as the fabric border node becomes the head-end replication point. As mentioned in the Design Guide and for this implementation guide, only head-end replication is supported and tested.

Within the overlay network, two different multicast implementations are available, Any Source Multicast (ASM) and Source Specific Multicast (SSM). ASM relies on group addresses where a source publishes to a specific multicast address and then any number of receivers indicate they want to receive traffic from that group address. This request to a group address is seen in the multicast routing table as (*,G) where the * is any source and the G represents the group address. When a receiver starts receiving the traffic from that source, the network node creates an entry in the multicast routing table called (S,G) where the S represents the IP address of the source.

ASM relies on a routing protocol to manage the location of receiver membership requests. The protocol supported by Cisco DNA Center is Protocol Independent Multicast (PIM) and specifically, PIM Sparse mode. In this configuration, PIM Sparse mode creates a Shared Path Tree (SPT) that allows sources and receivers to locate each other. This requires designating one node as the Rendezvous Point (RP) which forms the root of the SPT. While the IOS feature set supports numerous dynamic methods of choosing an RP, the Cisco DNA Center workflow only supports a static RP configuration. Therefore, it is important to consider where the sources and receivers are when choosing the rendezvous point.

The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature.

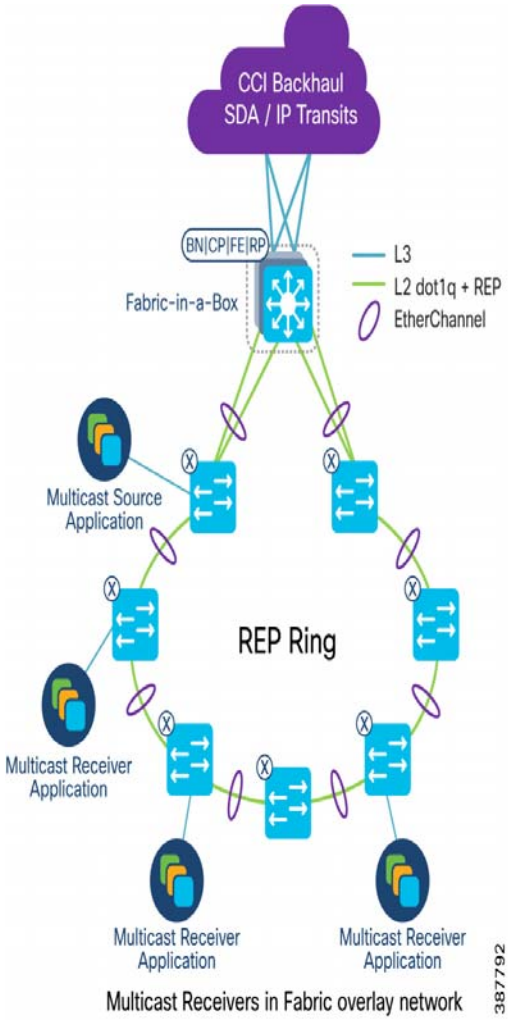
In the CCI network, two scenarios are supported, multicast within a PoP site and multicast between PoP sites. Because of how Cisco DNA Center configures the multicast deployment, it is not recommended to support both scenarios in the same VN overlay when using ASM. This is due to the placement of the RP and whether it is external or internal to the fabric site.

This chapter includes the following major topics:

Configuring SD Access Multicast within a PoP

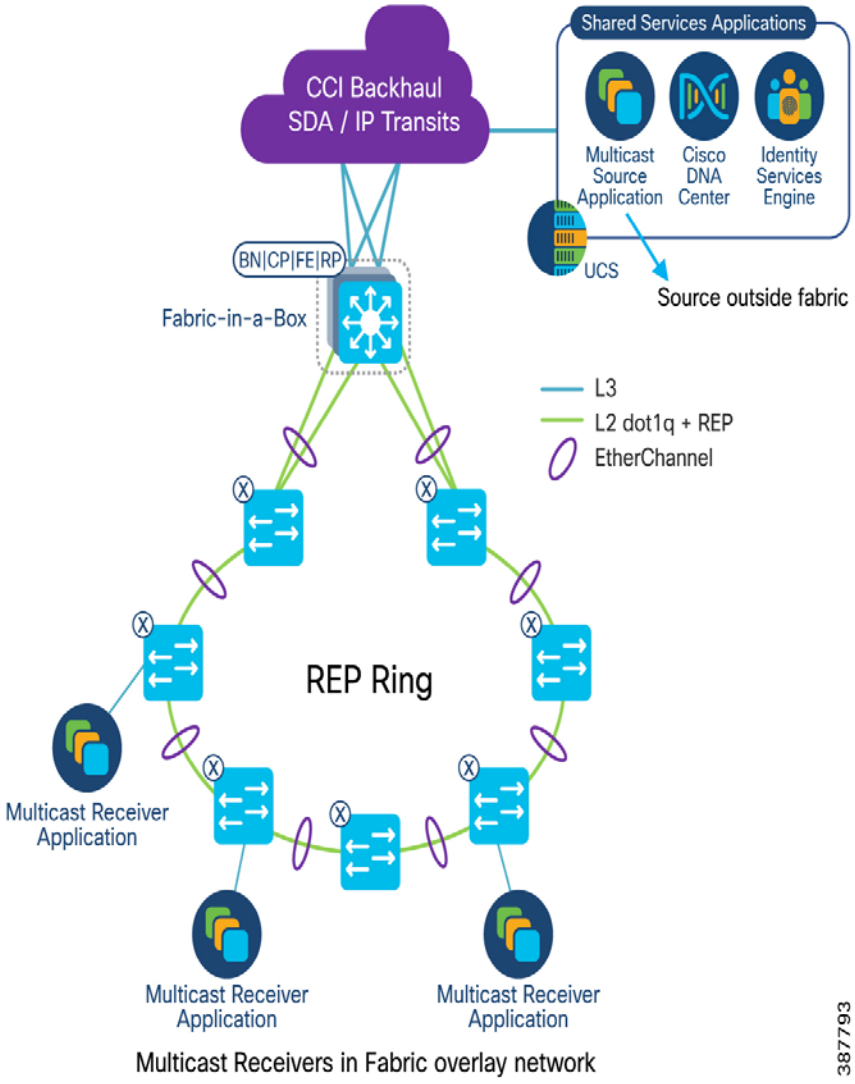
If a source and its receivers are primarily within a fabric PoP or if the source and receivers are not separated by an MPLS IP transit, the multicast configuration is very straight forward from the Cisco DNA Center workflow. An example topology showing the multicast source and receivers is below in Figure 332.

Figure 332 Multicast within a PoP Site–Source and Receiver within PoP



Below is an example showing the multicast source outside the fabric with the receivers in a single fabric.

Figure 333 Multicast within a PoP Site—Source Outside and Receivers Inside PoP



Cisco DNA Center must first be configured to enable multicast in every site where the receivers may be located. The workflow for this starts at the Fabric Site within the Fabric Provisioning section, as shown in Figure 334.

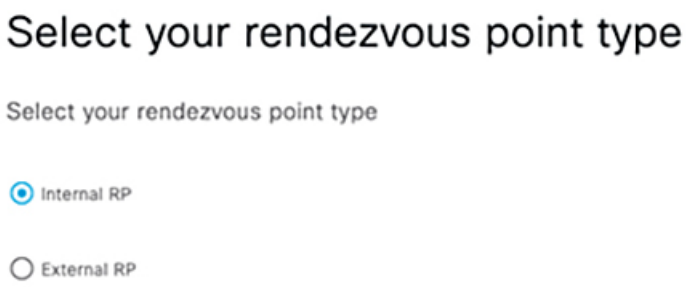
Figure 334 Edit Multicast in a Fabric Site

The option for multicast will say “Configure Multicast” if not enabled or “Edit Multicast” if enabled. Within the multicast wizard, it will require configuring whether the site is using head-end replication versus native multicast, the virtual network, whether ASM or SSM is used in the overlay, the IP pool to be mapped, and the location of the rendezvous point whether internal or external.

As mentioned before, head-end replication is being used in CCI to minimize the amount of manual configuration on the network devices.

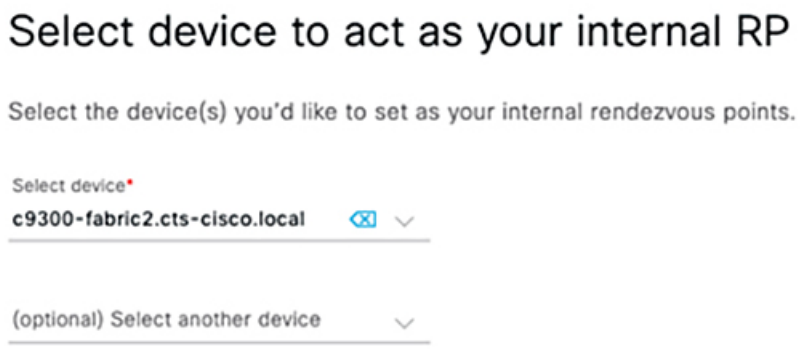
The decision needs to be made whether ASM or SSM will be supported in the overlay. As mentioned before, choosing ASM requires also choosing a rendezvous point. When enabling multicast within a PoP site, an internal rendezvous point should be chosen. Note that this configuration creates a single PIM domain within the fabric site and if inter-PoP multicast traffic needs to occur at a later time, additional manual configuration will need to be added or the setup needs to change per the section discussing multicast between PoP sites.

Figure 335 Internal Rendezvous Point



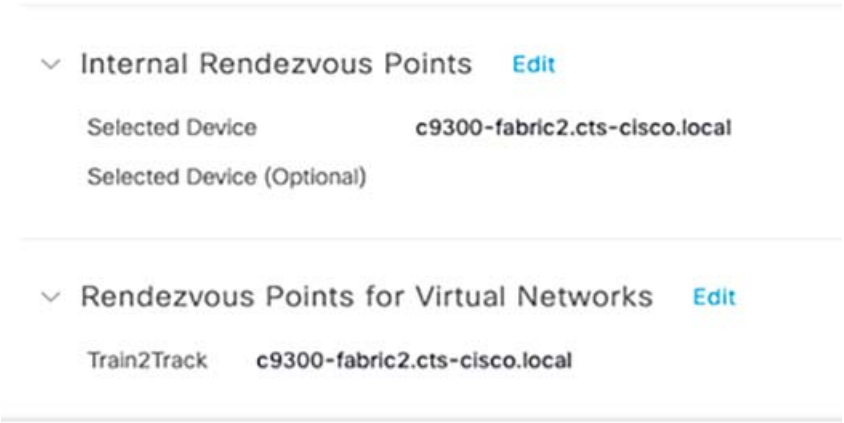
The workflow will then ask which fabric node is to be the internal RP and since PoP is using a fabric in a box setup, that node should be chosen as the RP as seen below.

Figure 336 Choosing Node to be Internal Rendezvous Point



After configuring the internal RP, the multicast summary should look like the one in Figure 337.

Figure 337 Intra PoP Multicast Summary



After deploying the multicast configuration, the fabric nodes will be configured with the appropriate commands. The commands added on the fabric in a box node are given below.

Multicast Configuration in Fabric-in-a-Box

Switched Virtual Interface for VN:

```
ip pim passive
ip route-cache same-interface
ip igmp version 3
ip igmp explicit-tracking
```

Loopback:

```
interface Loopback4111
 vrf forwarding Train2Track
 ip address 172.16.7.129 255.255.255.255
 ip pim sparse-mode
end
```

LISP Interface:

```
interface LISP0.4111
 ip pim sparse-mode
end
```

PIM and Multicast are also enabled at the global level for the VRF.

```
ip pim vrf Train2Track rp-address 172.16.7.129
ip pim vrf Train2Track register-source Loopback4111
ip pim vrf Train2Track ssm default
ip multicast-routing vrf Train2Track
```

Note that SSM is enabled even when ASM is configured as part of the workflow. By default, SSM uses the multicast group range of 232.0.0.0/8.

To validate multicast traffic a source must send traffic to a multicast group. In this example, the source traffic was a video stream to group address 239.10.10.10. Receivers must also subscribe this group address to receive the data. Below is the output of the fabric in a box multicast routing table from the source to a receiver.

```
(*, 239.10.10.10), 3d20h/stopped, RP 172.16.7.129, flags: SJCF
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1026, Forward/Sparse-Dense, 3d20h/00:02:52

(172.16.14.131, 239.10.10.10), 3d20h/00:02:44, flags: PFT
  Incoming interface: Vlan1026, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

SSM in Overlay

The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature.

By default, when ASM is configured from the Cisco DNA Center workflow, SSM is also configured at the same time. The default option enables SSM for the multicast group 232.0.0.0/8. If a different multicast group is desired, the SSM option in the multicast workflow in Cisco DNA Center supports a custom group address. When SSM is specifically configured, there is no option to add a rendezvous point. The differences in the Cisco DNA Center workflow are shown below.

Figure 338 Select SSM

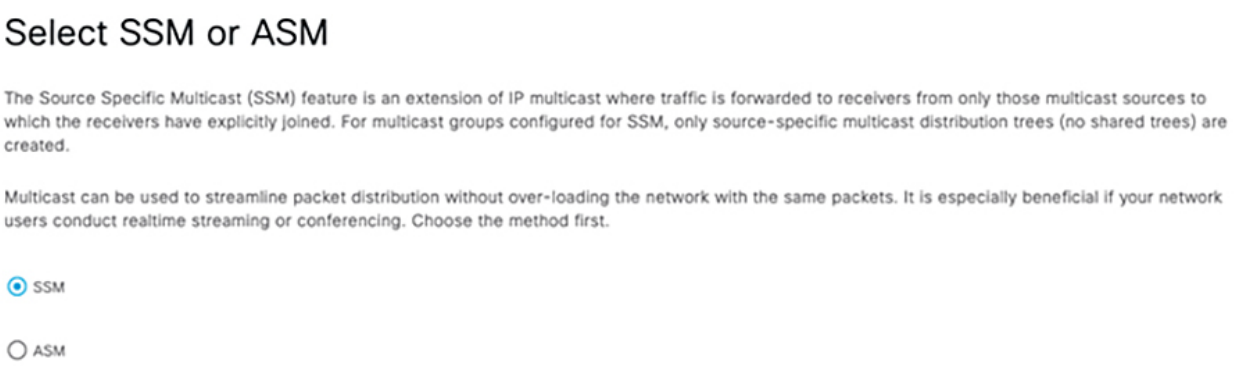
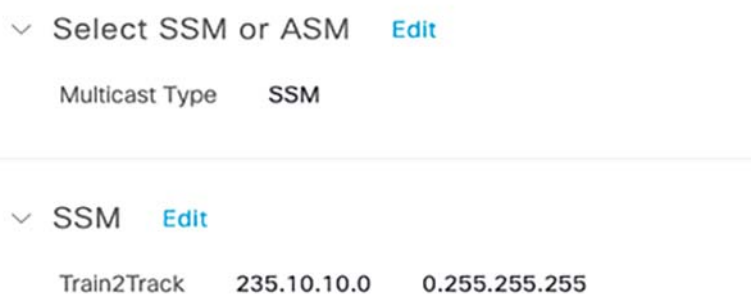


Figure 339 Choose SSM Range



The PIM configuration on the fabric node is also different since the SSM range is no longer the default group range.

```
ip pim vrf Train2Track ssm range SSM_RANGE_Train2Track
ip access-list standard SSM_RANGE_Train2Track
 10 permit 235.0.0.0 0.255.255.255
```

The below examples are using the default SSM range.

To verify SSM functionality, the multicast source sends the video stream to a group address in 232.0.0.0/8. The multicast receiver must then subscribe to the host IP of the source @ the group address. In VLC, this is configured as rtp://<Source IP>@<group address>:<port>

Below is the Mroute validation on the fabric in a box. The source and receiver are connected on different fabric devices.

```
(172.16.14.131, 232.10.10.10), 00:05:39/00:02:26, flags: sPTI
  Incoming interface: Vlan1026, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

Configuring Multicast between PoP Sites

IP Transit

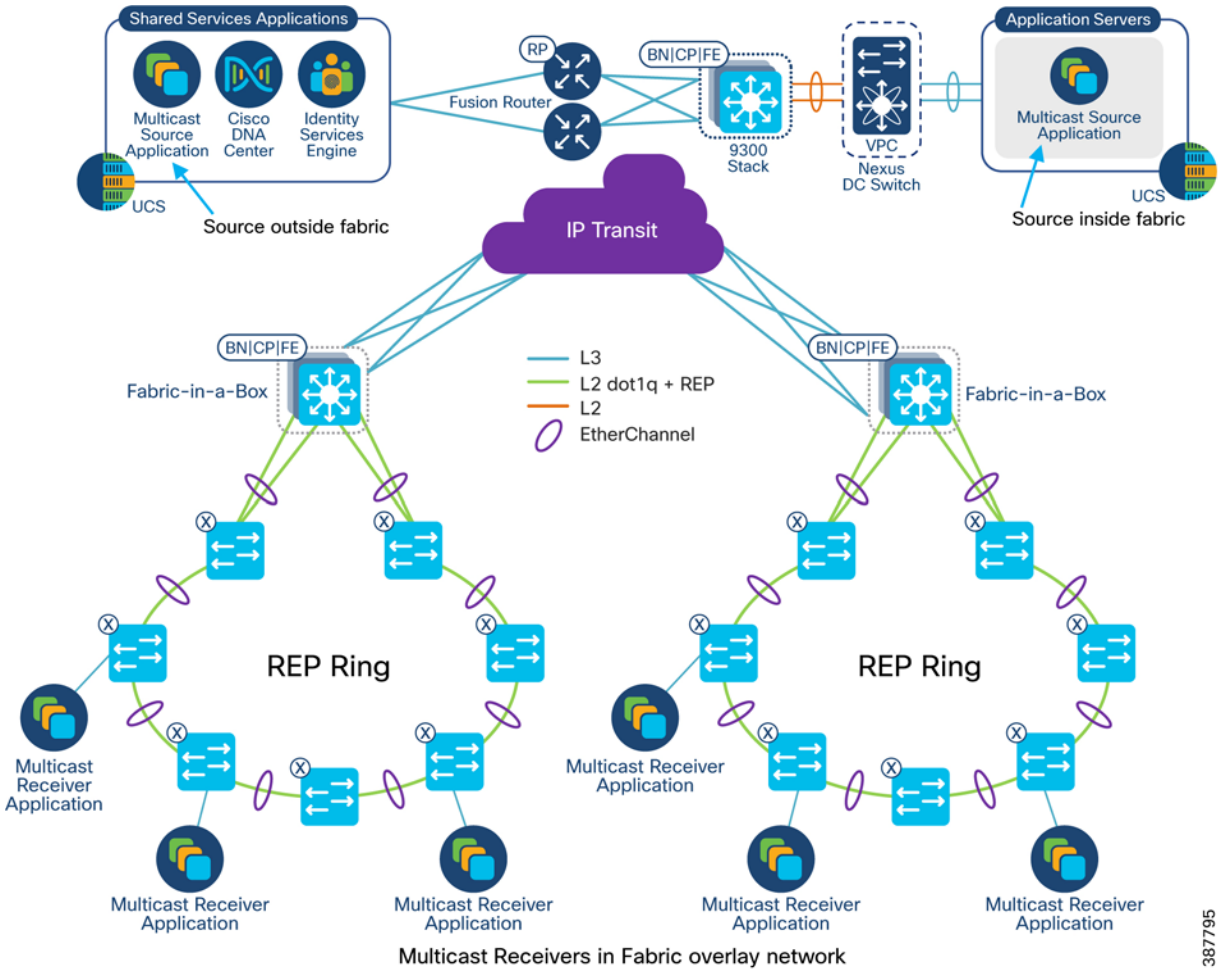
Before configuring multicast using IP Transit, several things must be considered. These include the location of the sources and receivers, the multicast configuration of the service provider core, and whether Any Source Multicast (ASM) or Source Specific Multicast (SSM) will be used in the network overlay.

To minimize the amount of manual configuration with ASM, it is recommended to place a multicast source behind the fusion router or at the data center fabric site. The rendezvous point could then be centrally located if the receivers are at the edge fabric sites. It should be noted that when configuring ASM through the Cisco DNA Center workflow, SSM with the default multicast group range (232.0.0.0/8) is also configured on the fabric node.

This section will describe the configuration from the Cisco DNA Center workflow as well as show the configuration from the fusion router and fabric nodes. A sample configuration for the service provider core will also be shown.

An example of the test configuration is shown in Figure 340.

Figure 340 Multicast over an MPLS IP Transit

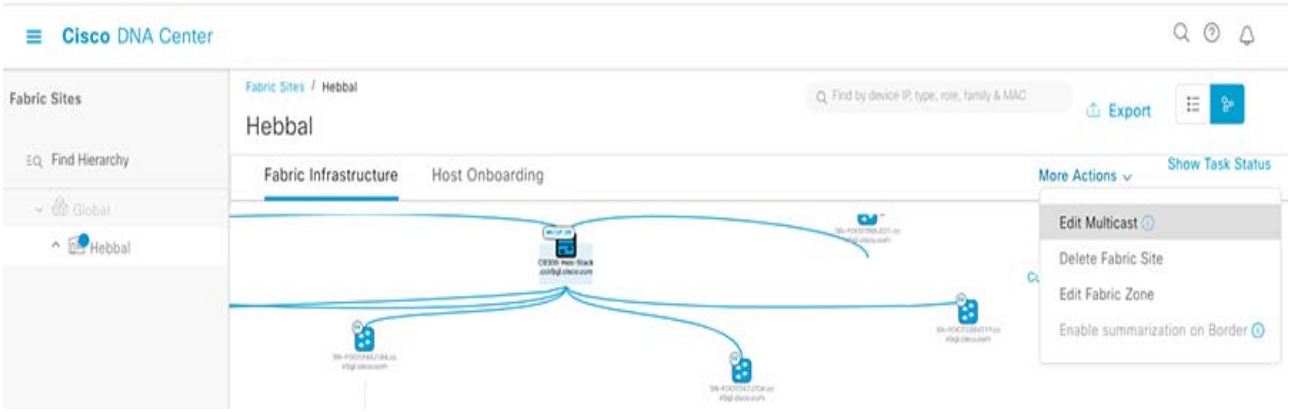


Prior to configuring multicast, IP pools must be configured in Cisco DNA Center under Design -> Network Settings -> IP Address Pools and then reserved in each site.

Multicast Source and Rendezvous Point at Fusion Router

In this example, the multicast source is behind the fusion router with the receivers in a VN. The VRF for the VN is extended to the multicast source to prevent the need for route leaking. Cisco DNA Center must then be configured to enable multicast in every site where the receivers may be located. The workflow for this starts at the Fabric Site within the Fabric Provisioning section seen in Figure 341

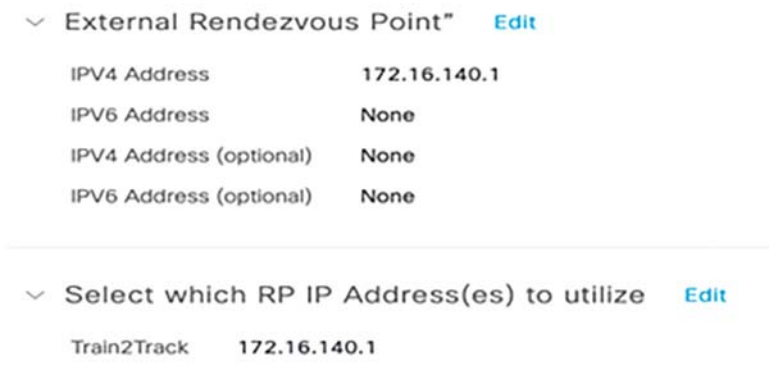
Figure 341 Edit Multicast in a Fabric Site



The option for multicast will say “Configure Multicast” if not enabled or “Edit Multicast” if enabled. Within the multicast wizard, it will require configuring whether the site is using head-end replication versus native multicast, the virtual network, whether ASM or SSM is used in the overlay, the IP pool to be mapped, and the location of the rendezvous point whether internal or external.

With the source behind the fusion router, the rendezvous point will point to an IP address in the VRF configured on the fusion router. When configuring the fabric sites, the external rendezvous point option must be chosen, and the previously mentioned IP address configured.

Figure 342 External Rendezvous Point



After deploying the multicast config, the fabric nodes will be configured with the appropriate commands. The commands added on the fabric in a box node are shown below.

Multicast Configuration in Fabric-in-a-Box

Switched Virtual Interface for VN:

```
interface Vlan1029
 ip pim passive
 ip route-cache same-interface
 ip igmp version 3
 ip igmp explicit-tracking
```

Loopback:

```
interface Loopback4111
 vrf forwarding Train2Track
 ip address 172.16.7.66 255.255.255.255
 ip pim sparse-mode
end
```

LISP Interface:

```
interface LISP0.4111
 ip pim sparse-mode
end
```

Border Interface:

```
ip pim sparse-mode
 ip route-cache same-interface
```

PIM and Multicast are also enabled at the global level for the VRF.

```
ip pim vrf Train2Track rp-address 172.16.140.1
ip pim vrf Train2Track register-source Loopback4111
ip pim vrf Train2Track ssm default
ip multicast-routing vrf Train2Track
```

Note that SSM is enabled even when ASM is configured as part of the workflow. By default, SSM uses the multicast group range of 232.0.0.0/8.

The fusion router and all devices up to the multicast source must also be configured to support multicast. This includes enabling PIM sparse-mode on all intermediate interfaces as well as multicast routing. A sample configuration for the fusion router is given below.

Multicast Configuration in Fusion Router

Source facing interface:

```
interface GigabitEthernet0/0/5.140
 encapsulation dot1Q 140
 vrf forwarding Train2Track
 ip address 172.16.140.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
```

Configure fusion router as rendezvous point:

```
ip pim vrf Train2Track rp-address 172.16.140.1
```

Configure multicast routing

```
ip multicast-routing vrf Train2Track distributed
```

MPLS IP Transit Multicast

An MPLS IP transit is used in this implementation between the fabric sites and must also be configured to pass multicast traffic. As described here: https://www.cisco.com/c/en/us/support/docs/ip/multicast/118985-configure-mcast-00.html, there are numerous ways to implement MVPN. For this implementation, Profile 0 or Rosen Draft was chosen. The MPLS core and therefore the multicast configuration is likely provided by a service provider so the choice of other MVPN profiles is outside the scope of this document. It is important to note that the provider multicast network is separate from the customer multicast network and serves to transport the different customer's multicast traffic in the most efficient way possible.

With this configuration, PIM runs on all the core interfaces and all the PEs in a multicast VRF (MVRF) become PIM neighbors by way of GRE tunnels. The PEs learn about other PIM neighbors using BGP.

Provider Edge + Core Routers

Each core facing interface as well as the interface in the multicast VRF should be configured for PIM sparse-mode. To configure the VRF for Rosen Draft, Multicast Distribution Tree (MDT) will be used. A default MDT is required, but a data MDT can also be used for higher bandwidth applications.

```
vrf definition cci-trackside
 rd 31:6
 !
 address-family ipv4
  mdt default 232.0.0.1
  mdt data 232.1.1.0 0.0.0.255
  route-target export 31:31
  route-target import 31:31
 exit-address-family
```

BGP passes the multicast information using the extended communities attribute and is configured in the global BGP config.

```
address-family ipv4 mdt
  neighbor 10.3.255.1 send-community extended
  neighbor 10.3.255.1 activate
 exit-address-family
```

PIM and Multicast routing must also be configured on each PE.

```
! Enables SSM in the provider multicast network
ip pim ssm default
! Configures the RP for the particular Customer VRF (fusion router)
ip pim vrf cci-trackside rp-address 172.16.140.1
! Enables global multicast routing
ip multicast-routing distributed
! Enables multicast routing for the Customer VRF
ip multicast-routing vrf cci-trackside distributed
```

On the core routers, the configuration is the same as the provider edge routers except for the lack of customer VRFs.

After the MPLS core is configured, PIM neighborships will form over the GRE tunnels to every PE with the multicast VRF configured.

An example of the MVRF PIM neighbor table is below.

```
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
172.16.15.1       BDI3036                  1d21h/00:01:16    v2    1 / S P G
172.16.1.57       BDI3037                  1d22h/00:01:24    v2    1 / S P G
10.3.255.2        Tunnel0                  3w0d/00:01:21     v2    1 / S P G
172.16.2.1        BDI3018                  1d21h/00:01:41    v2    1 / S P G
```

To validate multicast traffic a source must send traffic to a multicast group. In this example, the source traffic was a video stream to group address 239.10.10.10. Receivers must also subscribe this group address to receive the data. Below is the output of the multicast routers from the source to a receiver.

```
show ip mroute vrf <vrf>
```

Fusion Router:

```
(*, 239.10.10.10), 1d02h/00:03:27, RP 172.16.140.1, flags: SF
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0.31, Forward/Sparse, 1d01h/00:03:27
    Te0/2/0.3033, Forward/Sparse, 1d02h/00:02:56

(172.16.140.2, 239.10.10.10), 1d01h/00:03:00, flags: FT
  Incoming interface: GigabitEthernet0/0/5.140, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0.31, Forward/Sparse, 1d01h/00:03:27
    Te0/2/0.3033, Forward/Sparse, 1d01h/00:03:24
```

Ingress Provider Edge Router:

```
(*, 239.10.10.10), 00:12:16/00:03:02, RP 172.16.140.1, flags: S
  Incoming interface: BDI31, RPF nbr 10.2.1.93
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:12:16/00:03:02

(172.16.140.2, 239.10.10.10), 00:12:16/00:03:17, flags: Ty
  Incoming interface: BDI31, RPF nbr 10.2.1.93
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:12:16/00:03:02
```

Egress Provider Edge Router:

```
(*, 239.10.10.10), 00:14:28/00:03:25, RP 172.16.140.1, flags: S
  Incoming interface: Tunnel0, RPF nbr 10.3.255.2
  Outgoing interface list:
    BDI3037, Forward/Sparse, 00:11:53/00:03:25
    BDI3018, Forward/Sparse, 00:14:28/00:02:50

(172.16.140.2, 239.10.10.10), 00:14:28/00:02:53, flags: TY
  Incoming interface: Tunnel0, RPF nbr 10.3.255.2, MDT:[10.3.255.2,232.1.1.0]/00:02:41
  Outgoing interface list:
    BDI3037, Forward/Sparse, 00:11:53/00:03:28
    BDI3018, Forward/Sparse, 00:14:28/00:02:50
```

Fabric in a Box:

```
(*, 239.10.10.10), 00:19:28/stopped, RP 172.16.140.1, flags: SJC
  Incoming interface: Vlan3037, RPF nbr 172.16.1.58
  Outgoing interface list:
    Vlan1029, Forward/Sparse-Dense, 00:19:28/00:02:12

(172.16.140.2, 239.10.10.10), 00:19:28/00:02:04, flags: JT
  Incoming interface: Vlan3037, RPF nbr 172.16.1.58
  Outgoing interface list:
    Vlan1029, Forward/Sparse-Dense, 00:19:28/00:02:12
```

SSM in Overlay

The other option for multicast in the overlay is Source Specific Multicast (SSM). In this mode, a receiver expresses interest in a multicast group from a specific source as opposed to any source. This serves to reduce the amount of multicast traffic in the network. The multicast router only has to record the (S,G) entry instead of the additional (*,G) entry. The other advantage is that a rendezvous point is not necessary to support SSM. The disadvantage is that only IPv4 IGMP3 and IPv6 MLDv2 support this feature. The receiver's operating system must also support this feature.

By default, when ASM is configured from the Cisco DNA Center workflow, SSM is also configured at the same time. The default option enables SSM for the multicast group 232.0.0.0/8. If a different multicast group is desired, the SSM option in the multicast workflow in Cisco DNA Center supports a custom group address. When SSM is specifically configured, there is no option to add a rendezvous point. The differences in the Cisco DNA Center workflow are shown below.

Figure 343 Select SSM

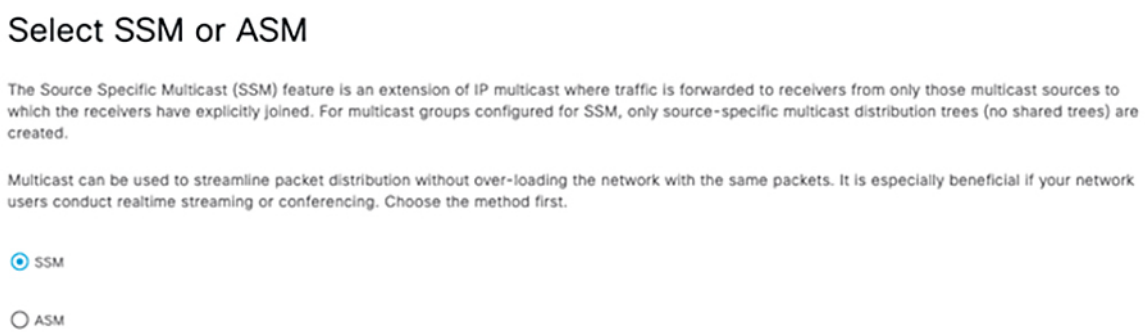
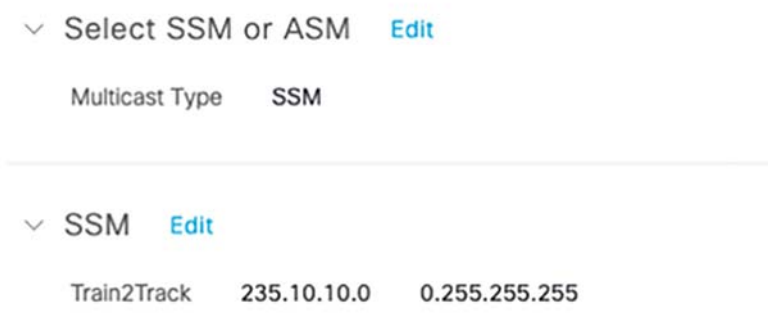


Figure 344 Choose SSM Range



The PIM configuration on the fabric node is also different since the SSM range is no longer the default group range.

```
ip pim vrf Train2Track ssm range SSM_RANGE_Train2Track
ip access-list standard SSM_RANGE_Train2Track
 10 permit 235.0.0.0 0.255.255.255
```

The examples below use the default SSM range.

To verify SSM functionality, the multicast source sends the video stream to a group address in 232.0.0.0/8. The multicast receiver must then subscribe to the host IP of the source @ the group address. In VLC, this is configured as rtp://<Source IP>@<group address>:<port>

Below is the Mroute validation on the multicast routers between the source and receiver.

Fusion Router:

```
(172.16.140.2, 232.10.10.10), 00:33:25/00:03:19, flags: sT
  Incoming interface: GigabitEthernet0/0/5.140, RPF nbr 0.0.0.0
  Outgoing interface list:
    Te0/2/0.3033, Forward/Sparse, 00:32:41/00:03:19
    GigabitEthernet0/0/0.31, Forward/Sparse, 00:33:25/00:02:33
```

Ingress Provider Edge Router:

```
(172.16.140.2, 232.10.10.10), 00:13:04/00:03:05, flags: sTy
  Incoming interface: BDI31, RPF nbr 10.2.1.93
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:13:13/00:03:05
```

Egress Provider Edge Router:

```
(172.16.140.2, 232.10.10.10), 00:13:04/00:03:05, flags: sTy
  Incoming interface: BDI31, RPF nbr 10.2.1.93
  Outgoing interface list:
    Tunnel0, Forward/Sparse, 00:13:13/00:03:05
```

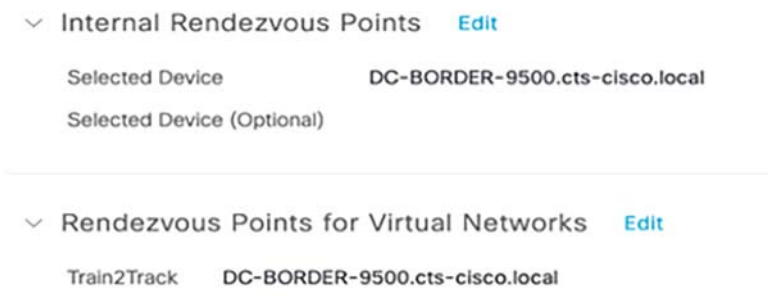
Fabric in a Box:

```
(172.16.140.2, 232.10.10.10), 00:11:10/00:02:24, flags: sTI
  Incoming interface: Vlan3037, RPF nbr 172.16.1.58
  Outgoing interface list:
    Vlan1029, Forward/Sparse-Dense, 00:11:10/00:02:24
```

Multicast Source and Rendezvous Point at Data Center Fabric Site

Another centrally located place for the multicast sources and rendezvous point is at the data center fabric site. The configuration procedure is very similar to the fusion router multicast setup. The data center multicast configuration must be done first because all edge fabric sites will point to the data center's multicast loopback as the external RP address. When configuring the data center fabric site for multicast, an internal rendezvous point is chosen instead of an external one. The sample output from the workflow is shown below.

Figure 345 Internal RP at Data Center Border



The MPLS core devices and fusion router must also be manually configured to point to this RP address.

SDAT Multicast

Configuring Multicast over SD-Access Transit

Enabling multicast between fabric sites necessarily means a transit is required to pass that traffic. In this section we cover the Headend Multicast Replication scenario over the SDA-Transit is discussed. In Headend Multicast Replication, the first Fabric Node that receives the multicast traffic (head-end) will replicate the multicast data into multiple unicast copies and send each copy to the Fabric Edge nodes where the receivers are located. This deployment only requires to have Any-Source Multicast (ASM) enabled in the Fabric Overlay.

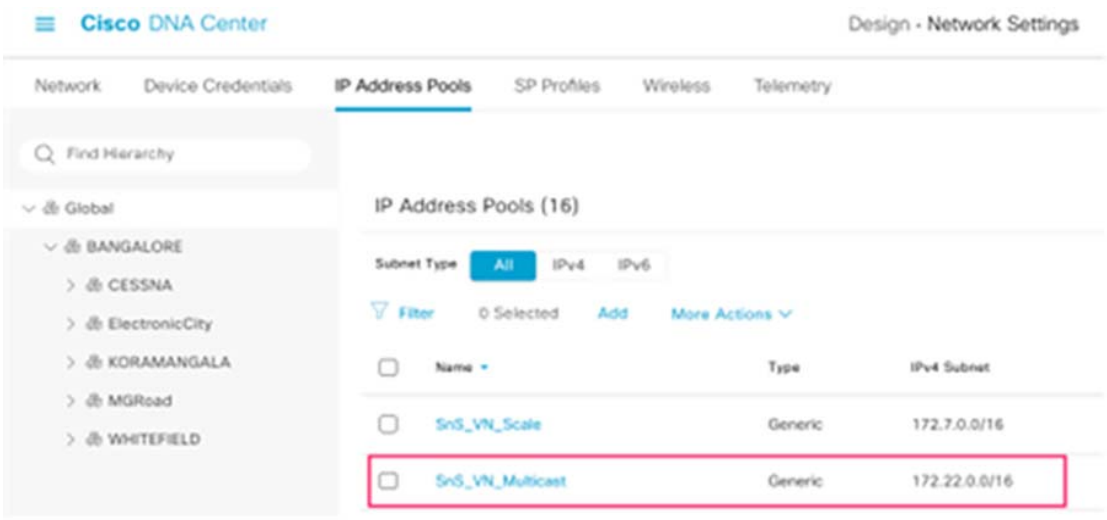
It is recommended to place a multicast source behind the fusion router or at the data center fabric site, as discussed in the design guide for enabling multicast forwarding across CCI PoPs. The Rendezvous Point (RP) is configured external to the CCI PoPs on the Fusion Router.

The Cisco DNA Center provides a workflow that helps enable group communication or multicast traffic in the virtual network. This section will describes the configuration from the Cisco DNA Center workflow and shows the configuration required on the fusion router.

Configuring Multicast Head-End Replication:

1. Create an IP address pool for multicast in the Global under the Network Settings, as shown in Figure

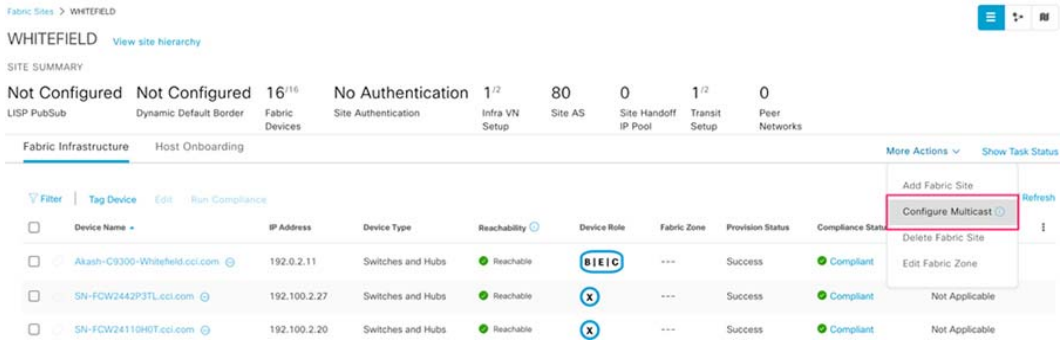
Figure 346 Cisco DNA Center Multicast Address pool



2. Reserve a Multicast IP Pool at the Site level. This IP Pool is used by DNAC to configure Loopbacks, a Rendezvous Point (RP), and Multicast Source Discovery Protocol (MSDP) if more than one RP is used. Repeat the same step for the other sites where you want to enable multicast.

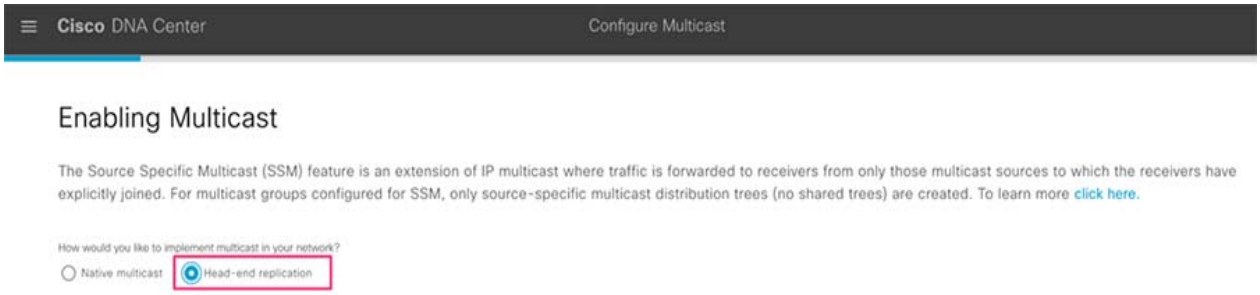
3. Go to the Fabric sites Infrastructure and select the fabric sites where you want to configure the multicast. and sStart configuring the multicast.

Figure 347 Cisco DNA Center Multicast Configuration



4. In the Enabling Multicast window, choose the method of multicast implementation for the network: Head-end replication. Click **Next**.

Figure 348 Cisco DNA Center Multicast Implementation selection



5. In the Virtual Networks window, select the virtual network on which you want to set up multicast. Click Next.
6. In the Multicast pool mapping window, select an IP address pool from the IP Pools drop-down list. The selected IP address pool is associated with the chosen virtual network. Click **Next**.
7. In the Select multicast type window, choose the type **Any Source Multicast (ASM)** to implement, and then click **Next**
8. Choose External RP as your rendezvous point type, and then click **Next**. In the popup window, enter the external RP IP address, in this case the logical IP address on the fusion router.
9. In the Select which RP IP Address(es) to utilize window, select an IP address for each Virtual Network. Click **Next**.
10. Review the multicast settings displayed in the Summary window and modify them, if required, before submitting the configuration. Click **Finish** to complete the multicast configuration and deploy.

Multicast Configuration in Fabric-in-box

After completing the steps above have been completed, verify the relevant Multicast configuration is pushed by DNAC Cisco DNA Center to the FiaB. The similar configurations are present on all the sites where you enabled Head-end replication Multicast.

Verify the Multicast Routing is enabled on the VRF:

```
Akash-C9300-Whitefield#show run | sec multicast
ip multicast-routing vrf SnS_VN
```

Verify configuration on a SnS_VN Loopback (4100) for the RP selection enables PIM on each interface including the logical LISP interface for that instance and on the L3 Hand-off SVI:

```
interface Loopback4100
 vrf forwarding SnS_VN
 ip address 172.22.2.2 255.255.255.255
 ip pim sparse-mode
end
interface LISP0.4100
 ip pim sparse-mode
end
 interface Vlan1023
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f138
 vrf forwarding SnS_VN
 ip address 172.20.2.1 255.255.255.0
 ip helper-address 10.10.100.42
 no ip redirects
 ip pim passive
 ip route-cache same-interface
```

```
 ip igmp version 3
 ip igmp explicit-tracking
 no lisp mobility liveness test
 lisp mobility SnS_VN-IPV4
 no autostate
end
```

Verify the configuration of the RP and enables SSM for this VN:

```
ip pim vrf SnS_VN rp-address 192.168.7.6
ip pim vrf SnS_VN register-source Loopback4100
ip pim vrf SnS_VN ssm default
Multicast Configuration in Fusion Router::
Configure the Multicast Routing on the VRF:
ip multicast-routing vrf SnS_VN distributed
Configure Multicast on the logical interface:
interface BDI16
 vrf forwarding SnS_VN
 ip address 192.168.7.6 255.255.255.252
 ip pim sparse-mode
end
Configure the RP in the SnS_VN VRF:
ip pim vrf SnS_VN rp-address 192.168.7.6
```

Verification of Multicast between PoP Sites over SDA-Transit:

For the verification of Multicast over SDA-Transit, the multicast source is connected at the central fabric site (i.e; Akash-C9300-Cessna site in our example) and the receivers are connected to the IE Switches at the PoP Site (i.e; Akash-C9300-Whitefiled site). In this example, the source traffic was a streamed to the group address 239.255.255.250. Receivers must also subscribe to this group address to receive the data. Below is the output of the multicast routers from the source to a receiver.

Central Fabric Site (Source side):

```
Akash-C9300-Cessna#show ip mroute vrf SnS_VN

<Snip>

(*, 239.255.255.250), 00:04:05/00:03:19, RP 192.168.7.6, flags: SF

  Incoming interface: Vlan167, RPF nbr 192.168.70.6

  Outgoing interface list:
    LISP0.4100, 192.0.2.11, Forward/Sparse, 00:04:05/00:03:19


 (172.5.0.22, 239.255.255.250), 00:00:24/00:03:05, flags: FT
  Incoming interface: Vlan1026, RPF nbr 0.0.0.0


  Outgoing interface list:
    LISP0.4100, 192.0.2.11, Forward/Sparse, 00:00:24/00:03:19

(*, 224.0.1.40), 00:04:39/00:03:07, RP 192.168.7.6, flags: SJCL
  Incoming interface: Vlan167, RPF nbr 192.168.70.6
  Outgoing interface list:
    LISP0.4100, 192.0.2.11, Forward/Sparse, 00:04:21/00:03:07
    Loopback4100, Forward/Sparse, 00:04:39/00:02:34
```

Fusion Router:

```
ISR-FUSION#show ip mroute vrf SnS_VN
<Snip>
```

```
 (*, 239.255.255.250), 00:01:17/stopped, RP 192.168.7.6, flags: SP
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null

(172.5.0.22, 239.255.255.250), 00:01:17/00:01:42, flags: P
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null


 (*, 224.0.1.40), 00:05:07/00:02:57, RP 192.168.7.6, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    BDI16, Forward/Sparse, 00:05:07/00:02:57
```

Receiver side PoP Site:

```
 Akash-C9300-Whitefield#sh ip mroute vrf SnS_VN

<Snip>

(*, 239.255.255.250), 00:04:43/stopped, RP 192.168.7.6, flags: SJC
  Incoming interface: LISP0.4100, RPF nbr 192.0.1.11
  Outgoing interface list:
    Vlan1026, Forward/Sparse-Dense, 00:01:31/00:02:13
    Vlan1023, Forward/Sparse-Dense, 00:04:43/00:02:12

(172.5.0.22, 239.255.255.250), 00:01:02/00:01:57, flags: JT
  Incoming interface: LISP0.4100, RPF nbr 192.0.1.11
  Outgoing interface list:
    Vlan1023, Forward/Sparse-Dense, 00:01:02/00:02:12
    Vlan1026, Forward/Sparse-Dense, 00:01:02/00:02:13

(*, 224.0.1.40), 00:04:59/00:02:09, RP 192.168.7.6, flags: SJCL
  Incoming interface: LISP0.4100, RPF nbr 192.0.1.11
  Outgoing interface list:
    Loopback4100, Forward/Sparse, 00:04:59/00:02:09
```

Implementation of SCADA Communication with Multiple Backhaul Types and Protocols

SCADA is a category of software application programs used for process control and the gathering of data in real time or near real time from remote locations to control equipment and report conditions. SCADA data can be used to create a local action as well as be transmitted to the SCADA Primary/Subordinate which is located in primary or secondary control center for monitoring and control purposes. The implementation in this guide focuses on Distributed Network Protocol 3 (DNP3) and MODBUS SCADA protocols.

The CCI solution is a centralized two-tier architecture, as shown in Figure 349. SCADA applications like Triangle Micro Works (TMW), a simulation software, or Water SCADA Applications and Outage Management System reside in the Control center.

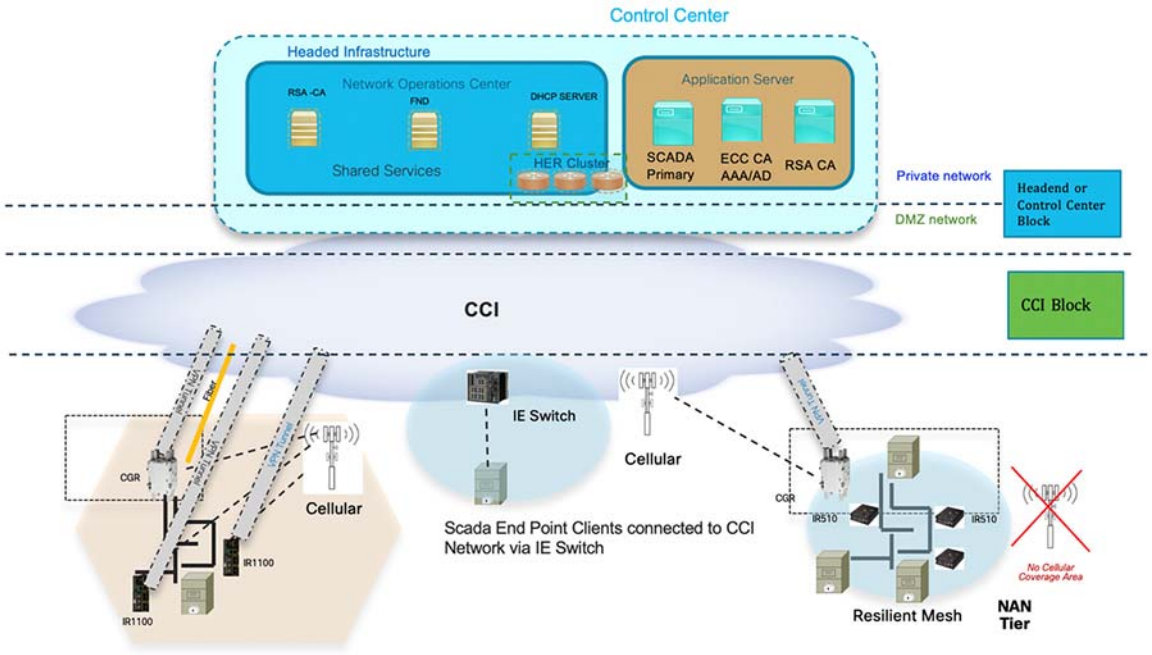
Cisco SCADA Gateways communicate with SCADA Remote Devices (PLC/RTU) in two ways, either over Serial or Ethernet. Cisco's SCADA Gateways backhaul their traffic over a Cellular, Ethernet, or CR-Mesh backhaul as defined in the CCI architecture.

To choose the correct Gateway, refer to the Design Guide at:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CCI/CCI/DG/cci-dg/cci-dg.html

This implementation guide covers both Cisco Cellular Gateway, Ethernet connected, and Cisco Resilient Mesh Gateway deployments.

Figure 349 CCI SCADA Implementation



Cisco Resilient (CR) Mesh implementation will be the correct choice for areas where cellular coverage is not available or less prevalent. Cisco CR mesh has three types of devices:

1. CR Mesh Coordination or Field Area Aggregation Router (FAR)
2. CR Mesh Gateways or Field Devices (FD)
3. CR Mesh Range Extenders

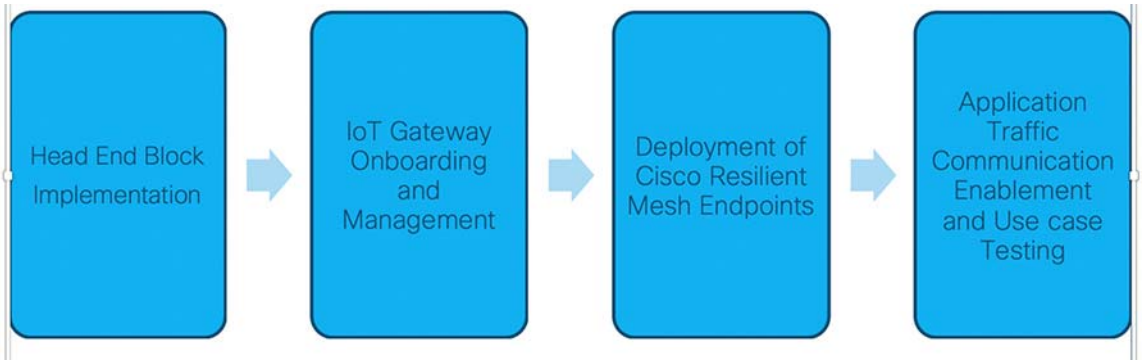
Cisco CGR 1240 with WPAN RF Module router plays the role of CR Mesh aggregator. CGR 1240 aggregates SCADA traffic and routes traffic to applications in the Control center. RTU/PLC are connected to IR510 CR Mesh Gateways via Ethernet or Serial (RS232) interfaces. When RF mesh coverage needs to be extended, Cisco IR530 is deployed as a range extender. The CR Mesh is formed using FAR, FD, and range extenders and can be implemented in multiple PHY modes. CR Mesh can support both OFDM and 2FSK modulation simultaneously supporting a maximum 600 kbps with channel spacing of 400 kHz.

Cisco IR1101 and CGR 1240 Cellular Gateways are chosen for SCADA deployments where:

- SCADA Application demands more bandwidth and has time sensitive requirements.
- SCADA Network has better Cellular signal coverage (for example, urban areas).

The flow of this implementation guide is depicted in Figure 350.

Figure 350 SCADA Implementation Flow

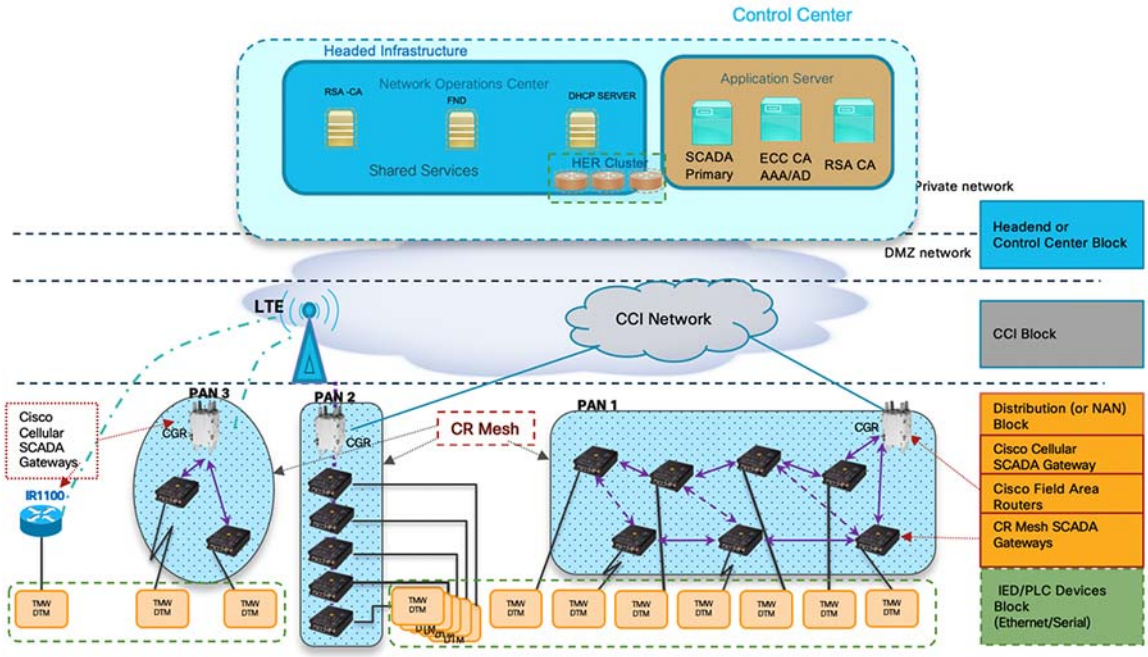


Note: For Headend Block Implementation, refer to Implementing Headend Network, page 176.

Solution Network Topology

This section focuses on the network topology and high-level implementation used for solution validation and implementation of the Cisco SCADA solution. It also describes the high-level solution validation topology used in this SCADA use case, which is depicted in Figure 351.

Figure 351 Cisco SCADA Validation Topology



The multiple layers of topology include:

1. The headend, which hosts the Control Center, includes:
   a. Application servers—Host SCADA application and they could also host other application servers (for example, ECC CA server and RSA CA server).
   b. Shared Services or Network Operations Center (NOC), which hosts the following headend components:
      - Dynamic Host Configuration Protocol (DHCP) Server or Cisco Prime Network Register (CPNR), Field Network Director (FND), and Headend Routers.
      - These components are essential for the Onboarding of the Cisco IOS Routers, which could be SCADA Gateways (IR1101) that are positioned along the SCADA Remote end devices or CGR1000 series of routers positioned as FARs.
   c. Headend Infrastructure block, which comprises:
      - Private network, where the protected part of the headend is located, along with SCADA and other application servers.
      - DMZ network, where the exposed part of the headend is located; it includes HER.
2. The CCI Block commonly refers to the transport of SCADA traffic via CCI Backhaul.
   – In this scenario, SCADA end devices are connected to Access Network (IE switch) via Ethernet backhaul.
3. The Distribution Block, which comprises the following three major sub-blocks:
   a. Cisco Cellular SCADA Gateways, which refer to Cisco IOS routers like the IR1100.
   b. Cisco Field Area Routers, which refer to Cisco IOS routers like the CGR1240. These routers are used for aggregating the Cisco Resilient Mesh Endpoints (also referred to as CR Mesh SCADA Gateways). The NAN Block is a subset of the Distribution Block, comprising CR Mesh devices, including Cisco FAR and CR Mesh endpoints.

c. Cisco Resilient Mesh SCADA Gateways with Edge Compute, which refer to the Cisco IR510 WPAN Industrial Router.

4. The IED/PLC Controller Devices Block, in which the remote SCADA devices (real/simulated) are connected to the Cisco SCADA Gateways (Cellular SCADA Gateway or Mesh SCADA Gateway) over an Ethernet/serial interface. The following components are simulated using the Triangle Micro Works (Distributed Test Manager or DTM) tool:
   - SCADA Primary/Subordinate located in Control Center.
   - PLC/RTUs located in the IED/PLC Devices Block layer.
5. The NAN Block, which comprises three Personal Area Networks (PANs):
   - CR Mesh-PAN1
   - CR Mesh-PAN2
   - CR Mesh-PAN3

   PAN3 has been validated over LTE backhaul. PAN1 and PAN2 have been validated over Ethernet backhaul.

IoT Gateway Onboarding and Management

This section includes the following major topics:

FND is used as the NMS in this solution. For information on installing and configuring FND, refer to Implementing Field Network Director for CCI, page 44. In this implementation guide, the terminology “IoT Gateway” is used to refer to both Cisco Cellular SCADA Gateways and Cisco FARs. As part of IoT Gateway onboarding, the IoT Gateways are registered with the FND. From that point on, the FND located in the Control Center could be used to remotely monitor/manage/troubleshoot the IoT Gateways, which are spread across the entire SCADA network.

This process has two phases:

1. IoT Gateway Configuration and Deployment
2. Remote Monitoring/Management/Troubleshooting of the IoT Gateway

Field Network Director Categories

Configuration from FND

The FND located in the staging environment helps in configuring of the IoT Gateways.

Network Operating Center or Shared Services

The FND located in the NOC/Control Center environment that helps with the configuration of IoT Gateways is referred to as the NOC or Control Center FND. This FND located in the Control Center helps with management of the IoT Gateways.

Note: The approach here is preconfiguration of the IoT Gateways that is done at the dedicated staging location. Once the devices are configured successfully, they are powered off and transported to the final deployment locations, where the devices are deployed and powered on.

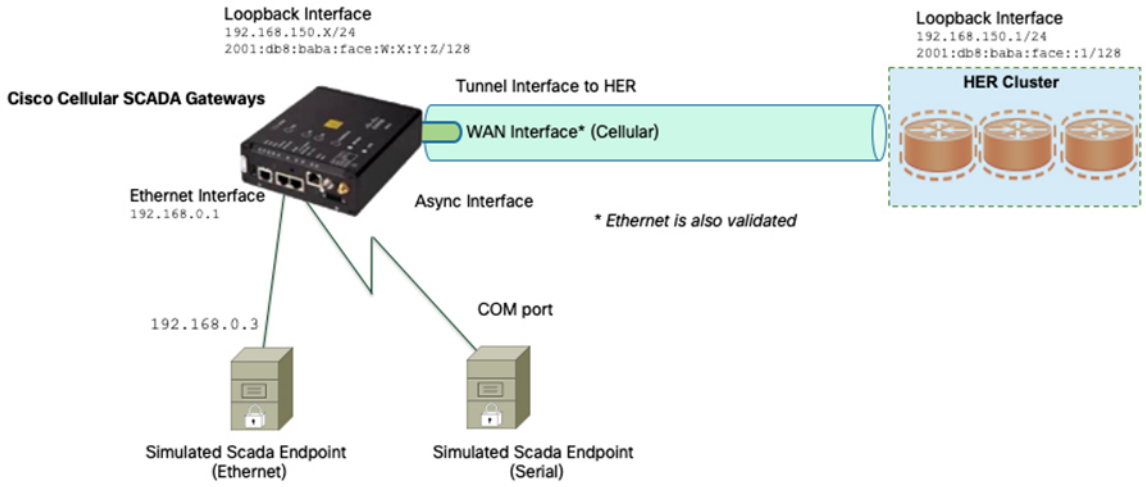
IoT Gateway Configuration and Deployment

IoT Gateways can be implemented in three different ways:

1. SCADA Remote Devices (PLC/RTU) connected to Remote POP Gateway IR1101—SCADA RTU/PLC will connect to Ethernet/serial interface of Remote POP Industrial Gateway (IR1101) having a Cellular backhaul.

   Refer to Secure Onboarding of Field Area Router—CGR1240, page 209 to on-board IR1101 into FND for remote management/configuration.

Figure 352 Cisco Cellular SCADA Gateways



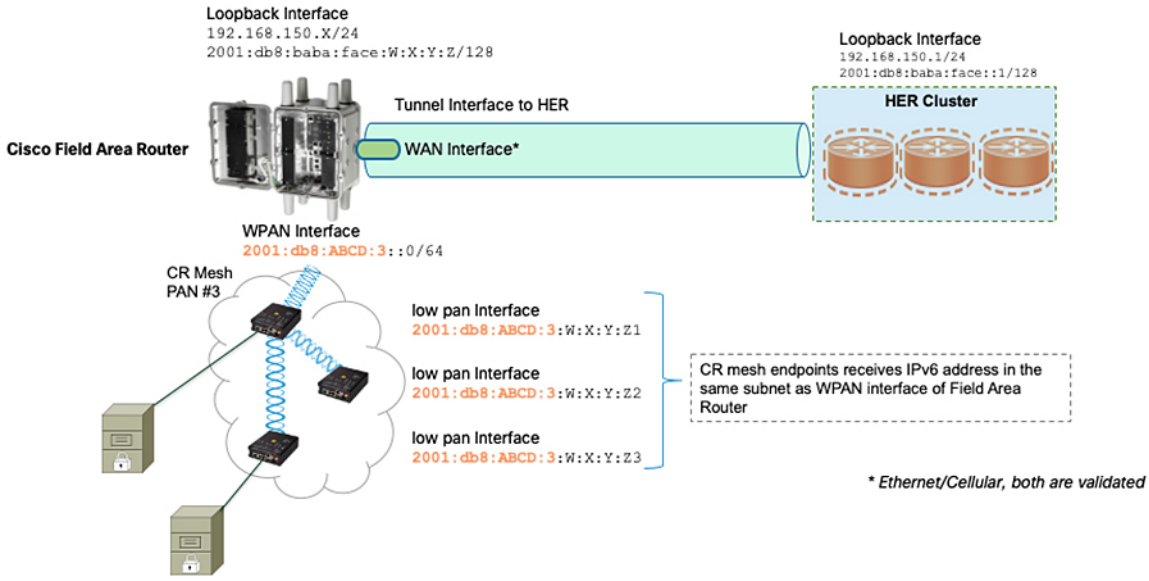
2. SCADA Remote Devices (PLC/RTU) connected to a Mesh Gateway IR510 aggregated by CR Mesh—SCADA RTU/PLC will be connected to Ethernet/serial interface of CR Mesh Gateway (IR510), which aggregates traffic to Field Area Routers (FAR). FARs aggregate the SCADA traffic from the CR Mesh network (NAN Tier) and route traffic to various SCADA application via the WAN tier (which could be a Cellular or Ethernet backhaul connection). In our scenario, FAR will transport SCADA traffic to SCADA Primary/Subordinate in two ways:

   – FAR connected to CCI Network—In this scenario, FAR will be connected to IE switch and FAR will have secure Flex VPN Secure tunnel to HER (Headend Router). CCI acts as transport.

   – FAR acts as Remote PoP (CGR 1240 with Cellular Interface).

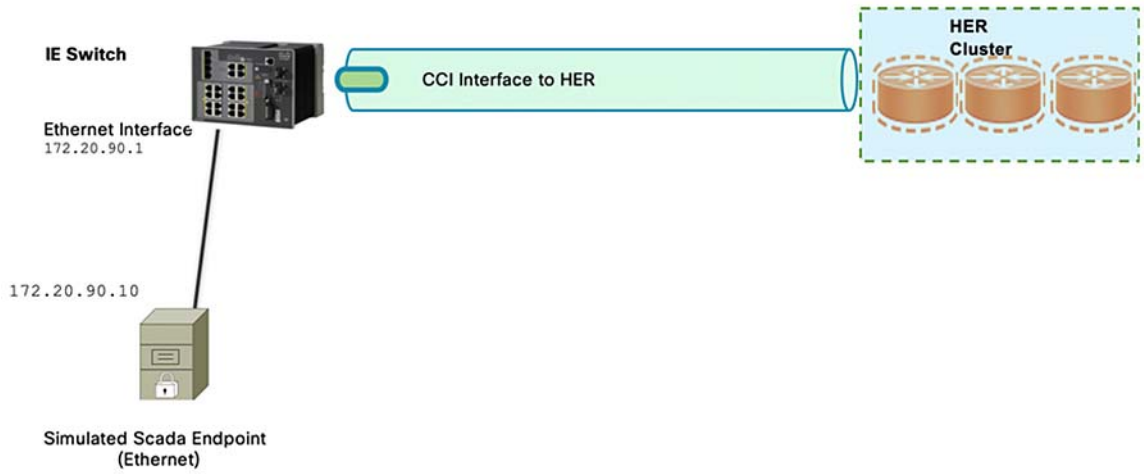
   Refer to Secure Onboarding of Field Area Router—CGR1240, page 209 to onboard CGR 1240 into FND for remote management/configuration. For onboarding IR510, refer to Enrollment of Cisco Resilient Mesh Endpoints—IR510, page 439.

Figure 353 Cisco Field Area Routers and Mesh Gateways



3. SCADA Remote Devices (PLC/RTU) connected directly to CCI Network (Ethernet Backhaul)—SCADA RTU/PLC will be directly connected to CCI Access network via Ethernet. SCADA RTU/PLCs can be connected to CCI Network Access devices (IE switches) and can aggregate SCADA traffic via CCI Network to SCADA control center. In this scenario only Ethernet ports are available to transport IP-based traffic.

Figure 354 SCADA Transport via CCI



With this, the Cellular SCADA Gateways or Cisco Field Area Routers could be onboarded and registered with FND, enabling further remote management and monitoring from FND.

The next section discusses in detail the implementation steps required to onboard the Cisco Resilient Mesh Endpoints like the Cisco IR510 WPAN Industrial Router to serve the functionality of the CR-Mesh SCADA Gateway.

Enrollment of Cisco Resilient Mesh Endpoints—IR510

This section includes the following major topics:

Staging

This section describes the implementation steps required to bring up the CR Mesh using IR510 Gateways for SCADA (also referred to as FDs). The IR510 connects to the CGR (also referred to as the FAR) via the Connected Grid Module (CGM) WPAN-OFDM-FCC module that needs to be installed within the FAR.

Note: For information on setting up the WPAN module, refer to the Connected Grid Module (CGM) WPAN-OFDM-FCC Module-Cisco IOS at following URL:

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/modules/cgm_wpan_ofdm/cgm_wpan_ofdm.html#pgfId-15768

Table 29 lists the basic components and their software versions needed to bring up the CR Mesh topology depicted in Figure 349.

Table 29 CR Mesh Components

Component	Product / Model	Software Image	Software Version
CGR	Cisco CGR1240/K9	cgr1000-universalk9-bundle.SPA.159-3.M2.bin	15.9(3)M2
CGM	CGM-WPAN-OFDM-FCC	cg-mesh-bridge-6.2-6219-ir510-1bf449d.bin	6.2.19
FD	IR510	cg-mesh-dagw-6.2-6219-ir510-1bf449d.bin	6.2.19
Configuration Writer Utility	cfgwriter	cfgwriter-6.0.20	6.0.20
HostOne Tool	fwubl	fwubl_win732bit_1.0.5	1.0.5

Certificate Creation and Installation on the IR510

The prerequisites for deploying a CR Mesh include obtaining all the necessary ECC certificates from the ECC CA server and configuring the AAA RADIUS server in ECC CA Server to authenticate the IR510 Gateway using a certificate-based authentication method. The FAR facilitates dot1x authentication between the IR510 and AAA server, thereby acting as the dot1x authenticator. The ECC certificate mentioned earlier is part of the configuration binary file (.bin) used to program the IR510 Gateway. The ECC certificates and procedures for generating the configuration file for IR510 are described in further sections.

Note: While the FD need ECC CA certificates for enrollment, FAR use RSA type certificate. The following certificates need to be obtained from the ECC CA to program an IR510 Gateway:

- The X.509 certificate of the IR510 in PKCS#12 format (.pfx) contains its private key and is used to program the node.
- The DER-encoded X.509 certificate (.cer) of the IR510 without the private key is used to enroll the node with the Active Directory.
- The DER-encoded X.509 certificate (.cer) of the ECC CA server is also used for programming the IR510.
- The CSMP certificate downloaded from the IoT FND in binary format (.cer) to validate node CSMP registration with IoT FND.

For details on setting up and configuring the ECC CA and AAA server and on obtaining all of the above certificates, refer to ECC Certificate Authority Installation, page 178.

The following section describes the process for generating a configuration binary file (.bin) used to program the IR510.

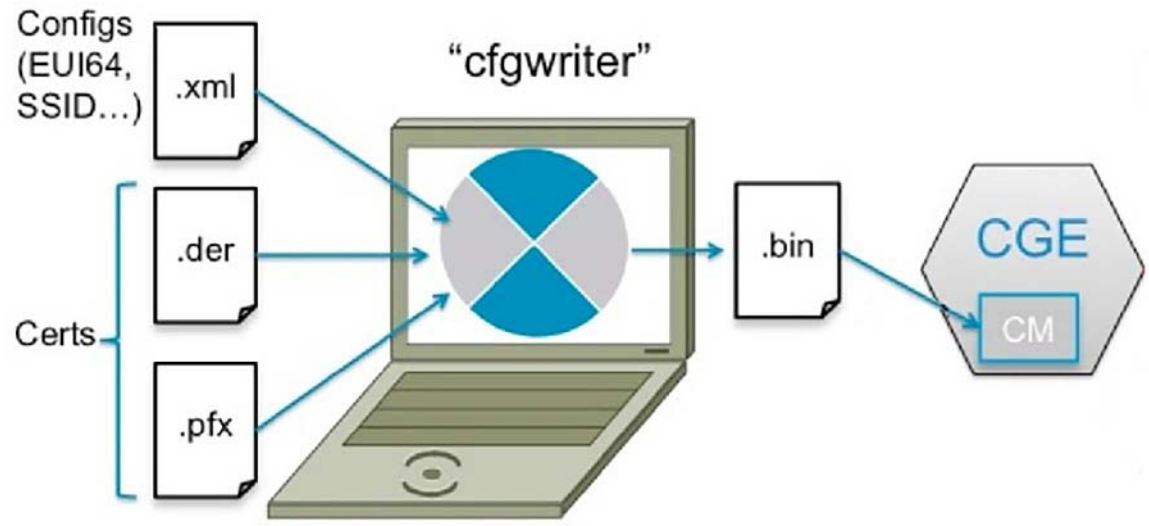
Bin File Creation

The configuration file for the IR510 Gateway is prepared in binary format using the Configuration Writer utility (cfgwriter).

Note: To obtain the cfgwriter utility discussed below, check with your account team or sales representative.

The cfgwriter utility is a java-based utility that takes as input an XML file with the node configuration information and produces a binary (.bin) memory file. This utility may be executed on any host platform with Java Run Time Environment installed. In this deployment, a Windows 10 machine with Java pre-installed was used to host the cfgwriter utility. The node configuration information, among other items, includes the SSID of the WPAN it must join and the security certificates. The schema of the XML configuration file and the corresponding documentation are packaged with the cfgwriter utility as a ZIP file.

Figure 355 cfgwriter Utility



The following XML file is used in this deployment to program the IR510 Gateway:

```
========================IR510.xml================================
<DevCfgSchema>
<Ieee_Cfg>
<SSID>adaptive</SSID>
<SecurityMode>1</SecurityMode>
<Ieee8021xAuthIntervalMax>120</Ieee8021xAuthIntervalMax>
<Ieee8021xAuthIntervalMin>60</Ieee8021xAuthIntervalMin>
<Ieee802154Mode>2</Ieee802154Mode>
<Ieee802154TxPwr>10</Ieee802154TxPwr>
<Ieee802154Dwell>
<window>12400</window>
<maxdwell>400</maxdwell>
</Ieee802154Dwell>
<Ieee802154PhyMode>166</Ieee802154PhyMode>
</Ieee_Cfg>
<Csmp_Cfg>
<RegIntervalMax>3600</RegIntervalMax>
<RegIntervalMin>300</RegIntervalMin>
<ReqSignedPost>true</ReqSignedPost>
```

```
<ReqValidCheckPost>true</ReqValidCheckPost>
<ReqTimeSyncPost>false</ReqTimeSyncPost>
<ReqSecLocalPost>false</ReqSecLocalPost>
<ReqSignedResp>true</ReqSignedResp>
<ReqValidCheckResp>true</ReqValidCheckResp>
<ReqTimeSyncResp>false</ReqTimeSyncResp>
<ReqSecLocalResp>false</ReqSecLocalResp>
</Csmp_Cfg>
<NetworkScale_Cfg>
<NetworkScale>small</NetworkScale>
</NetworkScale_Cfg>
</DevCfgSchema>
=========================================================
```

Note: In the above schema, phy mode 166 refers to adaptive modulation (discussed later) with a data rate of 600kb/s. Text in bold in the XML configuration represents mandatory configuration parameters.

The cfgwriter utility converts the input XML file into a binary format (.bin) output. Successful execution of the cfgwriter utility with the XML file and necessary certificates as input will return a “0” numeric code to Standard Output (stdout).

From the command prompt on a Windows PC, navigate to the folder where the cfgwriter utility and all the necessary certificates described in Table 30 are placed.

The following is the command syntax used to generate the config (.bin) file needed to program the IR510 node:

```
java -jar cfgwriter-6.0.20.jar -x <IR510.pfx> -p <password> -ca <CAcert.cer> -w <config.xml> --nmscert
<csmpcert.cer> <outputfile.bin>
```

The command line parameters used in the above command are described in Table 30.

Table 30 cfgwriter Utility Command Syntax Parameter Options

Parameter	Description
-x <IR510.pfxfile>	IR510 Cert & Private Key file in PKCS12(.pfx) format to be created and exported from the ECC CA server.
-p <password>	Password provided while exporting the IR510 (.pfx) certificate from the ECC CA Server
-ca <CAcert.cerfile>	Trusted ECC CA public Cert (DER encoded) to be installed on the IR510.
-w <config.xmlfile>	XML config file of the IR510 used to generate the corresponding binary .bin file
--nmscert <csmpcert.cerfile>	The .pem file certificate downloaded from IoT FND GUI in binary format (with extension changed to .cer) for mutual validation of csmp communication messages between IR510 and IoT FND.
<outputfile.bin>	Output bin file generated after successful execution of the specified command. A numeric code of “0 (zero)” seen on the standard output means command was successfully executed. This is the same config bin file which is used to program the IR510 later.

Figure 356 shows a sample command issued to generate the .bin file needed for IR510 programming.

Figure 356 Bin File Generation

Bin File Programming

The binary configuration file (.bin) prepared in the previous step, along with the correct firmware, is programmed into the IR510 node using another utility known as HostOne tool (fwubl). This tool is also placed on the same Windows machine where the cfgwriter utility was placed.

Note: To obtain the HostOne (fwubl) tool discussed below, check with your account team or sales representative.

From the same Windows machine, connect to the IR510 console port using an USB to serial converter connected through a Cisco RJ45 to DB9 (female) blue serial console cable. From the command prompt on Windows PC, navigate to the folder where the fwubl tool is placed along with the firmware image and configuration bin files of the IR510.

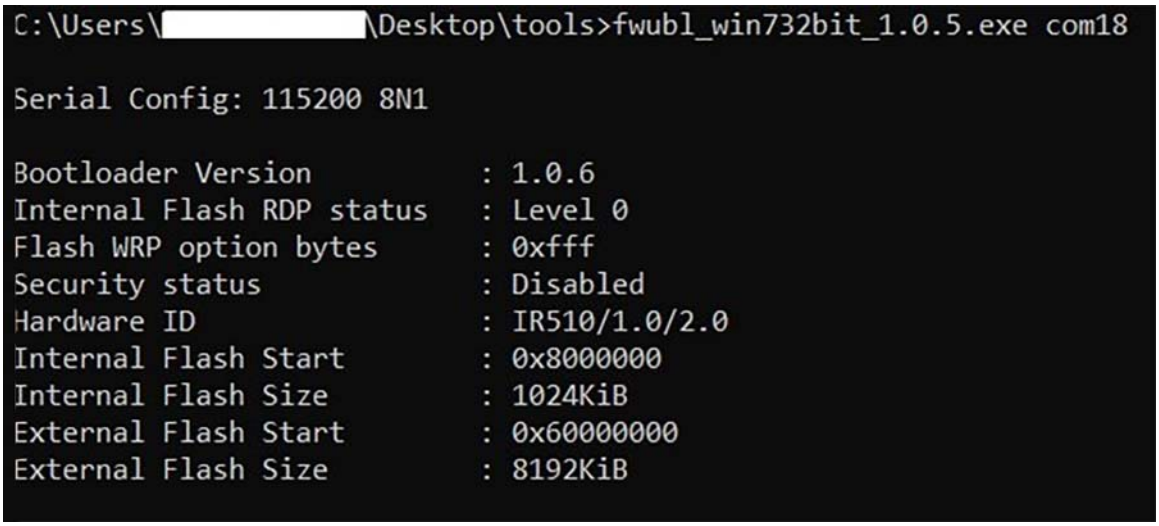
Note: Do not power on the IR510 unit without any attenuators, antenna, or RF cabling in place. It is highly recommended to keep the RF port on the node always connected; do not leave it to transmit in free air since without the right connector/RF cables, the radio has a high likelihood of becoming damaged.

Once the node is powered on, issue the following command to verify that the node is in bootloader mode first. If it is not, power cycle the node and check again as it would re-enter into the bootloader mode.

```
fwubl_win732bit_1.0.5.exe com<port>
```

The output from this command shows the current bootloader version on the node and a few other parameters. Figure 357 shows the sample output of an IR510 unit initially in bootloader mode.

Figure 357 IR510 in Bootloader State

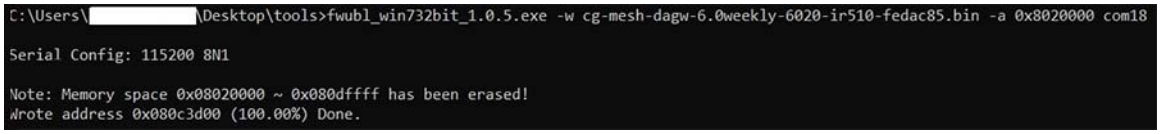


The next step is to program the firmware version on the IR510 into the memory location specified in the following command:

```
fwubl_win732bit_1.0.5.exe -w <IR510 firmware.bin> -a 0x8020000 com<port>
```

Figure 358 shows the sample output of firmware push issued to an IR510 unit.

Figure 358 Firmware Push on IR510



The next step is to program the configuration .bin file generated for the IR510 into the memory location specified in the following command:

```
fwubl_win732bit_1.0.5.exe -w <IR510 config.bin> -a 0x80E0000 com<port>
```

Figure 359 shows the sample output of the configuration bin push issued to an IR510.

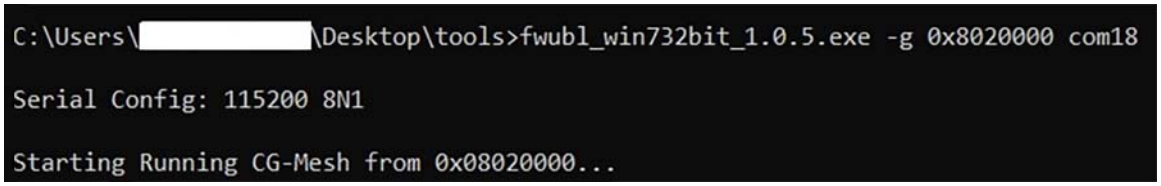
Figure 359 Config Bin Push on IR510

The final step is to enable CR Mesh on IR510 by bringing it out of bootloader mode by issuing the following command:

```
fwubl_win732bit_1.0.5.exe -g 0x8020000 com<port>
```

Figure 360 shows the sample output to run CG-mesh software on the IR510.

Figure 360 CR Mesh Enabled on IR510



Secure Onboarding of Mesh Nodes into CR Mesh

Staging, page 440 provided details on how to set up an IR510 Gateway to securely join the mesh network. This section discusses the components needed to enable secure onboarding of IR510 into the mesh network.

CR Mesh Endpoint—Authentication Call Flow

The FAR router provides security services such as 802.1x port-based authentication, encryption, and routing to provide a secure connection for the mesh endpoint all the way to the control center. IEEE 802.1x using X.509 certificates is the process used to securely authenticate a mesh node before allowing it to join the PAN or to even send packets into the network.

CR Mesh Endpoint Onboarding—Associated Touchpoints in the Headend

Table 31 lists the associated touchpoints that should be set up and configured as a prerequisite step before enabling secure onboarding process of mesh nodes.

Table 31 Associated Configuration Touchpoints at Different Places in the Solution

Associated Configuration Touchpoints	Purpose	Reference Link for Configuration
ECC CA Server	Issuing ECC type certificates for mesh end points and AAA server	Refer to ECC Certificate Authority Installation, page 178 for installing ECC CA server and configuring Radius server and Active Directory.
IoT FND	Obtaining CSMP certificate from IoT FND to program mesh nodes	Browse to point 8 referring to the “Certificates for CSMP tab” in “Configuring a Custom CA for SSM” at the following URL: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/install/4_2/iot_fnd_install_4_2.pdf Click the radio button showing the binary option and download the .pem binary certificate (manually change extension to .cer for programming into the IR510).

Associated CGR Configurations for Onboarding of the Cisco WPAN Industrial Router–IR510

Note: The following configurations are for reference purposes only. They would be dynamically provisioned by the FND CGR.

WPAN Configuration on CGR to Enable Secure Mesh

The following is the sample configuration of a CGR1240 for the WPAN interface. Note that the SSID configured on the WPAN interface below matches what was configured in the IR510 XML schema shown in an earlier section.

```
CGR1240_JAD20410B2Z#sh run int wpan 4/1
interface Wpan4/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 load-interval 30
 ieee154 phy-mode 166 165 164 2
 ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
 ieee154 dwell window 12400 max-dwell 400
 ieee154 panid 420
 ieee154 ssid adaptive
 ieee154 txpower 25
 ieee154 beacon-ver-incr-time 15
 outage-server 2001:DB8:16:110::151
 rpl dag-lifetime 60
 rpl dio-dbl 2
 rpl dio-min 14
 rpl version-incr-time 10
 authentication host-mode multi-auth
 authentication port-control auto
 ipv6 address 2001:DB8:ABCD:1::1/64
 ipv6 enable
 ipv6 dhcp server dhcpd6-pool rapid-commit
 no ipv6 pim
 dot1x pae authenticator
 mesh-security mesh-key lifetime 259200
end
```

AAA RADIUS Client Configuration on CGR

The following is the RADIUS client configuration needed on CGR1240 for enabling dot1x authentication of the mesh endpoint with the AAA server:

```
CGR1240_JAD20410B2Z#
!
aaa new-model
!
aaa group server radius ms-aaa server name aaa_server
!
radius server aaa_server
address ipv4 172.16.106.175 auth-port 1812 acct-port 1813 key <secret key>
!
aaa authentication dot1x default group ms-aaa
!
dot1x system-auth-control
!
```

Note: The secret key above configured on the CGR must match the secret key configured on NPS on ECC when adding CGR as a radius client.

Mesh Key Configuration on CGR

FAR is provisioned with a mesh key pushed from FND that is used to provide link layer encryption for the communication between the IR510 and the FAR.

The following command is used to verify if the key is indeed present on the CGR:

```
CGR1240_JAD20410B2Z#sh mesh-security keys Mesh Interface: Wpan4/1

Master Key Lifetime: 120 Days 0 Hours 0 Minutes 0 Seconds
Temporal Key Lifetime: 60 Days 0 Hours 0 Minutes 0 Seconds
Mesh Key Lifetime: 30 Days 0 Hours 0 Minutes 0 Seconds

Key ID: 0 *
Key expiry: Fri Feb 8 20:34:24 2019
Time remaining: 4 Days 0 Hours 51 Minutes 30 Seconds
Frame Counter: 200000 CGR1240_JAD20410B2Z#
```

DHCPv6 Server Configuration on CGR for Address Allocation

The CR Mesh nodes need to be assigned an IPv6 address for reachability from the CGR as well as from the control center. For this purpose, an IPv6 DHCP pool is configured on the CGR as shown below. However, a central DHCP server option, if available is recommended.

```
!
ipv6 dhcp pool dhcpd6-pool
address prefix 2001:DB8:ABCD:1::/64 lifetime infinite infinite vendor-specific 26484
suboption 1 address 2001:DB8:16:103::243 << FND IP Address
!
```

From the above mesh prefix, the first address 2001:DB8: ABCD:1::1/64 is assigned to the CGR WPAN interface while the mesh nodes are allocated an IPv6 address from the remaining pool. The sub-option 1 address specifies the IPv6 address of the IoT FND to the mesh nodes.

If CPNR is used as DHCP Server, the user needs to configure Relay Agent configuration on CGR to get the IPv6 addresses for Mesh Nodes.

```
cgr1000_wpanmodule(config-if)# ipv6 dhcp relay destination 2001:DB8:16:108::100
```

Note: Refer to Implementing Headend Network, page 176 for the complete configuration of CGR tested to bring up the CR Mesh.

MAP-T Infrastructure in CCI SCADA

Basic Overview of MAP-T

MAP-T refers to address and port mapping using a translation mechanism and is used to provide connectivity to IPv4 hosts over IPv6 domains by performing double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers.

A MAP-T domain comprises one or more MAP CE devices (IR510) and a border relay router (HER), all of which are connected to the same IPv6 network.

For a MAP-T domain to be operational, mapping rules known as basic mapping rules (BMR) and a default mapping rule (DMR) must be configured. While BMR is configured for the MAP IPv6 source address prefix, DMR is used to map IPv4 information to IPv6 addresses for destinations outside a MAP-T domain. Some port parameters like share-ratio and start-port are also configured for the MAP-T BMR whereas EA bits refer to the IPv4 embedded address bits within the MAP-T IPv6 address identifier of the MAP-T CPE.

For more details on MAP-T, refer to “Mapping of Address and Port Using Translation” at the following URL:

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/nat-xe-3s-book/ip-nat-divi-v4v6.html

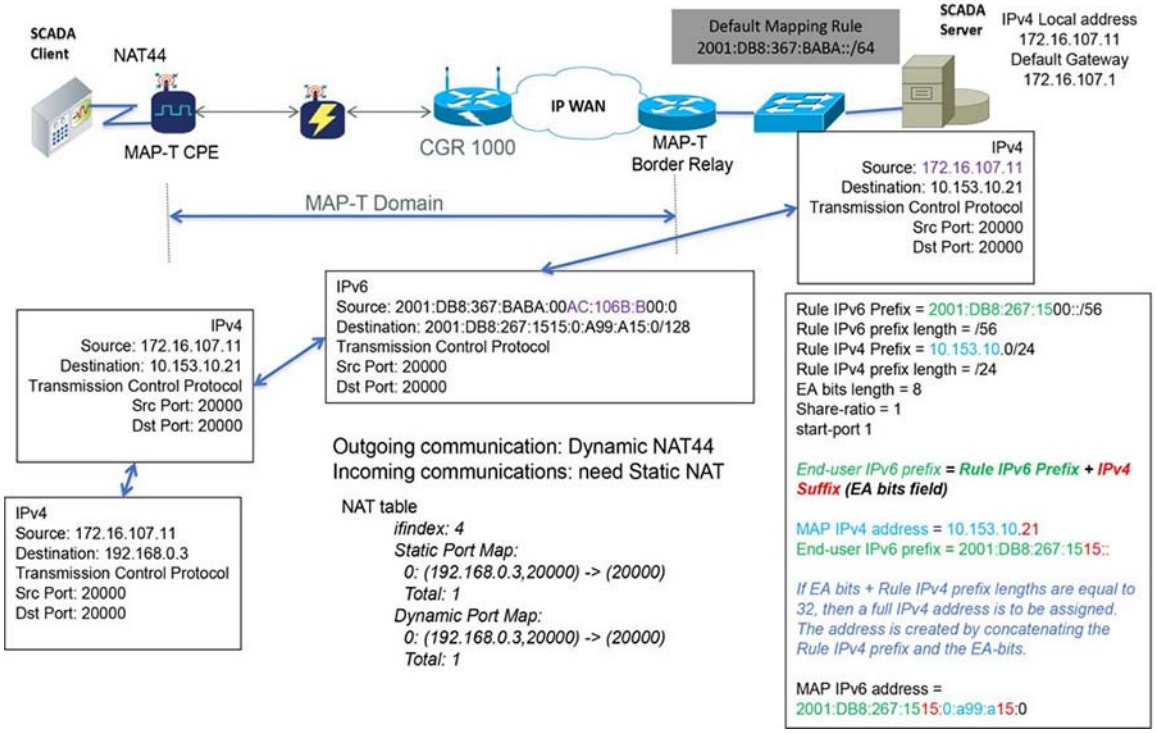
Packet Flow in MAP-T Network

The following is the logical packet flow between a SCADA client and the SCADA Primary/Subordinate:

SCADA Client --> IPv4 --> IR510 --> IPv6 --> CGR --> IPv6 --> HER --> IPv4 --> SCADA Primary/Subordinate

An actual sample packet flow, including MAP-T parameters like BMR and DMR used in this implementation, is illustrated in Figure 361.

Figure 361 MAP-T Packet Flow



While configuring MAP-T, the DMR prefix, the IPv6 user prefix, and the IPv6 prefix plus the embedded address (EA) bits must be less than or equal to 64 bits.

Note: MAP-T parameters like the BMR IPv6 prefix and associated prefix length unique to each node are configured as part of the .csv file uploaded to IoT FND whereas the DMR IPv6 and the BMR IPv4 prefixes and their associated lengths along with EA bit length are configured via the configuration template in IoT FND which is later applied to the nodes, as shown in Configuration Options from FND, page 449.

Map-T Points in the Network

IR510–MAP-T CE

A MAP-T CE device connects a user's private IPv4 address and the native IPv6 network to the IPv6-only MAP-T domain by first doing a NAT44 translation from the private to public (inside to outside) address within the v4 domain and then subsequently doing a v4 to v6 translation.

MAP-T BMR Prefix Selection for IR510.csv

The BMR prefix is used by the MAP-T CE to configure itself with an IPv4 address, an IPv4 prefix from an IPv6 prefix. As shown in Figure 361, the Rule IPv6 prefix represents the BMR IPv6 prefix used in the MAP-T network. As such, the BMR IPv6 prefix of 2001:DB8:267:1515::/56 corresponds to the MAP-T IPv4 address of 10.153.10.21 of an IR510 node.

HER–MAP-T Border Relay Router

The following configuration is needed on the HER to enable MAP-T border relay functionality:

```
FAN-PHE-HER#
!
nat64 settings fragmentation header disable nat64 map-t domain 1
default-mapping-rule 2001:DB8:367:BABA::/64 basic-mapping-rule
ipv6-prefix 2001:DB8:267:1500::/56 ipv4-prefix 10.153.10.0/24
port-parameters share-ratio 1 start-port 1
!
```

Additionally, the CLI command nat64 enable needs to be enabled as shown below on the HER interfaces participating in the MAP-T translations (such as the interface where the SCADA Primary/Subordinate connects and the tunnel interface towards CGR).

The HER interface connecting to the control center side where SCADA Primary/Subordinate resides is IPv4 based whereas the virtual-template interface of the HER connecting to the CGR on the WAN side is IPv6 based, as shown logically below:

CGR --> IPv6 --> (VTI) HER (Gig port) --> IPv4 --> SCADA Primary/Subordinate

Enabling nat64 on the SCADA Primary/Subordinate-facing Interface of the HER Shown Below

```
!
interface GigabitEthernet0/0/1 description to-SCADA-Master
ip address 10.40.100.101 255.255.255.0
standby version 2
standby 107 ip 10.40.100.100
standby 107 priority 253
standby 107 preempt
standby 107 name SCADA_MASTER1
nat64 enable
!
```

Enabling nat64 on the FAR-facing Virtual-Template Interface of HER Shown Below

```
!
interface Virtual-Template1 type tunnel ip unnumbered Loopback0
ip nhrp network-id 1 ip nhrp redirect nat64 enable
ipv6 unnumbered Loopback0 ipv6 enable
!
```

Configuration Options from FND

Csv File Import at FND

The following template can be used to add mesh endpoints to the FND database.

```
eid,deviceType,function,enduseripv6prefix,bmripv6prefixlen
```

These fields are explained in Table 32.

Table 32 Parameters of IR500.csv File

Parameter	Description
Eid	A Unique Element identifier to identify the device in log messages as well as in the IoT FND GUI.
deviceType	Used to identify the hardware platform.
Function	Used to identify the functionality of IR510 (i.e., SCADA Gateway).
enduseripv6prefix	The BMR IPv6 prefix unique to each mesh endpoint.
bmripv6prefixlen	The BMR IPv6 prefix length assigned to the mesh endpoint.

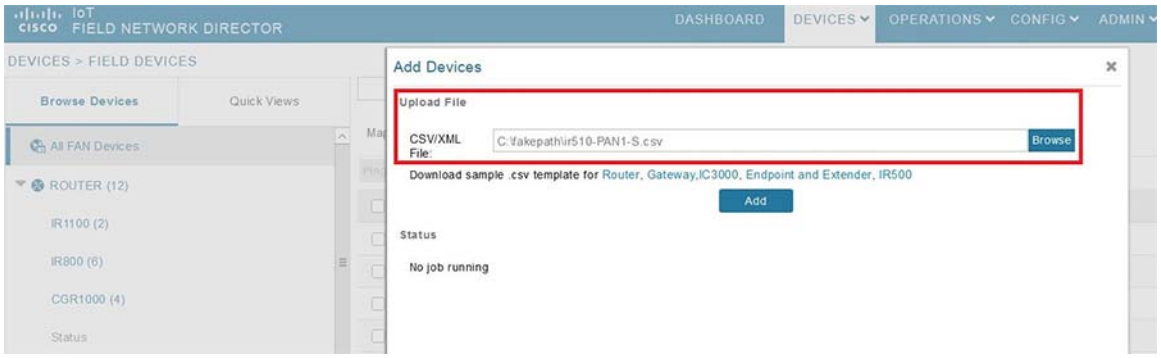
The following are the contents of a sample csv file used in this implementation:

```
eid,deviceType,function,enduseripv6prefix,bmripv6prefixlen
2ED02DFFFE6E0F03,ir500,gateway,2001:db8:267:1515::,56
2ED02DFFFE6E0F0B,ir500,gateway,2001:db8:267:1516::,56
```

```
2ED02DFFFE6E0F05,ir500,gateway,2001:db8:267:1517::,56
2ED02DFFFE6E0F27,ir500,gateway,2001:db8:267:1518::,56
2ED02DFFFE6E0F2D,ir500,gateway,2001:db8:267:1519::,56
2CD02D10006E0F4E,ir500,gateway,2001:db8:267:151A::,56
```

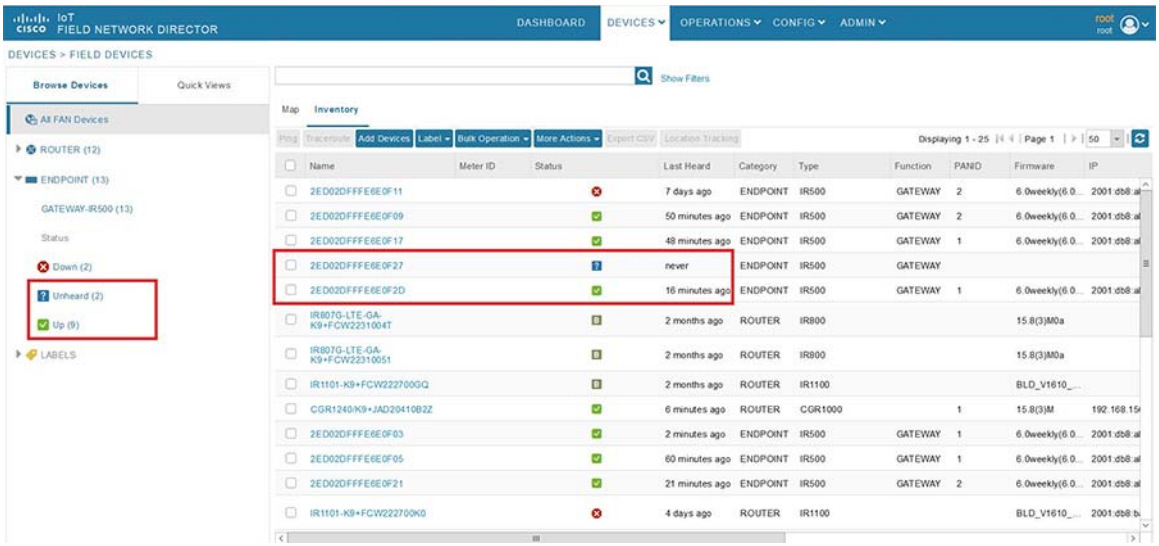
1. To upload the CSV file into IoT FND, navigate to the GUI.
2. From **Inventory tab -> Devices -> Field Devices -> Add Devices**, click **Browse** to upload the file as shown in Figure 362.
3. Click **Add**.

Figure 362 CSV File Upload to IoT FND



Once added, the devices will initially be in Unheard state. Once mesh nodes start registering with the FND, their device status turns green as shown in Figure 363.

Figure 363 Mesh Endpoint Status in FND



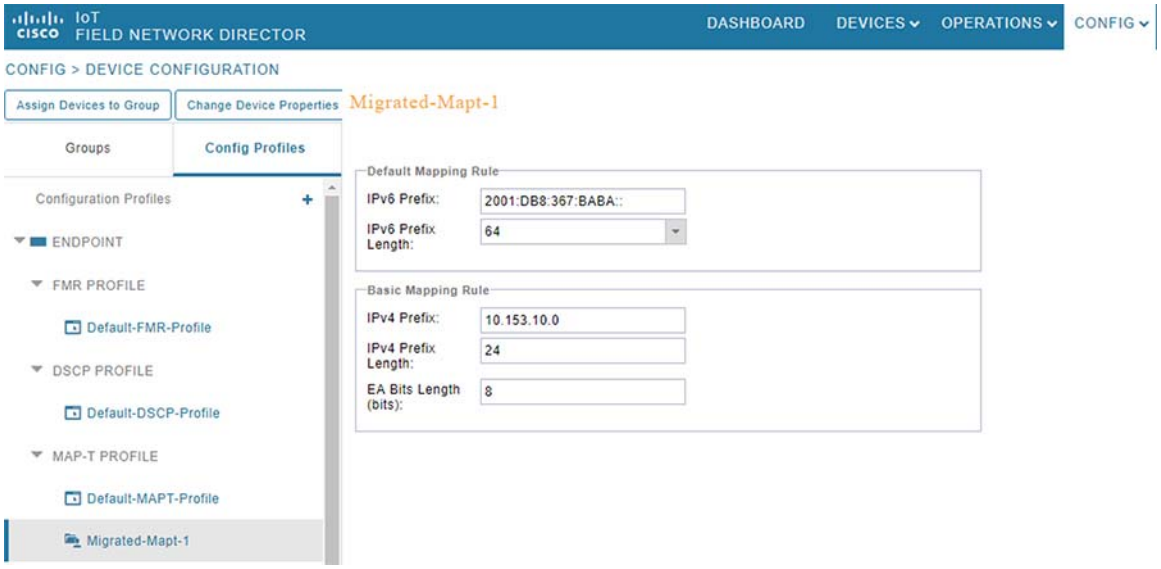
The nodes must register successfully with IoT FND before other settings like MAP-T, NAT44, and other serial configuration profiles be properly pushed/applied to the nodes. However, if those settings are pre-linked via the default profiles, the configuration would be automatically pushed to the nodes upon device registration.

Creation of MAP-T Group

1. To configure the MAP-T settings in FND, navigate to **Config -> Device Configuration**.
2. Under **Config Profiles**, click the **Add Profile** icon (**+**).

3. Create a new MAP-T profile with the correct settings for BMR and DMR rules, as shown in Figure 364.

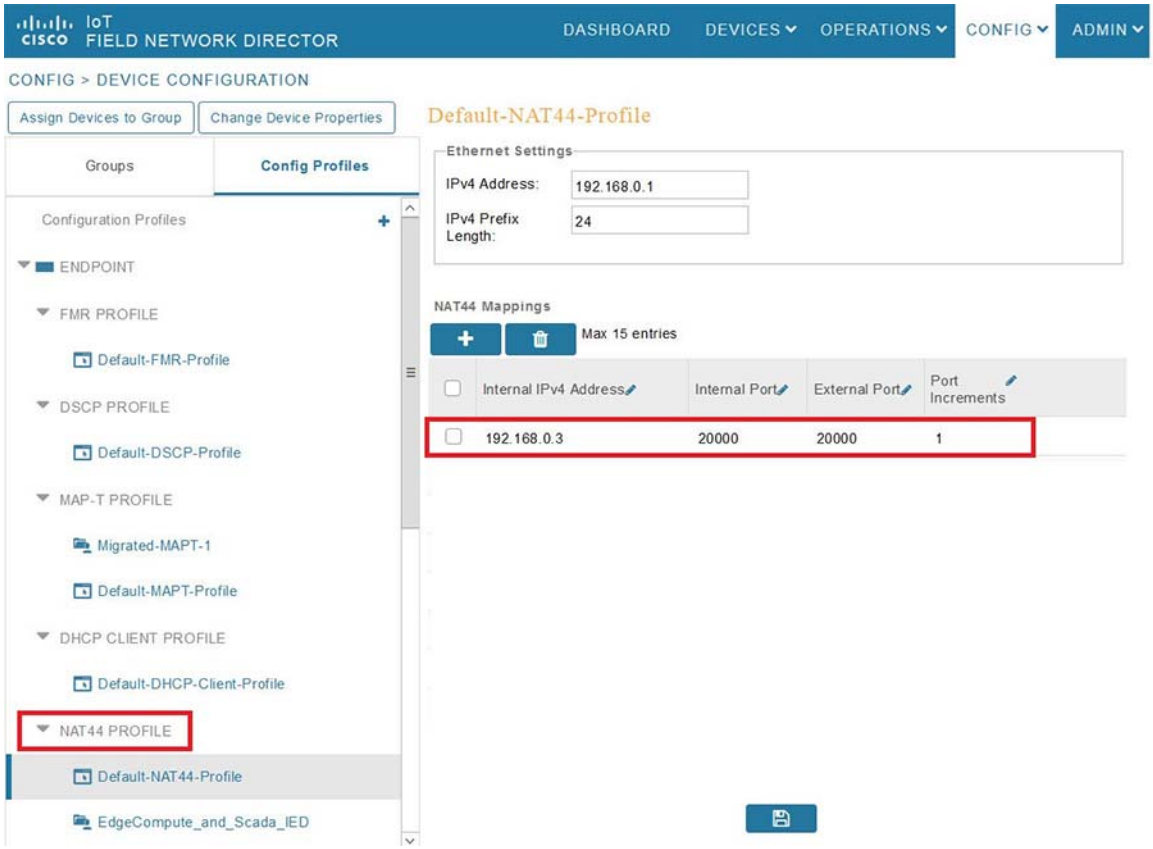
Figure 364 Creating MAP-T Profile



Creation of NAT44 Group on FND

1. To configure the NAT44 settings for mesh endpoints in FND, navigate to **Config Profiles -> Config -> Device Configuration**.
2. Click the **Add Profile** icon (**+**).
3. Create a new NAT44 profile with the correct Internal IPv4 address, internal, and external ports, as shown in Figure 365.

Figure 365 Creating a NAT44 Profile



In Figure 365, the IPv4 address and prefix length of the IR510 are specified under **Ethernet Settings**.

The Internal IPv4 address refers to the internal address of the NAT44-configured device like the SCADA client, which is connected behind IR510. The internal port refers to the internal port number on which the SCADA client would be listening. The external port refers to the external port number of the SCADA client accessed by devices from outside MAP-T domain.

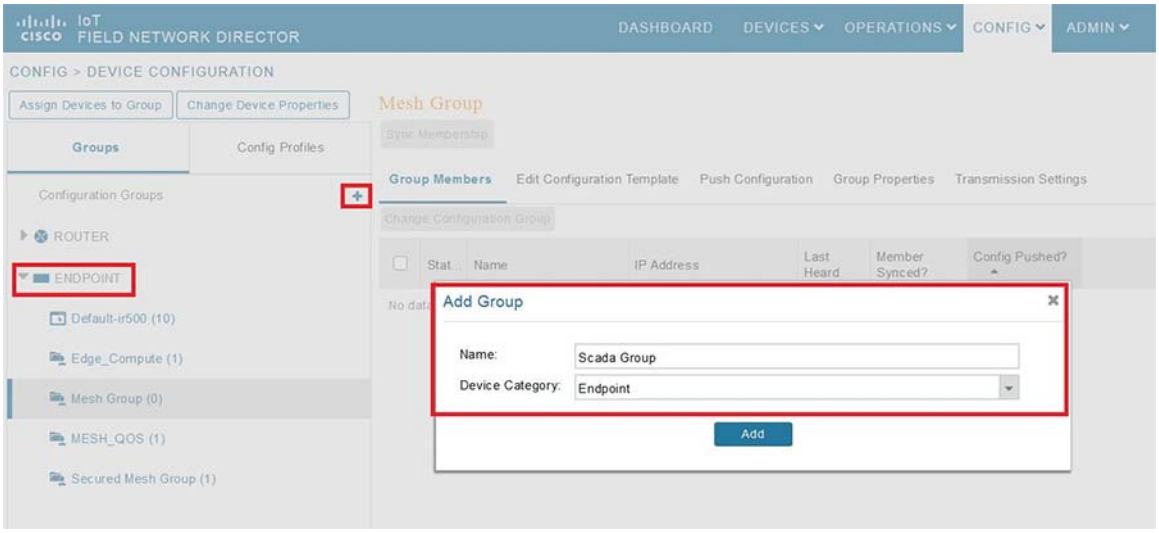
Note: Since 192.168.0.2 is reserved for the Guest OS inside the IOX portion of the IR510 unit, it is recommended to use a different address such as 192.168.0.3 for the SCADA client and, accordingly, multiple NAT44 mappings like the one shown above could be created for different ports.

Creation of Configuration Group on FND

Initially all the IR510s added to the FND are placed in the Default-IR500 group. Depending on the deployment, some of them can be moved to a newly created configuration group in which the corresponding MAP-T, NAT44 profiles can be selectively applied and a configuration pushed to these nodes.

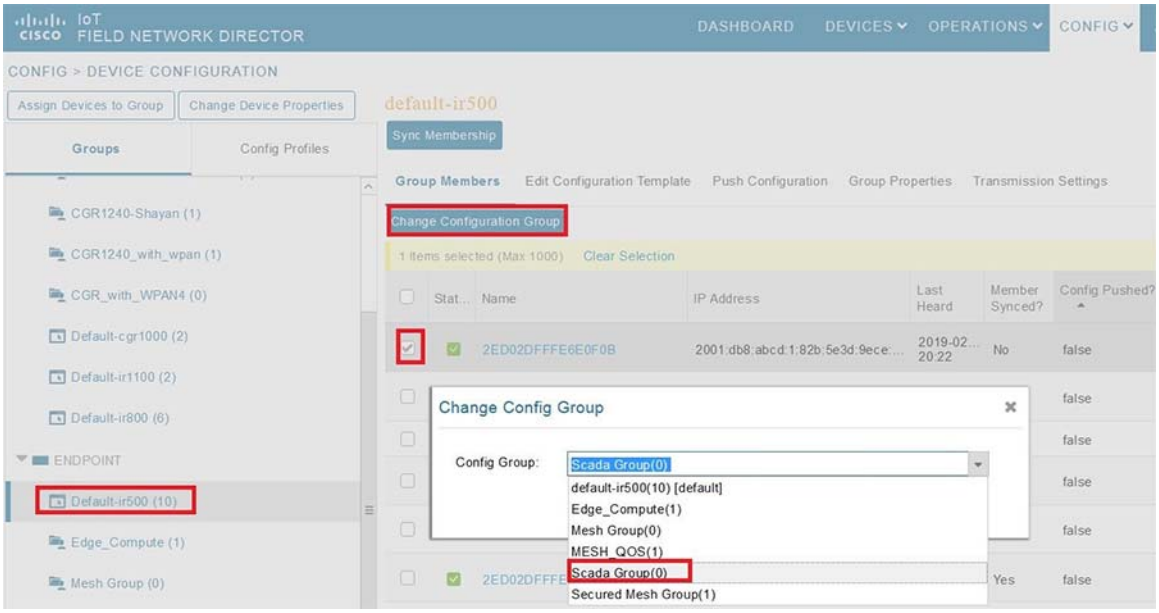
1. To create a configuration group, navigate to the **Groups tab -> Config -> Device Configuration**.
2. Click the **Add Group** icon (**+**).
3. Then create a new group of type Endpoint as shown in Figure 366.

Figure 366 Creating an Endpoint Configuration Group



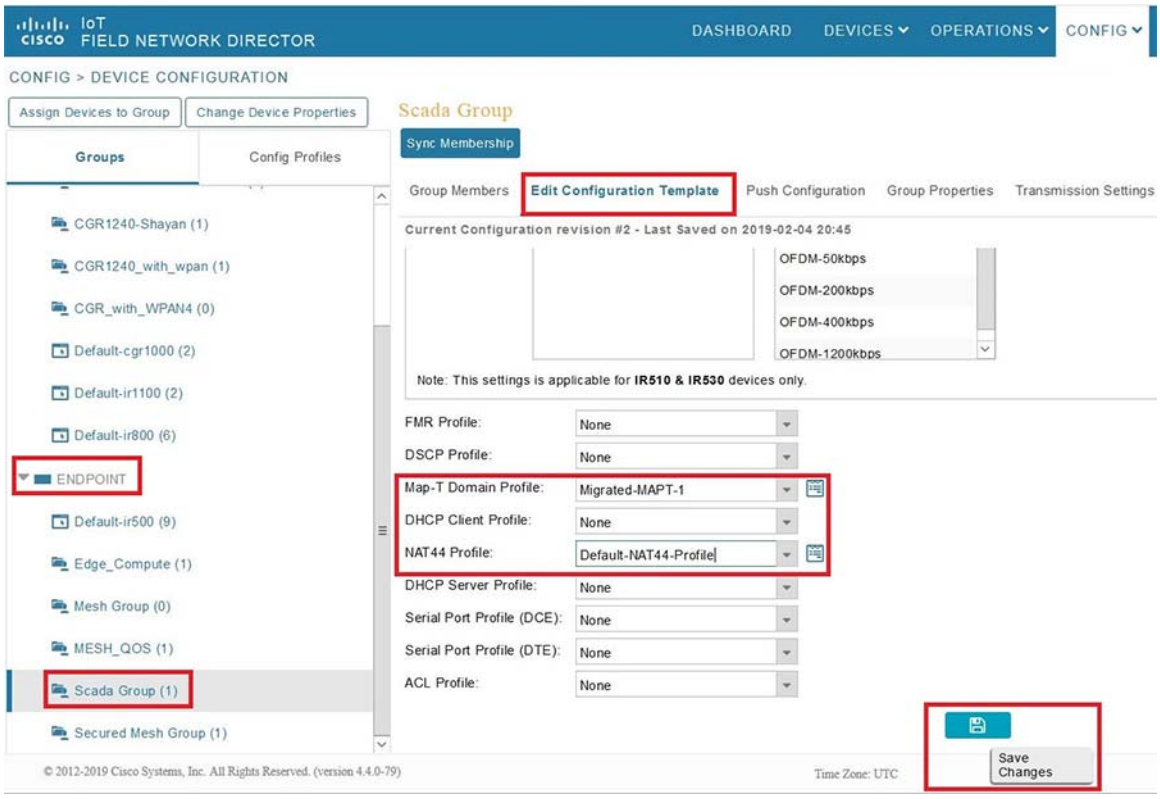
4. Move some of the mesh nodes from the default endpoint group to the newly created group based on the deployment.
5. Navigate to the default endpoint group, select the nodes of interest, and click **Change Configuration Group**.
6. Then select the newly created configuration group in the drop-down menu as shown in Figure 367.

Figure 367 Moving IR510 to the New Configuration Group



7. Once devices are moved to the newly created configuration group, from the **Edit** configuration template, select the MAP-T and NAT44 profiles created earlier.
8. Click **Save Changes** for these settings to be applied to the devices part of this group, as shown in Figure 368.

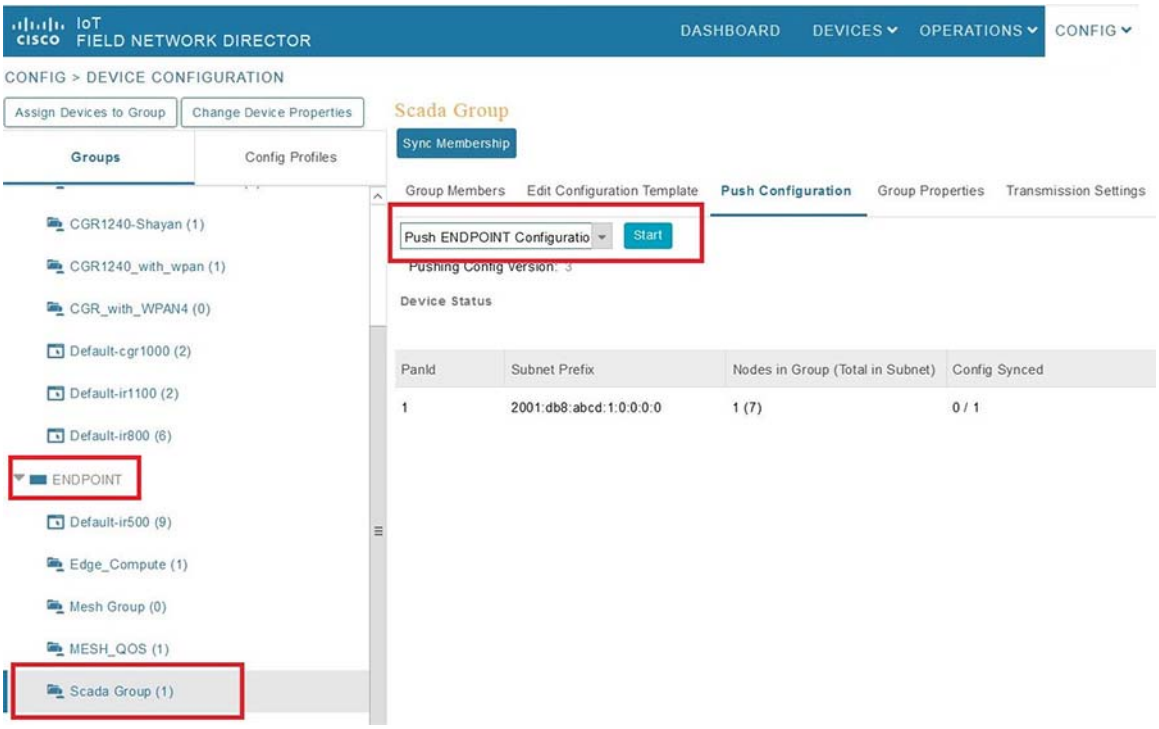
Figure 368 Editing the Configuration Template



9. Finally, push the configuration to the devices in this group by navigating to the **Push Configuration** tab and select **Push Endpoint Configuration**.

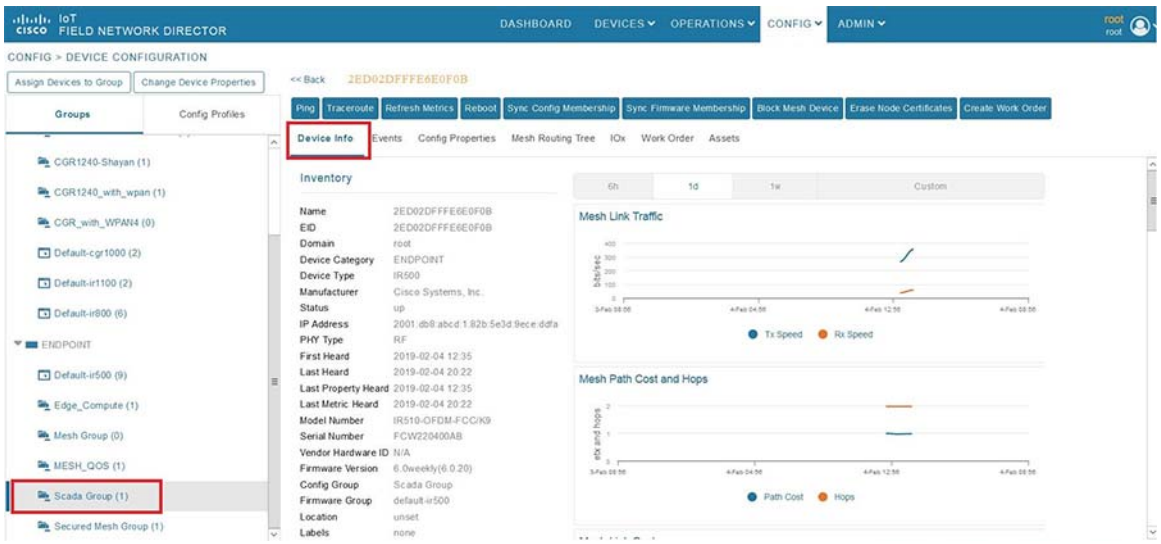
10. Click **Start** as shown in Figure 369. This completes the configuration settings from FND to the mesh node that are needed to operate as a SCADA gateway.

Figure 369 SCADA Configuration Push



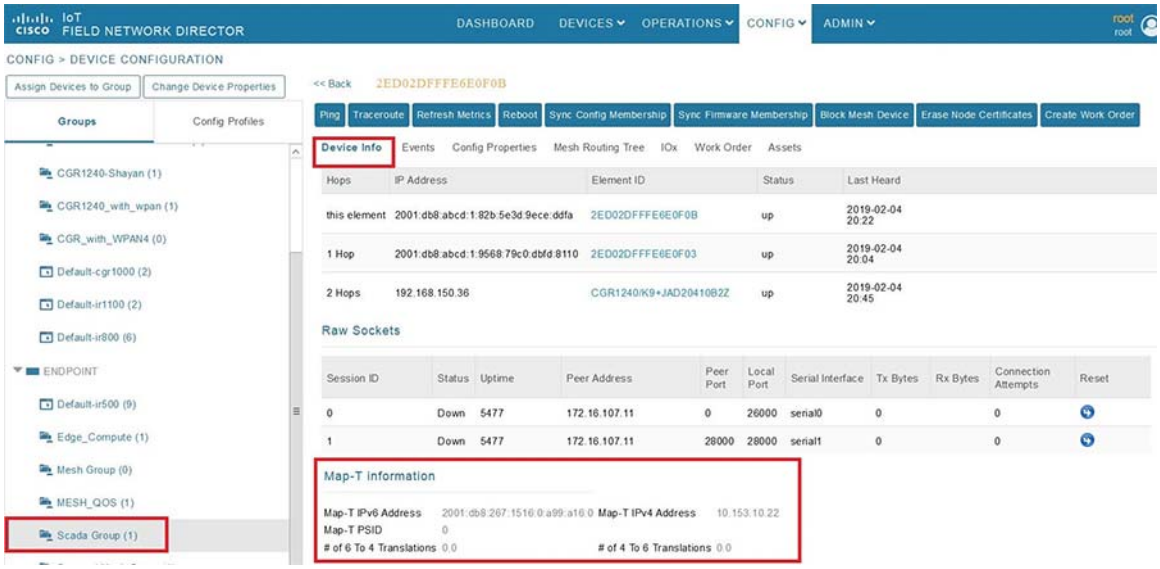
11. The final step is to verify that all the configuration settings are properly applied to the IR510. Click on the node inside the configuration group and navigate to the **Device Info** tab, as shown in Figure 370.

Figure 370 Verify Configuration Settings on IR510–1



12. On scrolling further down, the MAP-T settings applied to the device can be verified, as shown in Figure 371.

Figure 371 Verify Configuration Settings on IR510–2



Routing Advertisements from FAR to HER

Note: HER advertises a default route to all the FARs in order to provide connectivity to control center components.

Deployment of Cisco IoT Gateway

Advertising Summary Route of LoWPAN Prefix

Once the CR Mesh has been formed, the IR510 Gateways have reachability only to the FAR. The mesh nodes need a way to communicate all the way to control center components like IoT FND for management purposes. To achieve this, the IPv6 LoWPAN address subnet assigned to the mesh endpoints is advertised to the HER (which has reachability to the control center components) using the IKEv2 prefix injection over the FlexVPN tunnel. Specifically, the mesh prefix is advertised as part of the IPv6 ACL, which is part of the FlexVPN authorization policy as shown below.

Note: The configuration shown below is for reference purposes only since ZTD addresses it.

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy route set interface
route set access-list FlexVPN_Client_IPv4_LAN
route set access-list ipv6 FlexVPN_Client_IPv6_LAN
route redistribute connected route-map snapshot
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
permit ipv6 2001:DB8:ABCD:1::/64 any' Mesh IPv6 LoWPAN prefix!
!
```

Advertising MAP-T BMR IPv6 Prefix Using Snapshot Routing

As discussed above, besides advertising the Mesh LoWPAN prefix of the IR510 to the HER, even the MAP-T BMR IPv6 prefix of the nodes needs to be reachable from the control center to communicate with the SCADA clients connected to the IR510. To achieve this, the IKEv2 snapshot routing feature is implemented wherein the BMR IPv6 prefix assigned to the mesh endpoints is included in the route map redistributed inside the FlexVPN authorization policy, as shown below.

Note: Basically, the BMR IPv6 /128 address of the nodes that appear/disappear from the HER routing table are the ones that match the route-map snapshot shown below.

```
!
crypto ikev2 authorization policy FlexVPN_Author_Policy route set interface
route set access-list FlexVPN_Client_IPv4_LAN route set access-list ipv6 FlexVPN_Client_IPv6_LAN route
redistribute connected route-map snapshot
!
route-map snapshot permit 10 match ipv6 route-source snapshot set tag 10
!
ipv6 access-list snapshot
permit ipv6 2001:DB8:267:1500::/56 any' BMR IPv6 prefix!
```

SCADA Communication Protocols

This implementation focuses on DNP3 and MODBUS as SCADA communication protocols with serial and IP-based connectivity. Application traffic enablement of SCADA control center to SCADA Remote Devices (PLC/RTU) requires routing, raw socket configuration, and Ethernet based connectivity, which are key for application traffic flow.

The operations have been executed using a SCADA simulator known as the Distributed Test Manager (DTM), which has the capability of simulating both the SCADA control traffic and systems and the SCADA remote traffic and devices.

Table 33 SCADA Protocol Matrix

Transport Type	SCADA Control Center	SCADA Remote Systems
IP	DNP3 IP	DNP3 IP
Raw Socket	DNP3	DNP3
Protocol Translation	DNP3 IP	DNP3
IP	MODBUS IP	MODBUS IP
Raw Socket	MODBUS	MODBUS

Note: SCADA over CCI supports only Ethernet backhaul and protocols DNP3 IP, MODBUS IP are valid over here.

SCADA Operations

Operations that can be executed when the communication protocol is DNP3, DNP3 IP, DNP3-DNP3 IP translation are as follows:

- Poll–(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU))
- Control–(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU))
- Unsolicited Reporting–(SCADA Remote Device (PLC/RTU) > SCADA Primary/Subordinate) Notification from Client.

Operations that can be executed when the communication protocol is MODBUS IP, MODBUS Raw Socket are as follows:

- Read /Write Coil(s)–(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU))
- Read /Write Holding Register(s)–(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU))
- Read Discrete Input(s) and Input Register(s)–(SCADA Primary/Subordinate > SCADA Remote Device (PLC/RTU))

Table 34 SCADA Operations

Register References	Action	Description
0xxx	Read/Write	Coils Outputs
1xxx	Read	Discrete Inputs
3xxx	Read	Input Registers
4xxx	Read/Write	Holding Registers

This document focuses on SCADA protocols such as the MODBUS and DNP3 protocols.

Application Traffic Communication Enablement

This section includes the implementation of the following major topics:

- SCADA control center Point-to-Point Implementation Scenarios over Cellular Gateways.
- SCADA Communication with IP Intelligent Devices
- SCADA Communication Scenarios over CR Mesh Network (IEEE 802.15.4)
- SCADA Communication with Serial-based SCADA using Raw Socket TCP
- Legacy SCADA (Raw Socket TCP Server).
- SCADA Communication with CCI Network. [SCADA end point connected directly via Ethernet to CCI]

CCI Solution supports the SCADA service models shown in Table 35.

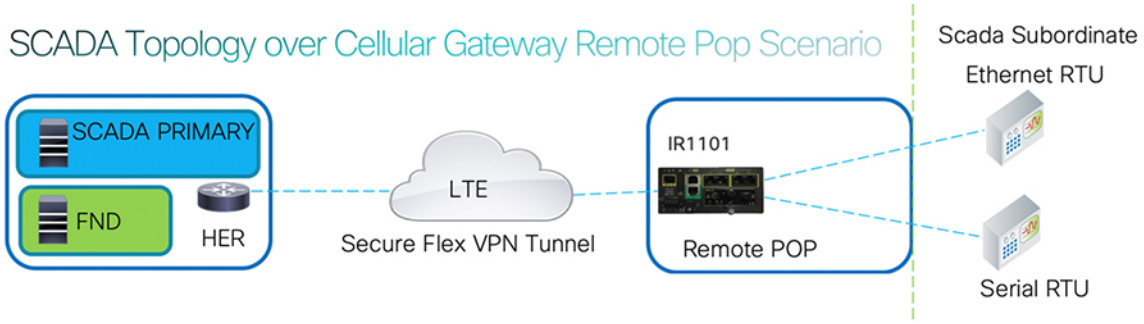
Table 35 SCADA Service Models

Service	Connectivity	Service Model
Legacy SCADA (DNP3)	Point-to-Point (Primary/Remote Device) Single Control Center	Raw Socket Over FlexVPN
SCADA Gateway (DNP3) to IP Conversion (DNP3-IP)	Point-to-Point (Primary/Remote Device) - Single Control Center	Protocol Translation over FlexVPN
SCADA (DNP3-IP)	Point-to-Point (Primary/Remote Device)- Single Control Center	FlexVPN - Single SCADA Primary/Subordinate
Legacy SCADA (MODBUS)	Point-to-Point (Primary/Remote Device)- Single Control Center	Raw Socket Over FlexVPN
SCADA (MODBUS-IP)	Point-to-Point (Primary/Remote Device)- Single Control Center	FlexVPN - Single SCADA Primary/Subordinate

SCADA Application Server Point-to-Point Implementation Scenarios Over Cellular Gateways

In this scenario, the Control Center will be hosting SCADA applications. The SCADA Remote Device (PLC/RTU) is connected to the Cellular SCADA Gateway (IR1101) via serial or Ethernet interface. The SCADA Primary/Subordinate residing in the Control Center can communicate with the end point using the DNP3 (IP/Serial) or MODBUS (IP/serial) protocol.

Figure 372 SCADA Topology over Cellular Gateway



This document focuses on SCADA protocols such as the DNP3 and MODBUS protocols.

IR1101 is implemented as Cellular SCADA Gateway. ASR 1000s/CSR1000v implemented act as a HER, which terminates FlexVPN tunnels from SCADA Gateways.

The following sections focus on:

- SCADA Communication with IP intelligent devices
- SCADA Communication with legacy devices
  - Raw Socket TCP
  - Protocol Translation (only for DNP3)

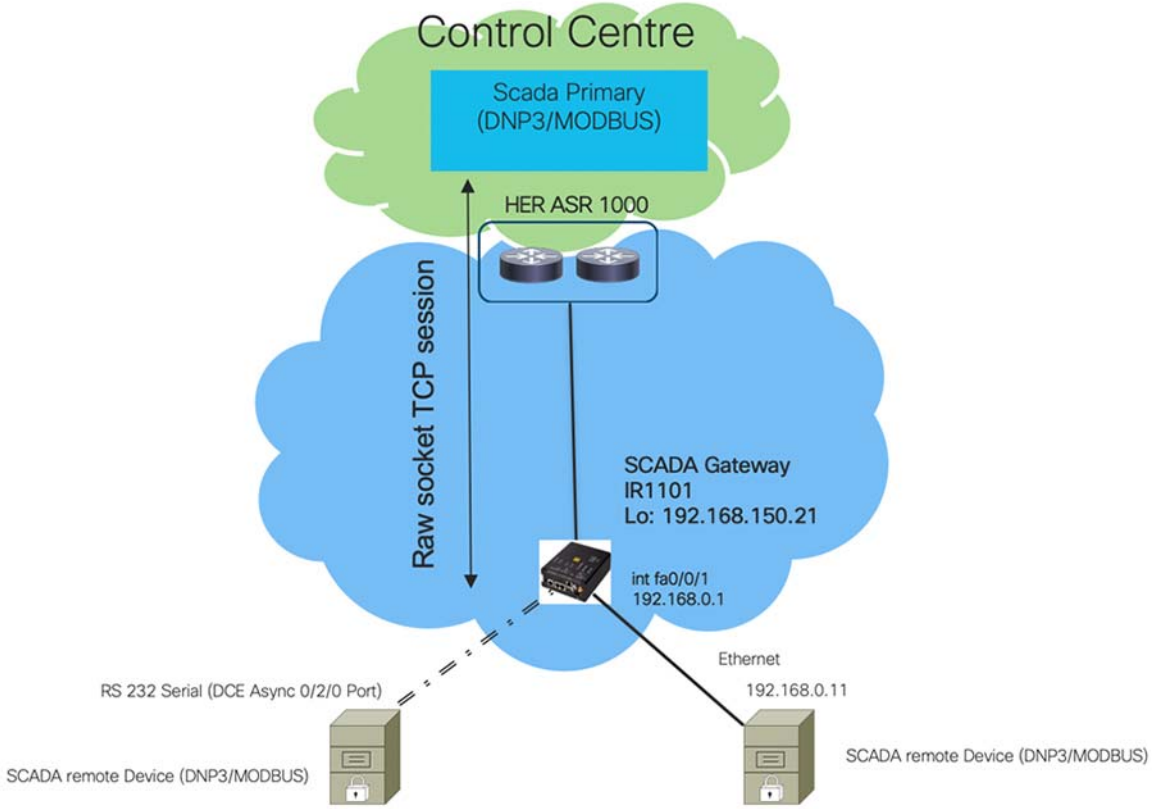
DNP3 and MODBUS Connectivity to SCADA Remote Devices (PLC/RTU)

- SCADA Remote Device (PLC/RTU) is connected to the SCADA Gateway via the Ethernet port, then it is pure IP traffic. The IP address of the SCADA Gateway can be NATed so that the same subnet between the SCADA Remote Device (PLC/RTU) and the Ethernet interface of the SCADA Gateway can be re-used. This approach will ease the deployment.
- If the SCADA Remote Device (PLC/RTU) is connected using asynchronous serial (RS-232 or RS-485):

  Gateway Tunnelled Raw Socket using DNP3 or MODBUS:

  - SCADA traffic at a remote site can be transmitted as RAW Socket or encapsulated into IP at a local gateway.
  - SCADA control server can consume as DNP3, DNP3/IP, or MODBUS communication directly.
  - SCADA Gateway in the control center can convert DNP3/MODBUS traffic back to Raw Socket.

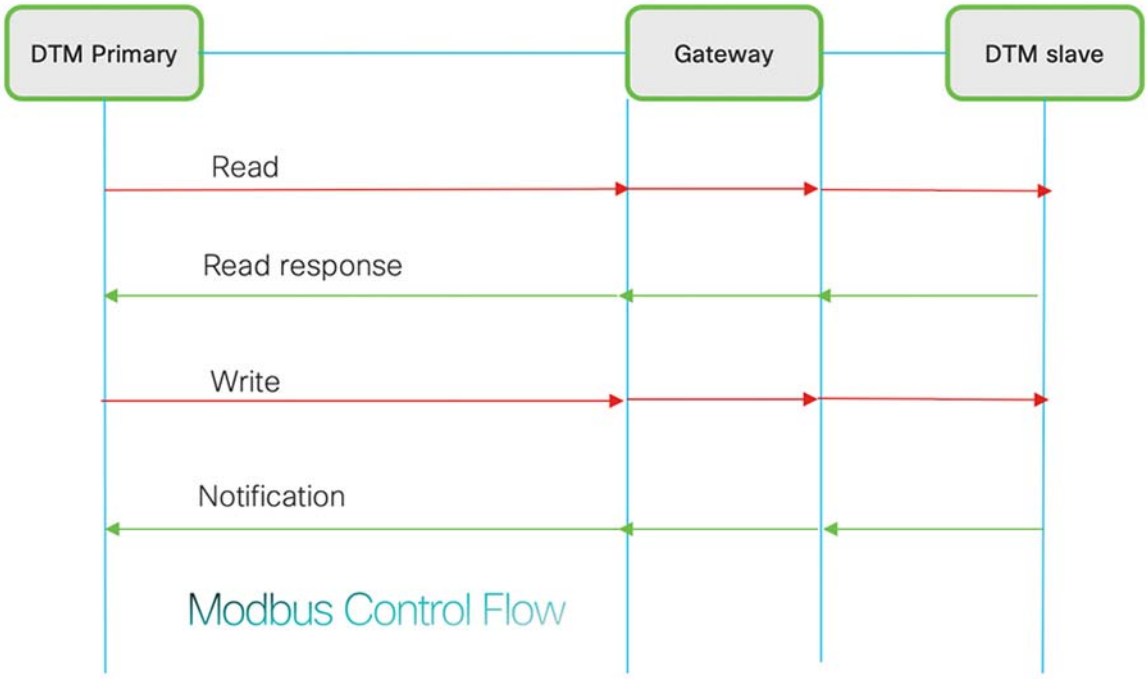
Figure 373 SCADA DNP3/MODBUS with IR1101



SCADA Communication with IP Intelligent Devices

- Protocol Validation—The protocol validated for this release is DNP3/MODBUS IP.
- MODBUS Validation—See the flow diagram in Figure 374.

Figure 374 MODBUS IP Serial Control Flow



As shown in Figure 374, in MODBUS the SCADA Primary/Subordinate can perform a read and write operation to a Remote Device (PLC/RTU) via the SCADA Gateway over the IP Network. SCADA Gateway interface connected to SCADA Remote Device (PLC/RTU) has the following configuration. This configuration is for reference purpose only.

IR1101 Gateway Configuration for MODBUS IP

The interface connected to SCADA Client has the following configuration:

```
interface Loopback0
 ip address 192.168.150.21 255.255.255.0

 interface Vlan1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 !

 int fastEthernet 0/0/1 /*It's a layer 2 port, corresponding layer 3 port int interface vlan1*/
 switchport access vlan 1
 !

 interface Tunnel0
 ip nat outside
 !
 ip nat inside source static tcp 192.168.0.11 502 interface Loopback0 502
```

MODBUS Configuration

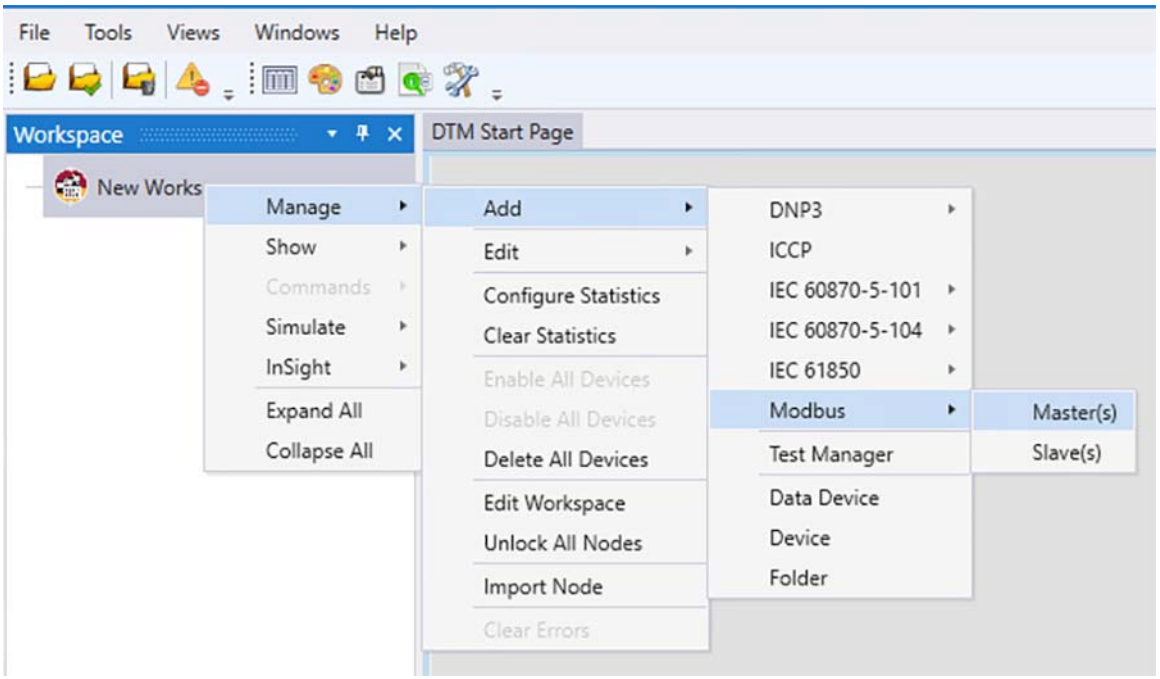
SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate is residing in the Control Center. The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Devices (PLC/RTU). The description below shows the DTM simulator configuration which vary based on the testing scenario. Representative field testing with non-simulated traffic and equipment can be found in the Distributed Automation Implementation guide at:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/IG/DA-FA-IG/DA-FA-IG.html

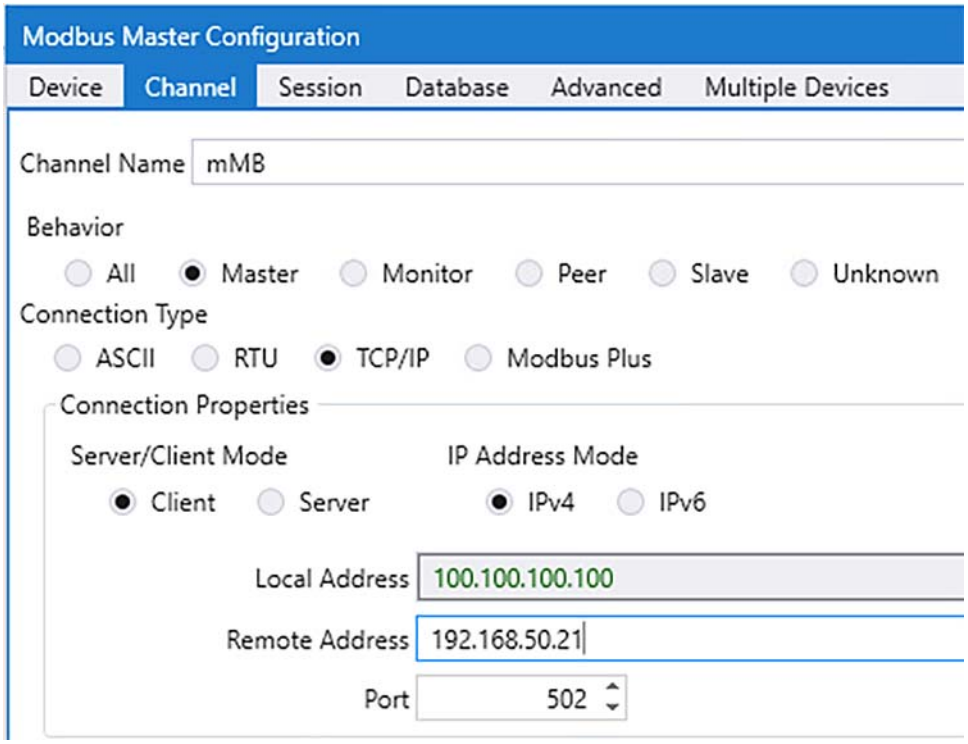
1. Open the SCADA Primary/Subordinate Application and add a new MODBUS Server.

Figure 375 SCADA Server Creation



2. From the **Channel** tab, configure the SCADA Primary/Subordinate, as shown in Figure 375 (Local Address: Address of SCADA Primary/Subordinate).

Figure 376 SCADA Primary/Subordinate Configuration



3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA Remote Device (PLC/RTU), which is configured to act as TCP Server.

4. Populate the remote address field with the Loopback IP of the Cellular gateway (Remote Address should be loopback IP of IR1101, with NAT/PAT configuration redirecting the IP and Port to the SCADA Remote Device (PLC/RTU)).

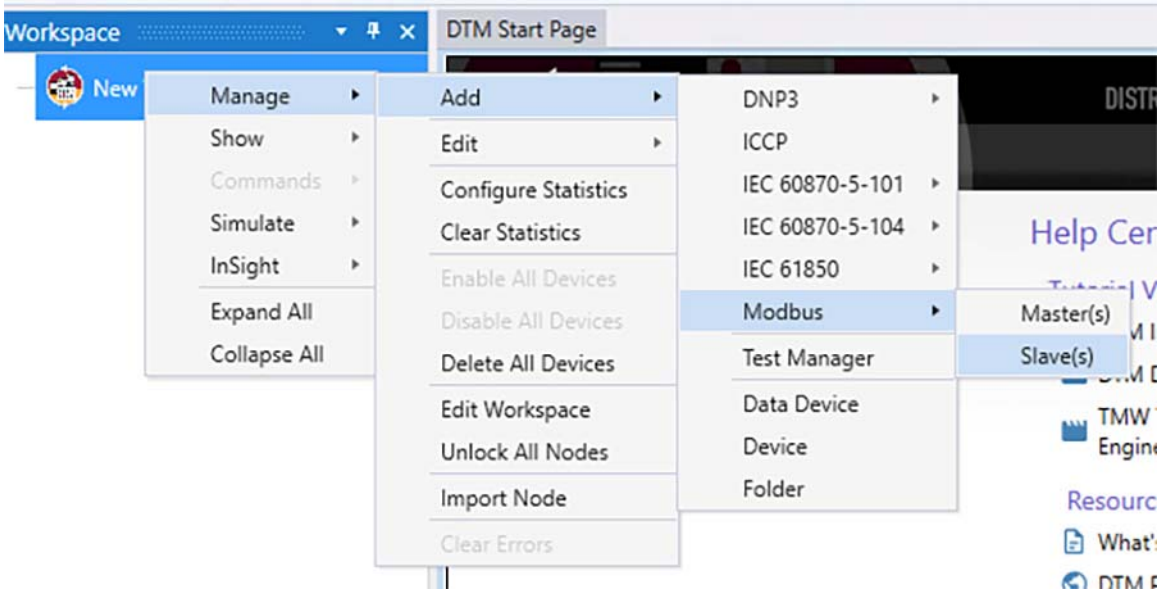
5. Populate the port with 502, which is the port used in SCADA Primary/Subordinate.

SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate.

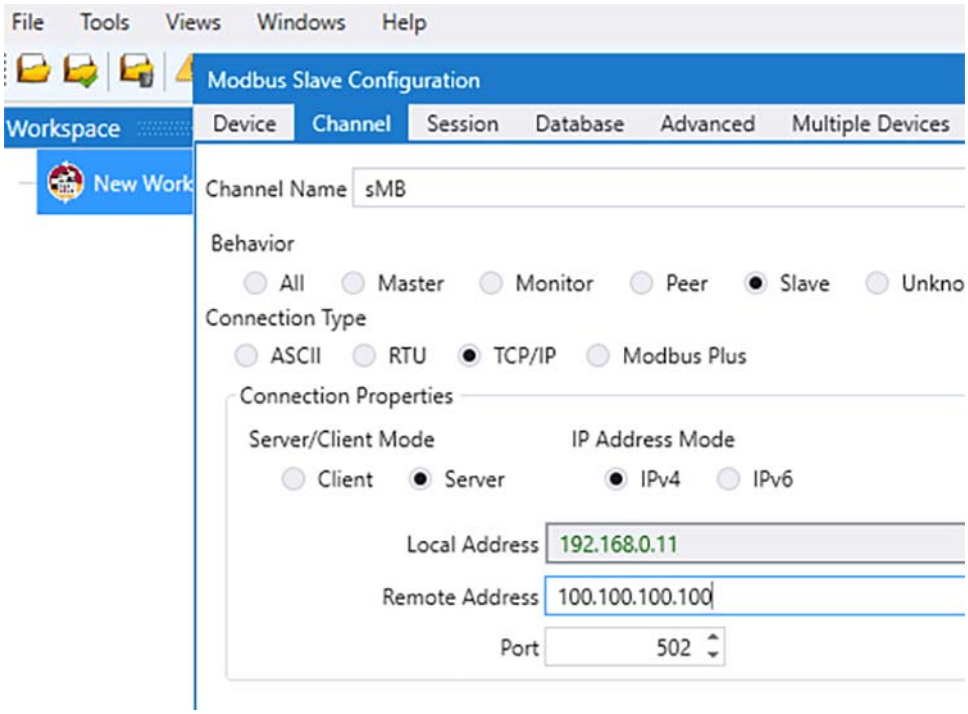
1. Open the SCADA Remote Device Application and add a new MODBUS Client.

Figure 377 SCADA Remote Device (PLC/RTU) Creation



2. From the **Channel** tab, configure the SCADA Remote Device (PLC/RTU), as shown in Figure 378.

Figure 378 SCADA Remote Device (PLC/RTU) Configuration



3. Populate the remote address field with SCADA Primary/Subordinate IP and Local Address as SCADA Remote Device (PLC/RTU) IP.

4. Populate the port with 502, which is the port used in SCADA Primary/Subordinate.

SCADA Operations for MODBUS

In MODBUS, the SCADA Primary/Subordinate requests the corresponding data from SCADA Remote Device (PLC/RTU) and SCADA Remote Device (PLC/RTU) responds to the request (It is usually Send Request from Primary and Read Response from SCADA Remote Device (PLC/RTU) type messages). The client does not initiate response/request on their own and only responds to messages from SCADA Primary/Subordinate.

They are four different types of tables are used to store information and data, based on the data user can request read or write into corresponding data points:

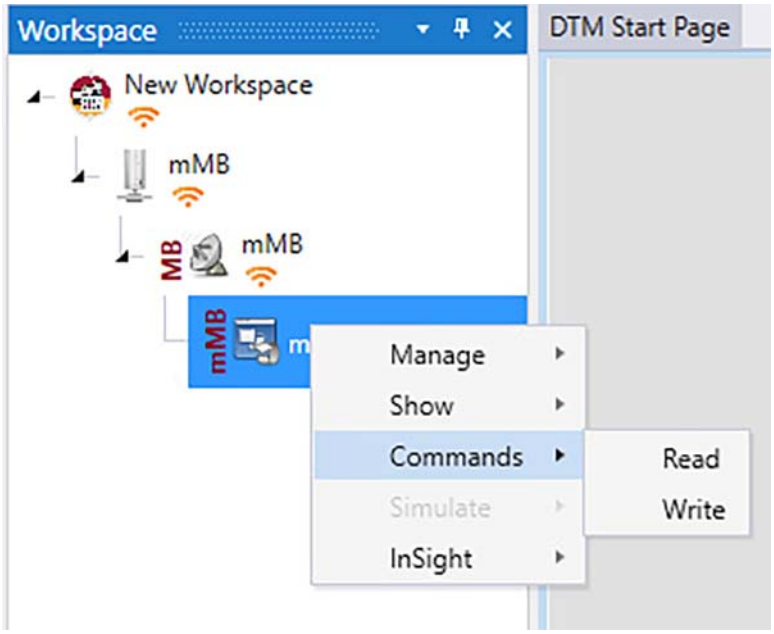
- Two tables are used to store simple discrete information called Coils:
  - Coils—User can perform Read/Write operations from SCADA MODBUS Server.
  - Discrete inputs—User can perform Read operations from SCADA MODBUS Server.
- Another two tables are used to store numeric 16-bit values called as Registers:
  - Input Registers—User can perform Read operations from SCADA MODBUS Server.
  - Holding Registers—User can perform Read/Write operations from SCADA MODBUS Server.

Read Operation:

Read operation is SCADA Primary/Subordinate trying to read data (coil, register) from SCADA Remote Device (PLC/RTU).

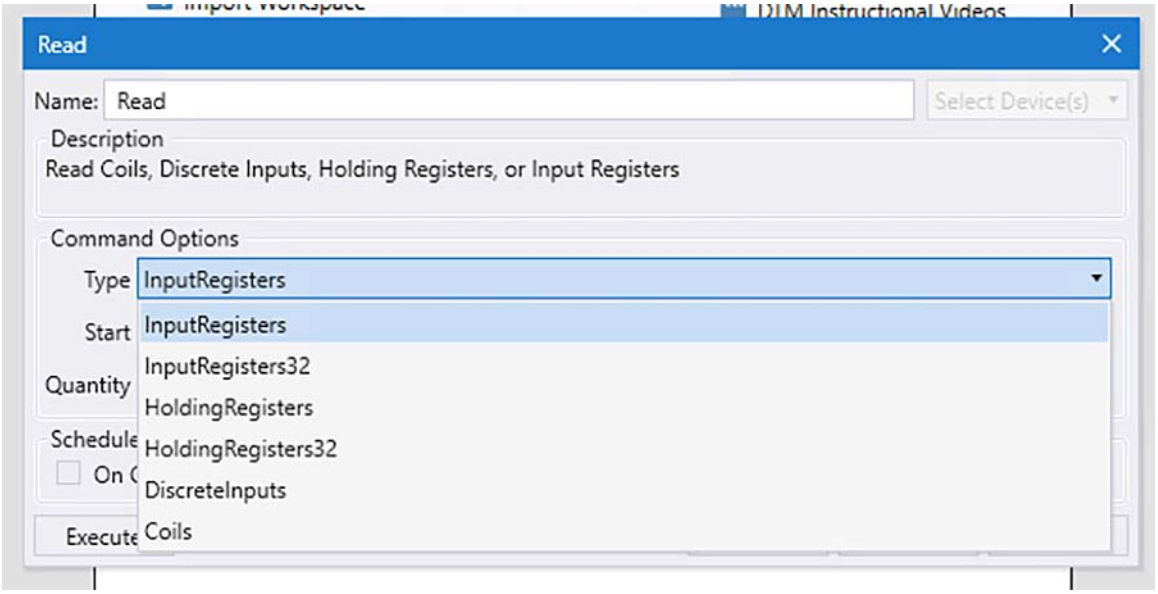
Step 1: User need to select **Read** option from SCADA Primary/Subordinate as show in Figure 379.

Figure 379 SCADA Read Operation from Primary



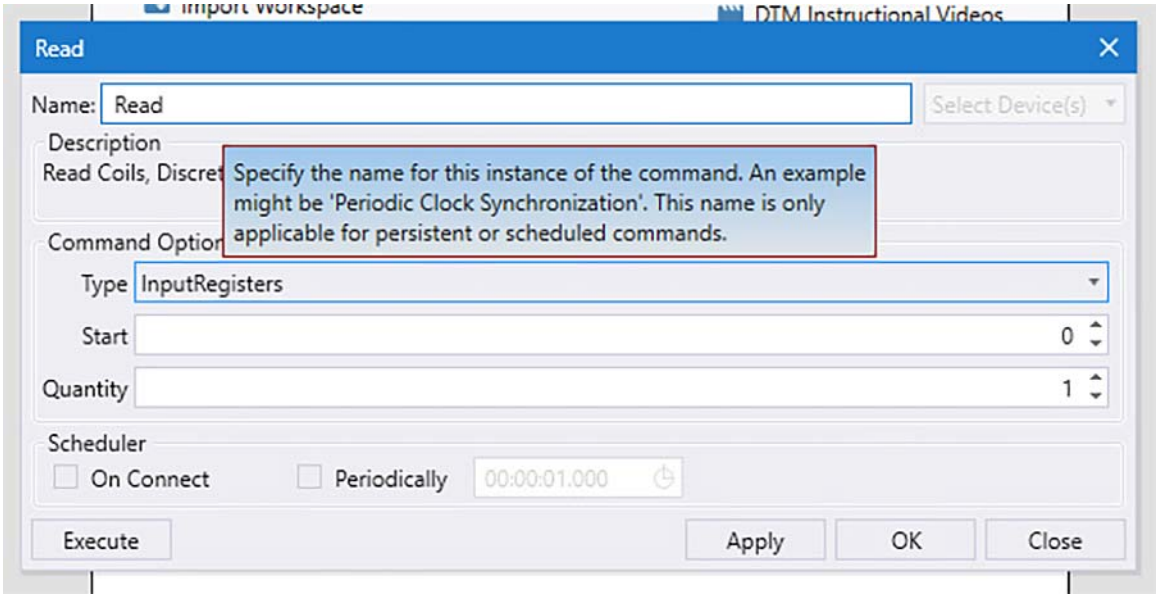
Step 2: Prompt will appear as shown in Figure 380 to select type of data. The user can select the type of data values.

Figure 380 SCADA Read Operation from Primary with Data Values



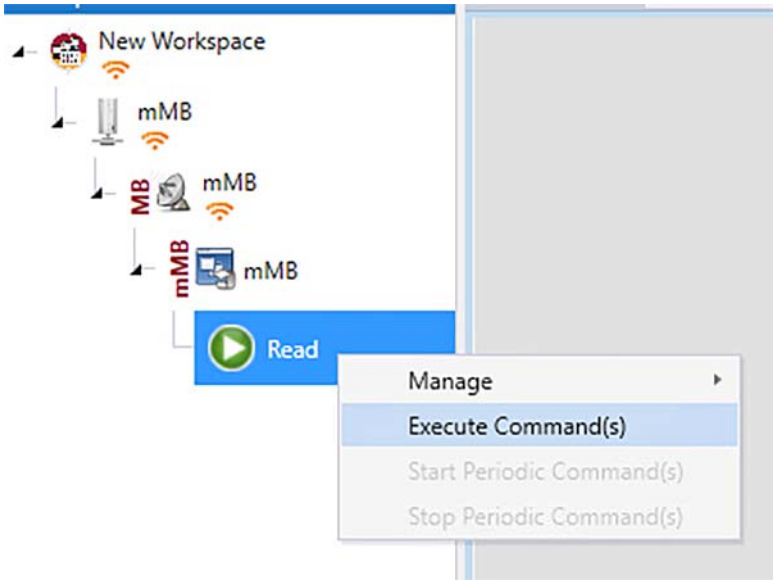
Step 3: User can select the **Start value** and **Quantity** and select **OK**.

Figure 381 SCADA Read Operation from Primary with Type Input Registers



Step 4: User can execute the corresponding commands as shown in Figure 382 to get the data.

Figure 382 SCADA Read Operation from Primary: Executing Commands

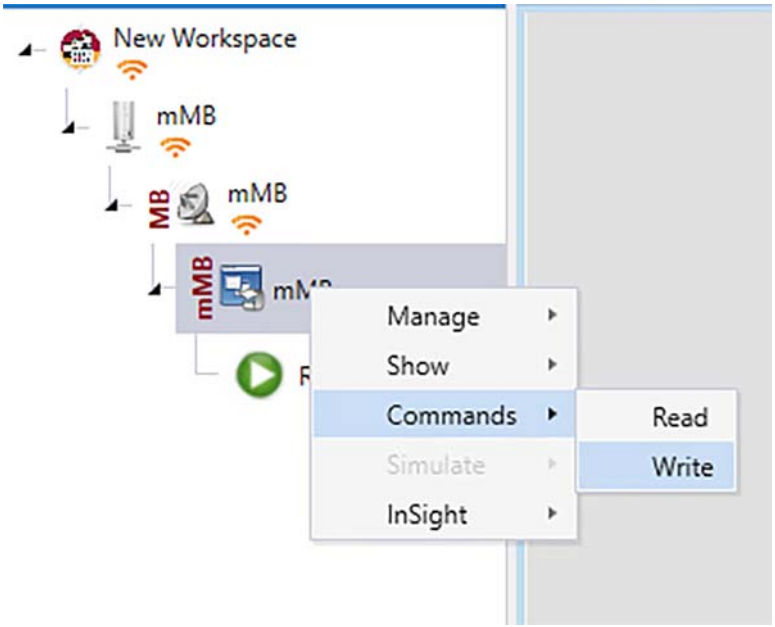


Write Operation:

Write operation is SCADA Primary/Subordinate trying to write data (Coil, Holding register) to SCADA Remote Device (PLC/RTU).

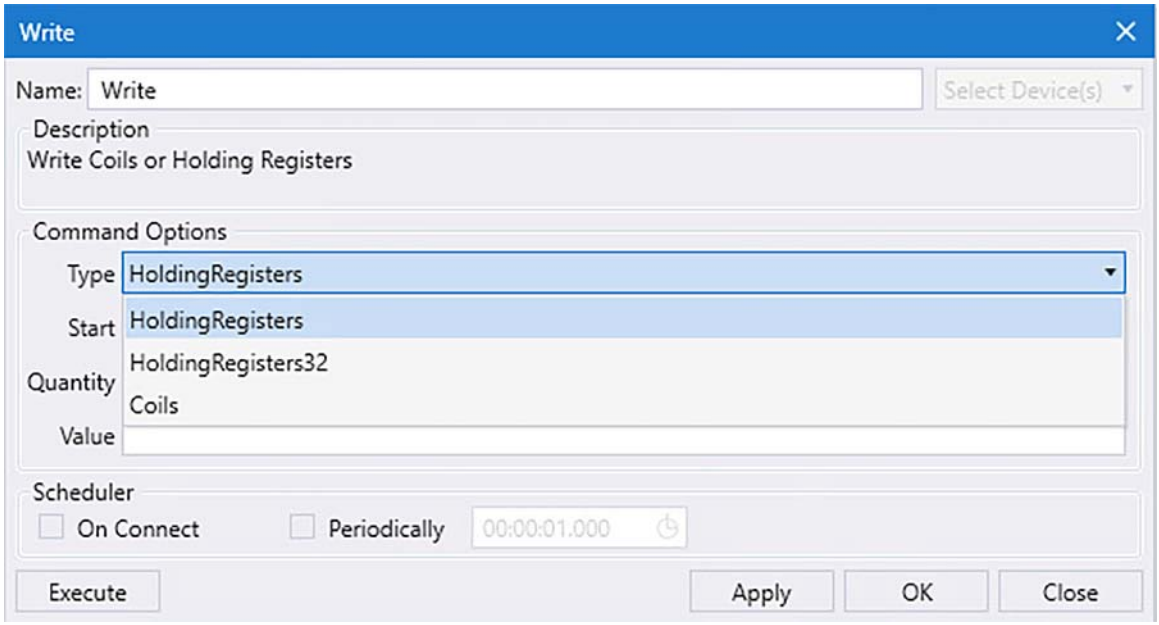
Step 1: User need to select **Write** option from SCADA Primary/Subordinate as show in Figure 383.

Figure 383 SCADA Write Operation from Primary



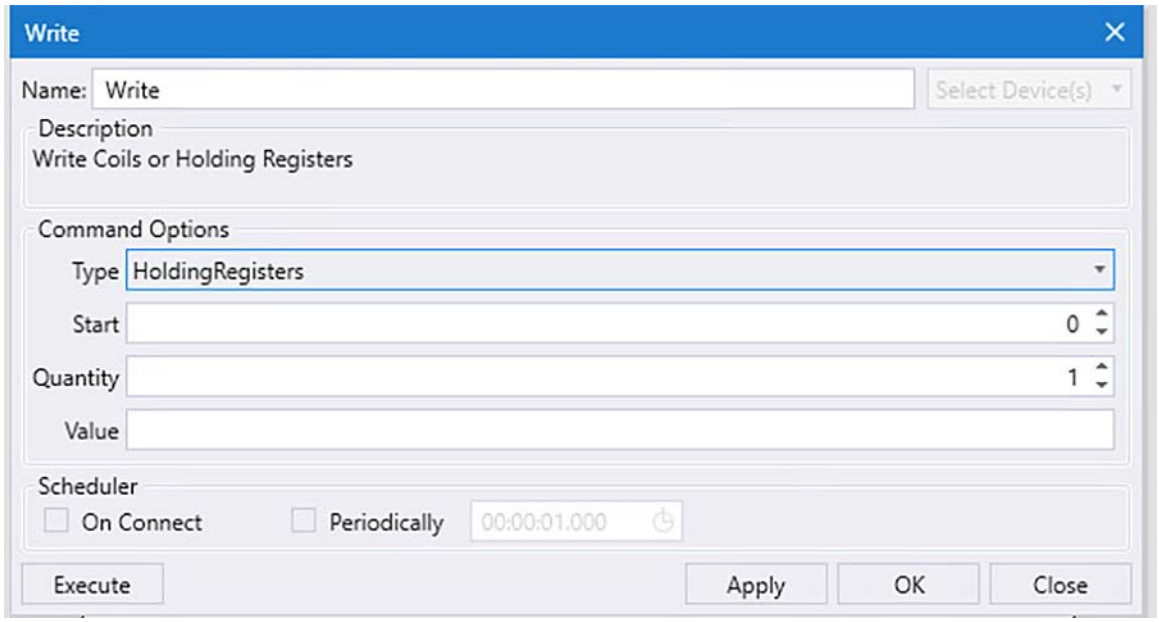
Step 2: Prompt will appear as shown in Figure 384 to select type of data. The user can select the type of data.

Figure 384 SCADA Write Operation from Primary with Data Values



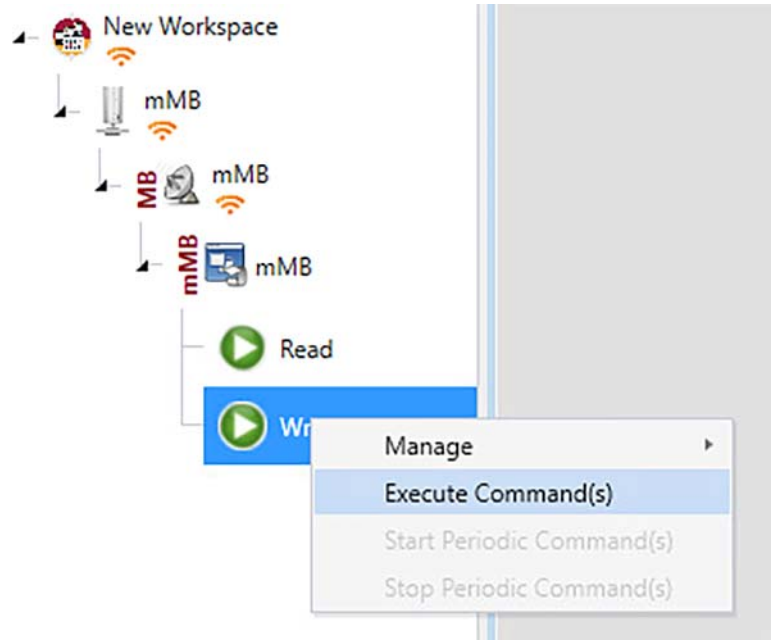
Step 3: User can select the **Start value** and **Quantity** and select **OK**.

Figure 385 SCADA Write Operation from Primary with Holding Registers



Step 4: User can execute the corresponding commands as shown in Figure 386 to get the data.

Figure 386 SCADA Write Operation from Primary: Executing Commands

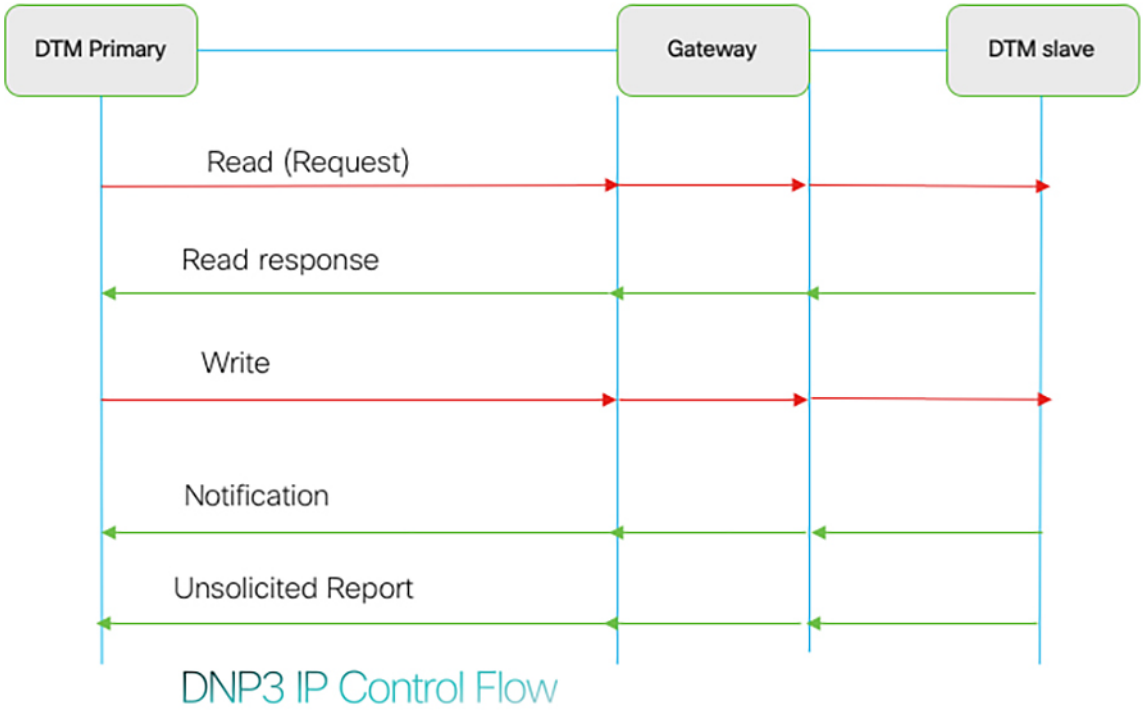


For more information regarding the MODBUS testing and simulation, refer to the Triangle Micro Works Documentation and DTM User Guides:

- https://www.trianglemicroworks.com/products/testing-and-configuration-tools/dtm-pages

DNP3 Validation

Figure 387 DNP3 IP Control Flow



As shown in Figure 387, the SCADA Primary/Subordinate can perform a read and write operation to a Remote Device via the SCADA Gateway. The Remote device can send the Unsolicited Reporting to the SCADA Primary/Subordinate via the SCADA Gateway over the IP network.

IR1101 SCADA Gateway Configuration

The interface connected to SCADA Client has the following configuration:

```
interface Loopback0
 ip address 192.168.150.21 255.255.255.0

 interface Vlan1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 !

 int fastEthernet 0/0/1 /*It's a layer 2 port, corresponding layer 3 port int interface vlan1*/
 switchport access vlan 1
 !

 interface Tunnel0
 ip nat outside
ip nat inside source static tcp 192.168.0.3 20000 interface Loopback0 20000
```

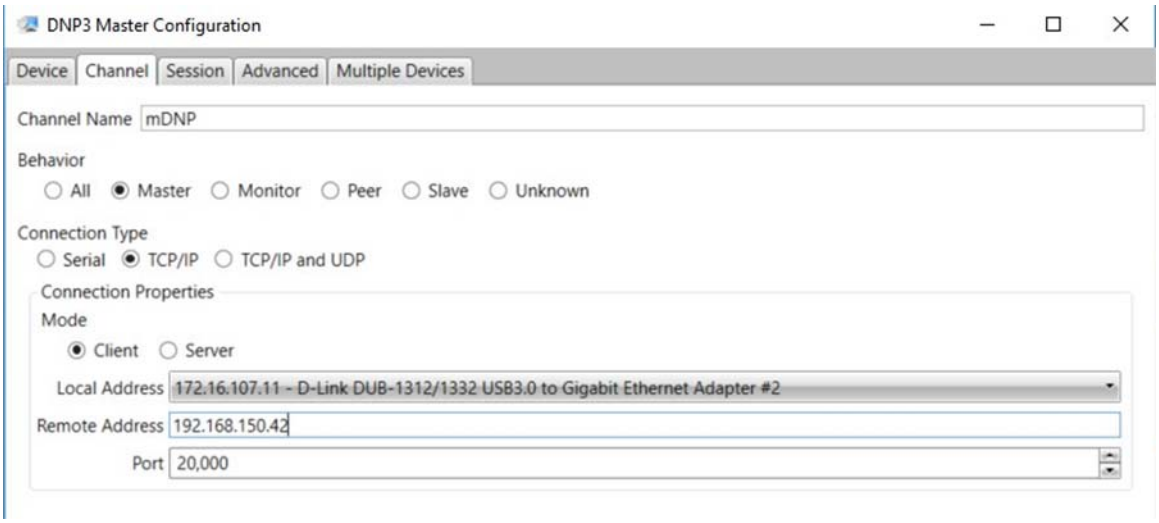
SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate resides in the Control Center. The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU)[1].

1. Open the **SCADA Primary Application** and add a new **DNP3 Server**.

2. From the Channel tab, configure the SCADA Primary/Subordinate, as shown in Figure 388.
3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA End Device, which is configured to act as TCP Server.
4. Populate the remote address field with the **Loopback IP** of the Cellular gateway.
5. Populate the port with **20000**, which is the port used in the Cisco IOS configuration.

Figure 388 SCADA Primary/Subordinate Configuration



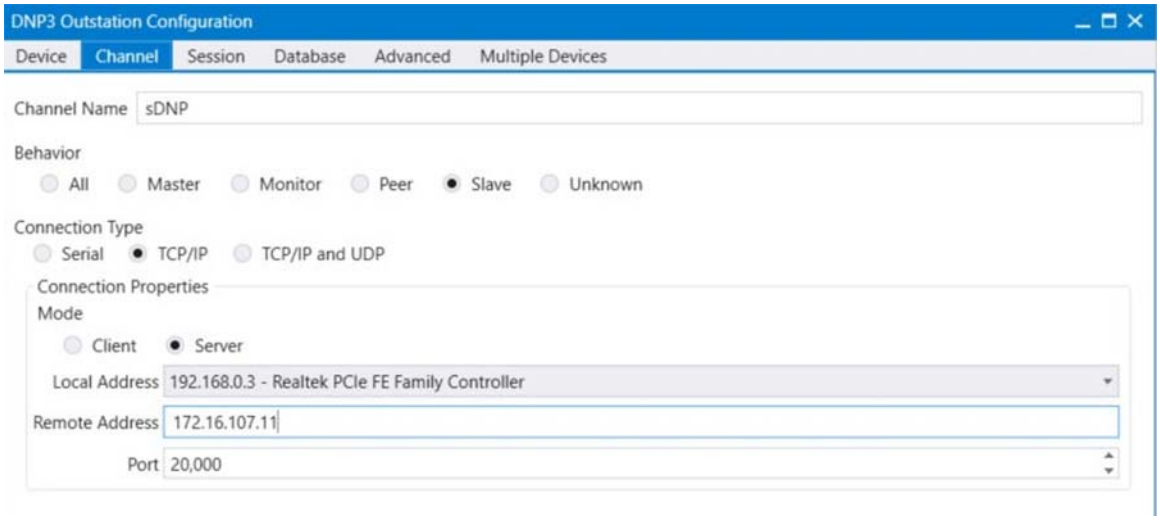
SCADA End Device (PLC/RTU) Configuration

As per the topology, the SCADA End Device resides in the field area. The following configuration must be required for the SCADA End Device to communicate with the SCADA Primary/Subordinate.

1. Open the **SCADA End Device Application** and add a new **DNP3 Client**.
2. From the **Channel** tab, configure the SCADA Primary/Subordinate, as shown in Figure 389.
3. Populate the remote address field with **SCADA Primary IP**.
4. Populate the port with **20000**, which is the port used in SCADA Primary/Subordinate.

1. The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Figure 389 SCADA End Device Configuration



SCADA Operations for DNP3

The SCADA Primary/Subordinate and the SCADA End Device can communicate via Poll, Control, and Unsolicited Reporting. Poll and Control operations are initiated from the SCADA Primary/Subordinate. Unsolicited Reporting is sent to the SCADA Primary/Subordinate from the End Device.

Poll Operation

The Poll operation is performed by the SCADA Primary/Subordinate. The SCADA Primary/Subordinate can execute a general Poll in which all the register values are read and sent to the SCADA Primary/Subordinate as shown in Figure 390.

The user can select Integrated Data Poll, RBE Data Poll, and Read Specific Data as shown in Figure 391.

Figure 390 Operations Performed Using DNP3

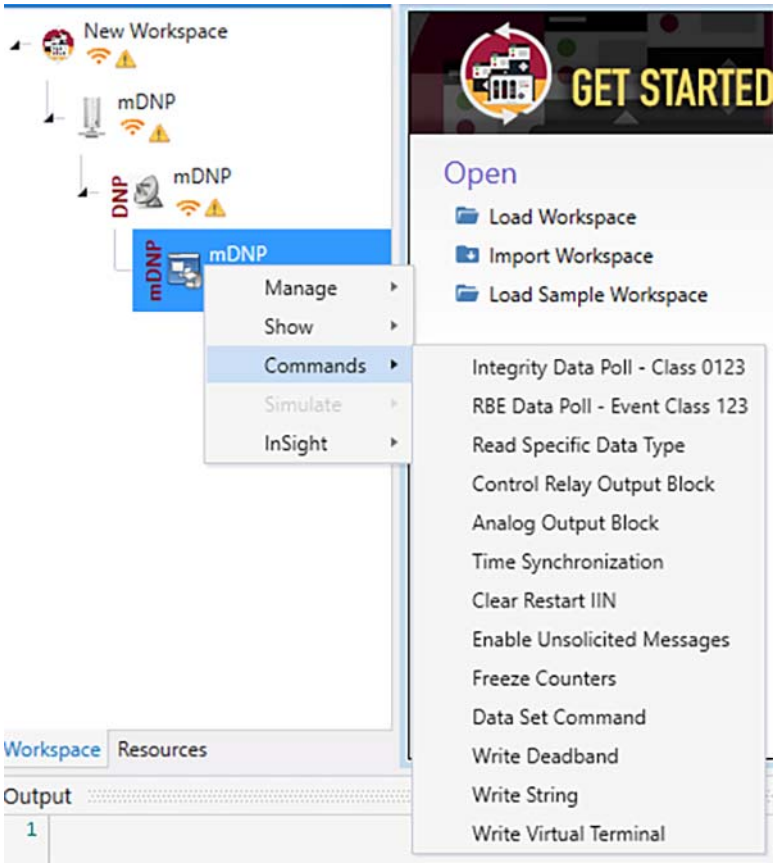


Figure 391 SCADA Primary/Subordinate Analyzer Logs before Poll Operation

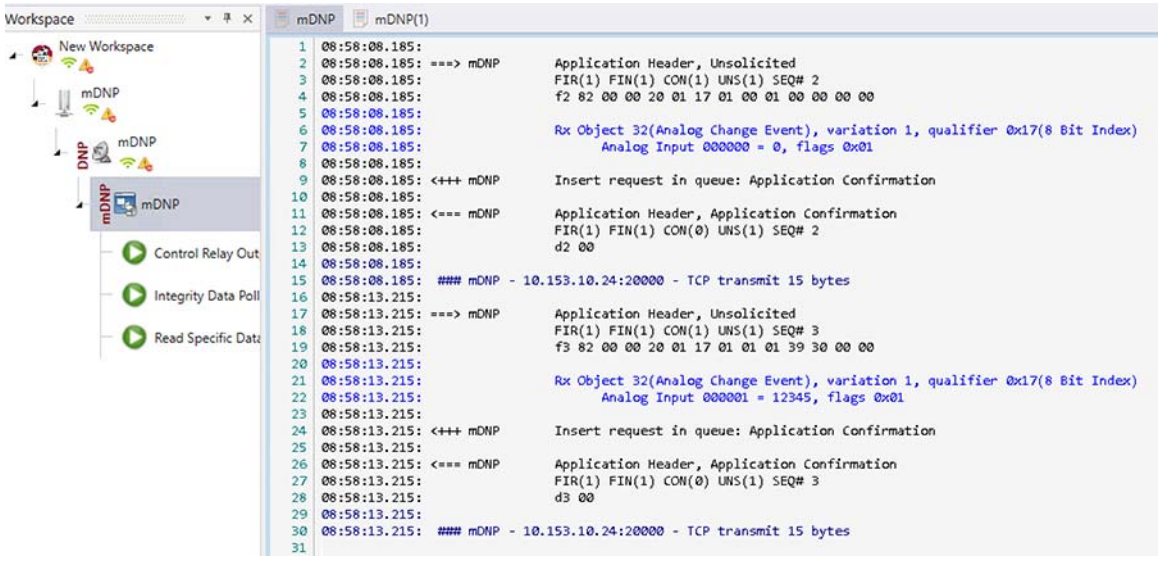
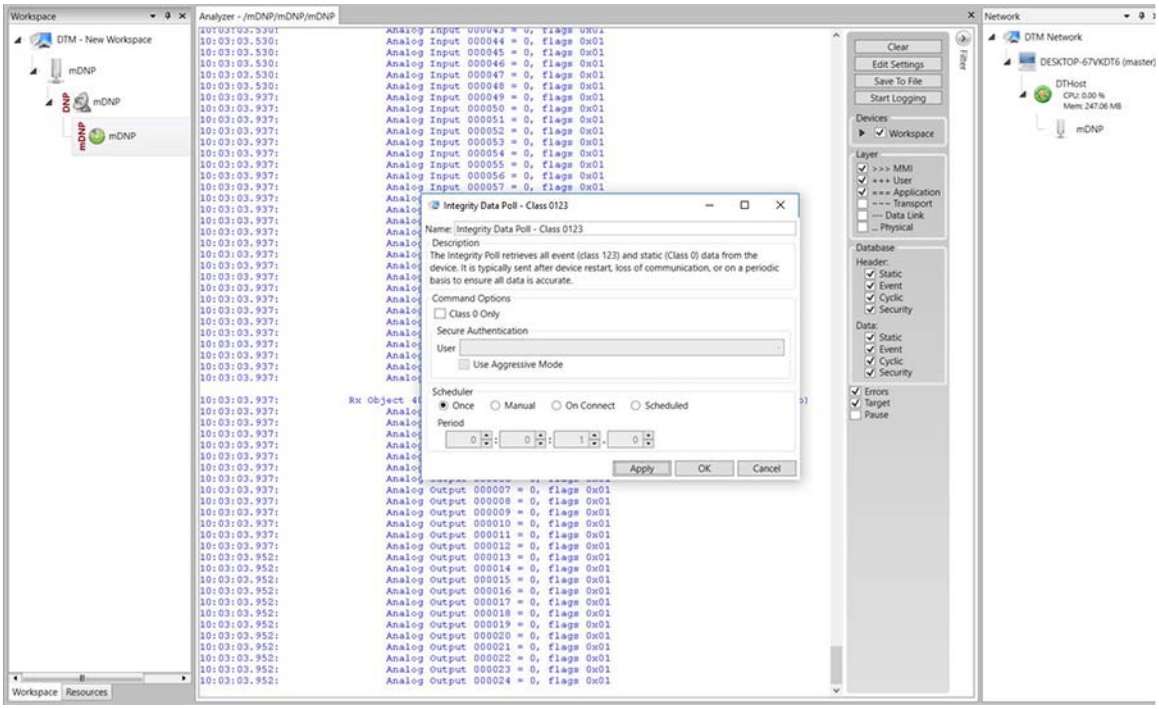


Figure 392 SCADA Primary/Subordinate Analyzer Logs after Poll Operation



Control Operation

Control operation basically sends the control command from the SCADA Primary/Subordinate to the SCADA Remote Device (PLC/RTU) in order to control the operation of end devices. The control command can be executed, and the results can be seen on the analyzer. The value of Control Relay Output is changed and is notified to the Primary. Figure 393 shows control relay output status before sending the control command to the Subordinate.

Figure 393 SCADA Remote Device (PLC/RTU) Register before Control Operation

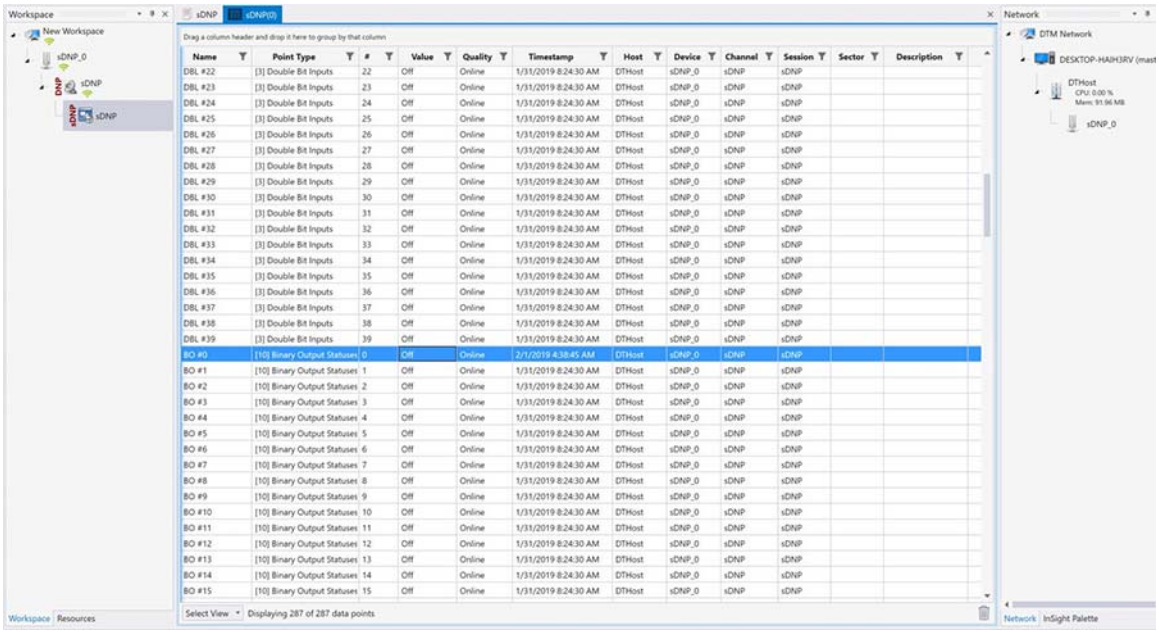


Figure 394 shows how SCADA Primary/Subordinate sends the control command.

Figure 394 SCADA Primary/Subordinate Sending Control Command

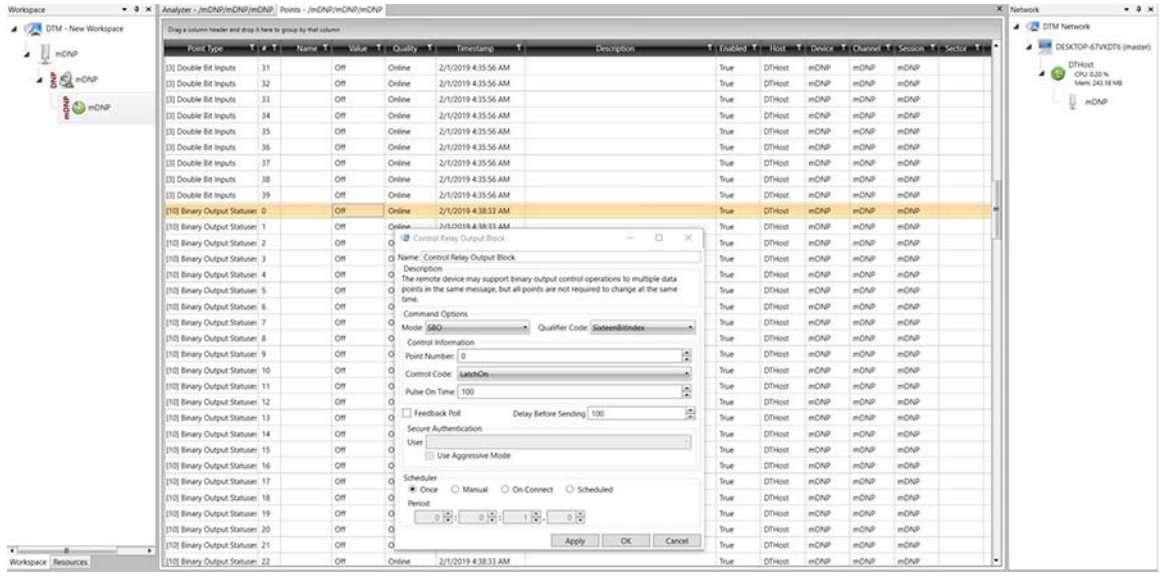
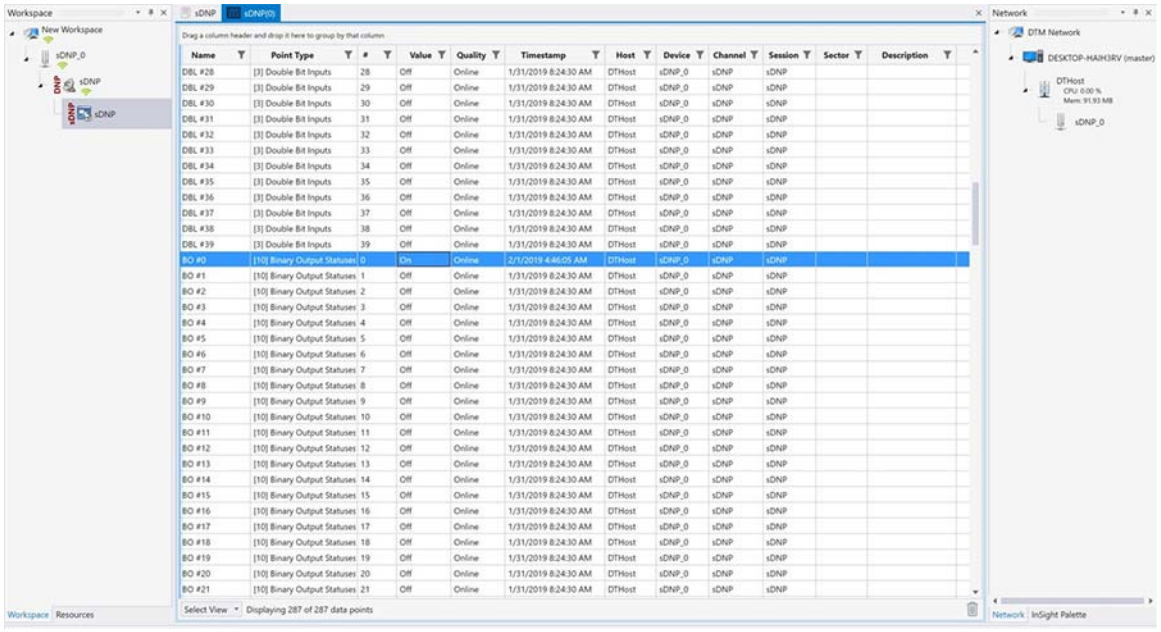


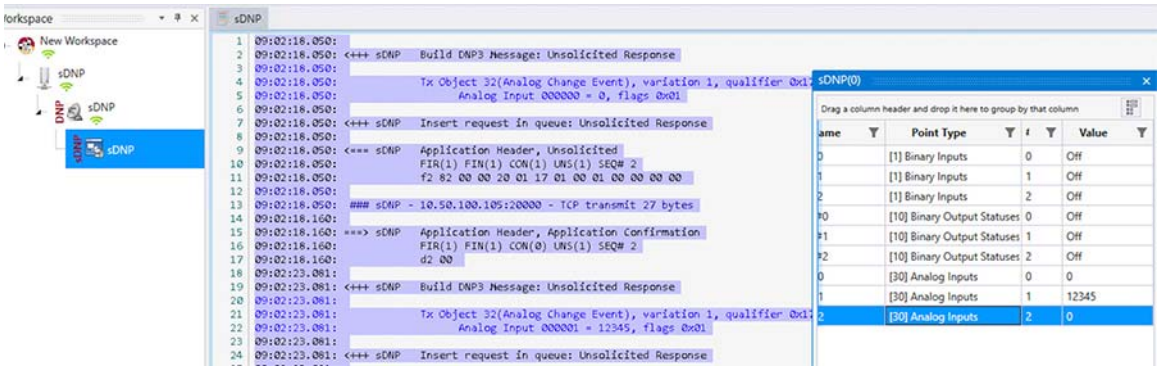
Figure 395 DNP3 Client Register after Control Operation



Unsolicited Reporting

Unsolicited Reporting is initiated by the SCADA Remote Device (PLC/RTU), which is connected to the SCADA Gateway. Changes to the value of the Subordinate register are notified to the SCADA Primary/Subordinate. This notification can be seen on the SCADA Server Analyzer.

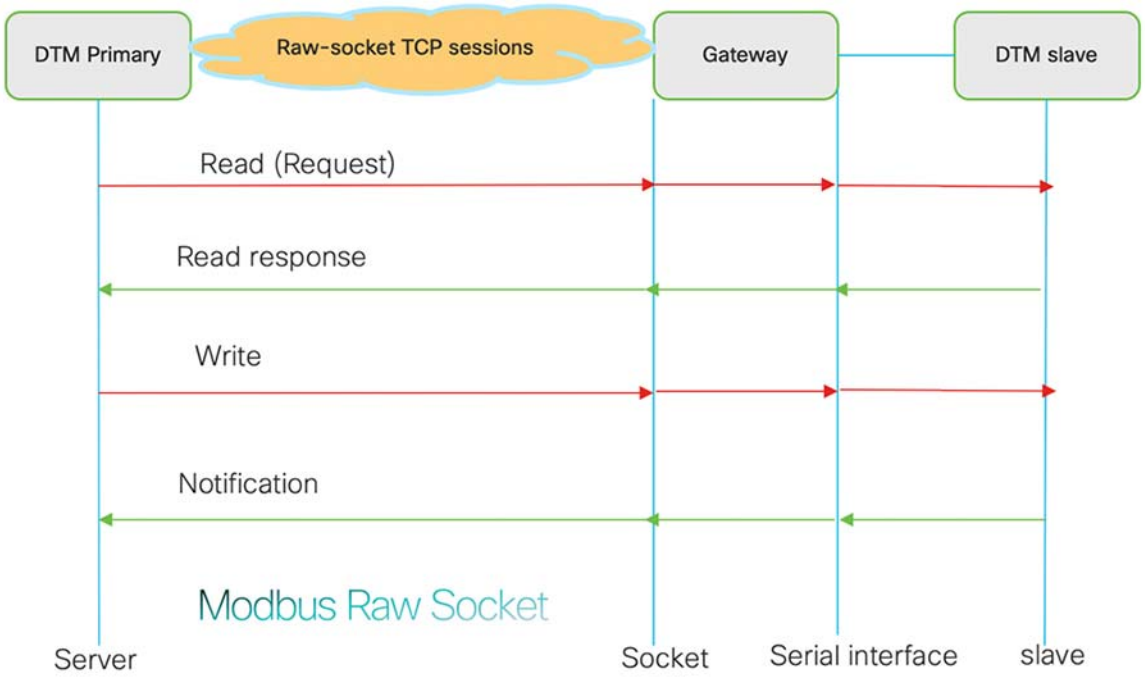
Figure 396 DNP3 Client Sending Solicit Response to Server



Legacy SCADA (Raw Socket TCP)

- Protocol Validation—The protocol validated for this release is MODBUS.
- MODBUS Control Flow—See the flow diagram in Figure 397.

Figure 397 MODBUS Control Flow



As shown in Figure 397, the DTM Primary can read and write the Remote Device via the Cellular Gateway using TCP Raw Socket. For more details about Raw Socket, refer to the CCI Design Guide.

Legacy SCADA (Raw Socket TCP)—MODBUS

Gateway Configuration for MODBUS TCP Raw Socket

Raw socket is a method of transporting serial data through an IP network. This feature can be used to transport SCADA data from SCADA Remote Devices (PLC/RTU). Raw Socket supports TCP or UDP as transport protocol. An interface can be configured with any one of the protocols but not both at the same time.

This section shows the sample configuration for raw socket TCP on Cisco IR1101.

Interface Configuration on IR1101 (Raw Socket Configuration)

```
interface Async0/2/0
 no ip address
 encapsulation raw-tcp
end
!
```

Corresponding Line Configuration

```
!
line 0/2/0
  raw-socket tcp server 502 192.168.150.16
  raw-socket special-char 7
  raw-socket packet-timer 500
  raw-socket packet-length 32
  transport preferred none
  stopbits 1
  databits 8
  parity none
!
```

In the above configuration IR1101 acts as a TCP server which listens on port 502 (Port numbers vary for MODBUS) and local binding IP of 192.168.150.16.

The user can verify the raw socket configuration with the following show commands:

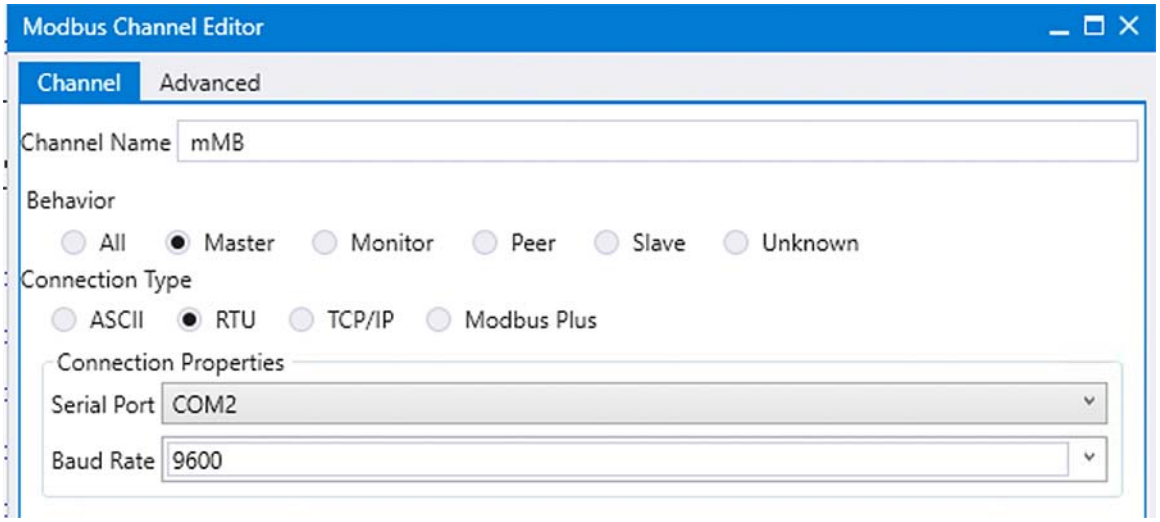
- **show raw-socket tcp detail** (information about line registration and connections, socket mapping)
- **sh raw-socket tcp sessions** (information about TCP session)
- **show raw-socket tcp statistic** (information about TCP serial statistics)

SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate is residing in the Applications Server Center. The following configuration is required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU). In this implementation, SCADA DTMW simulator is used instead of a real SCADA device.

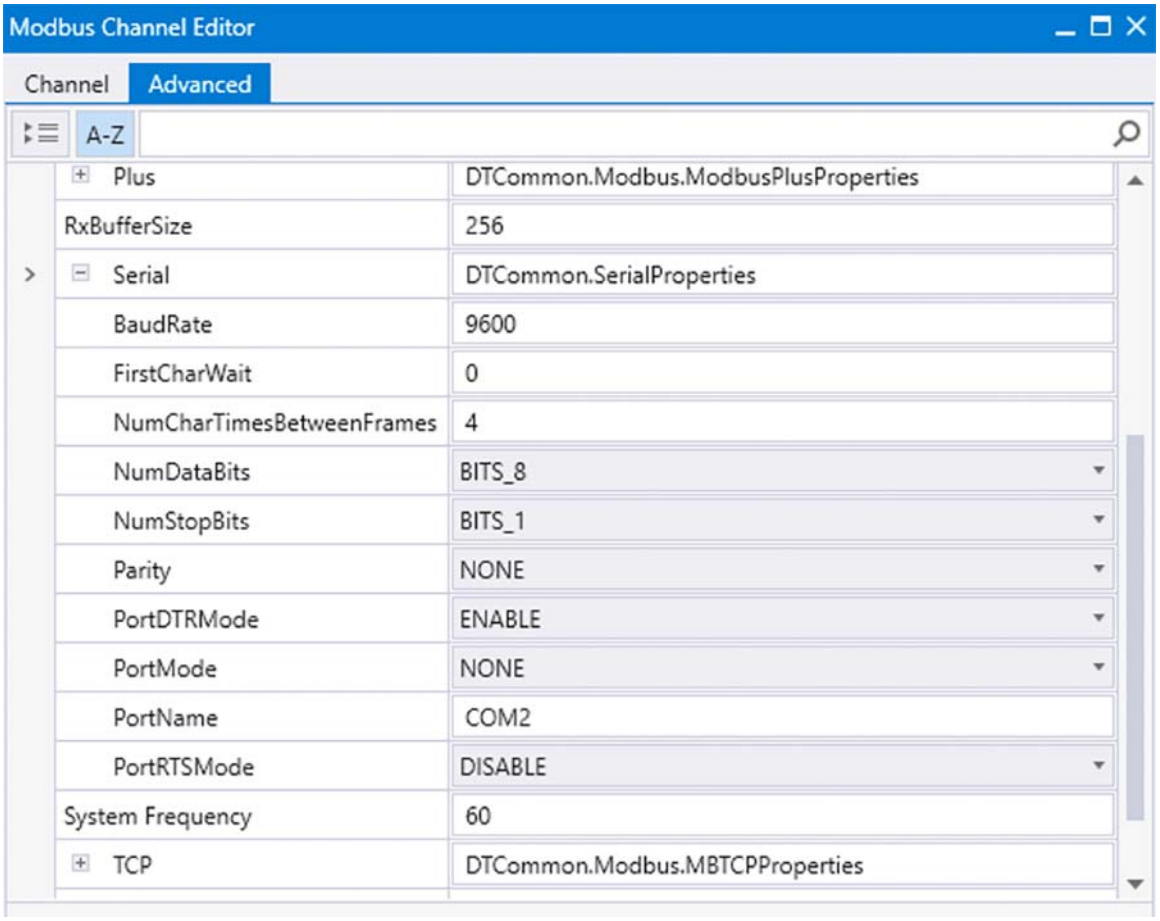
1. Open the **SCADA Primary Application** and click **Add a new MODBUS Server**.
2. From the **Channel** tab, configure the SCADA Primary/Subordinate as shown in Figure 398.

Figure 398 SCADA Primary/Subordinate Configuration



3. On the SCADA Primary/Subordinate, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching for your device configuration.

Figure 399 SCADA Primary/Subordinate Variables

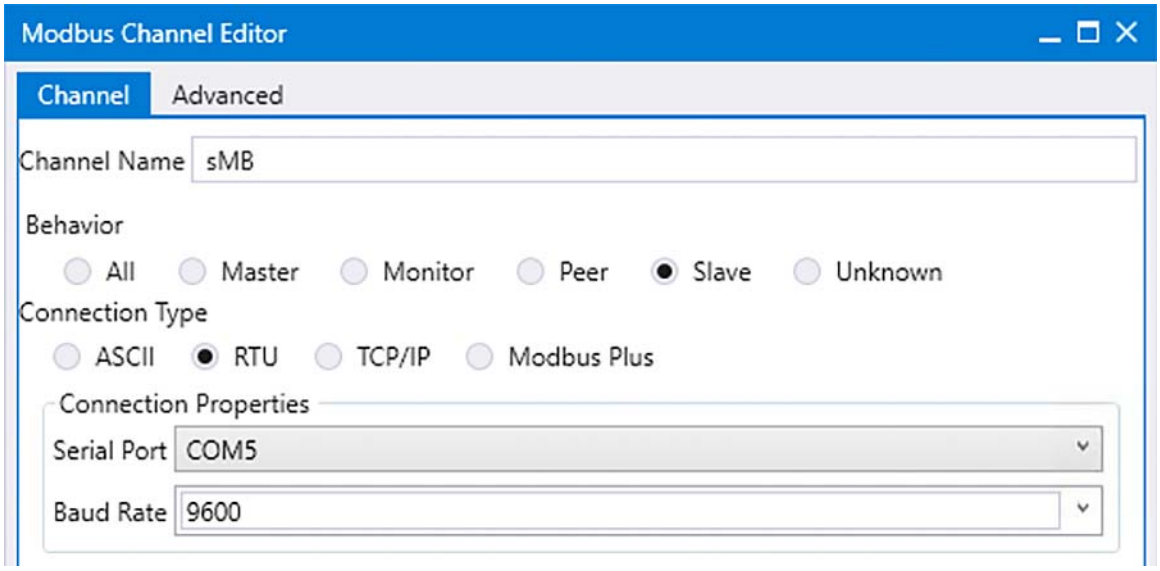


SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. In this implementation, SCADA DTMW simulator is used instead of a real SCADA device.

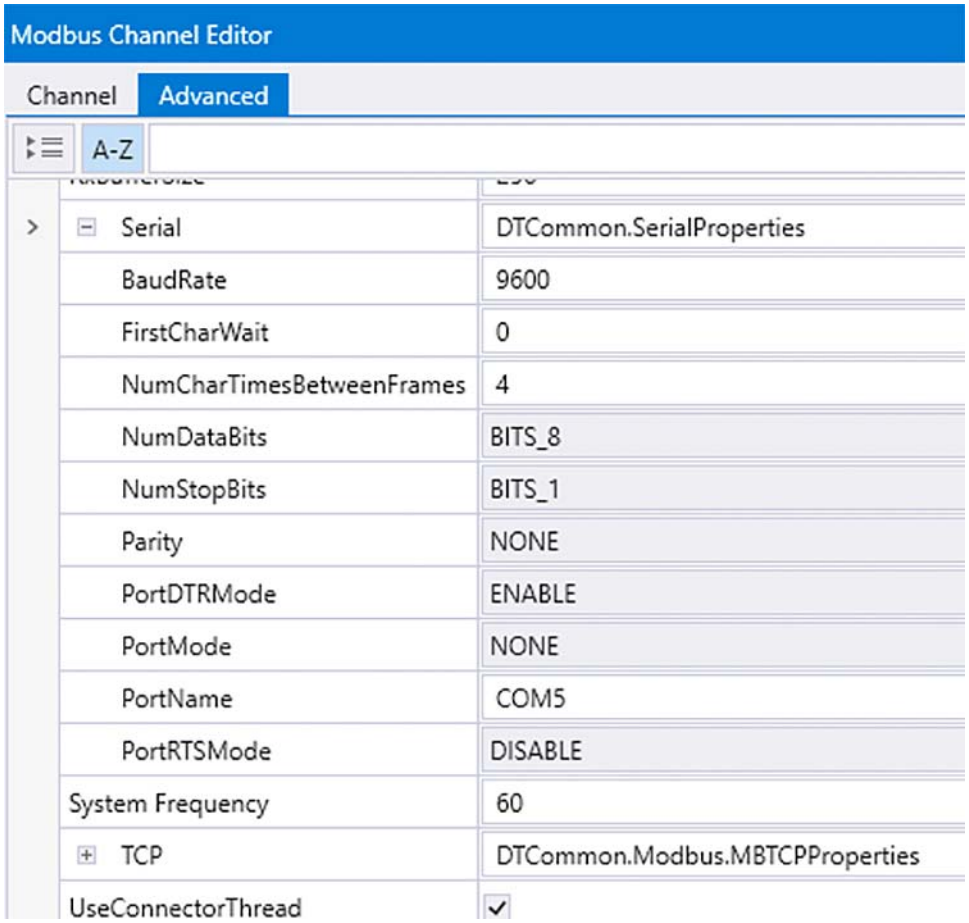
1. Open the **SCADA Remote Device Application** and click **Add a new MODBUS Client**.
2. From the **Channel** tab, configure the SCADA Remote Device (PLC/RTU) as shown in Figure 400.

Figure 400 SCADA Remote Device (PLC/RTU) Configuration



3. On the SCADA Remote Device (PLC/RTU), select the appropriate serial port, baud rate, data bits, stop bits and parity matching for your device configuration.

Figure 401 SCADA Remote Device (PLC/RTU) Variables



SCADA Operations of Legacy SCADA

The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS, page 465.

Figure 402 shows the sample images on the SCADA Primary/Subordinate when the MODBUS connection is established. The user can check the baud rate, parity, data and stop bits.

Figure 402 SCADA Operations for MODBUS IP–1

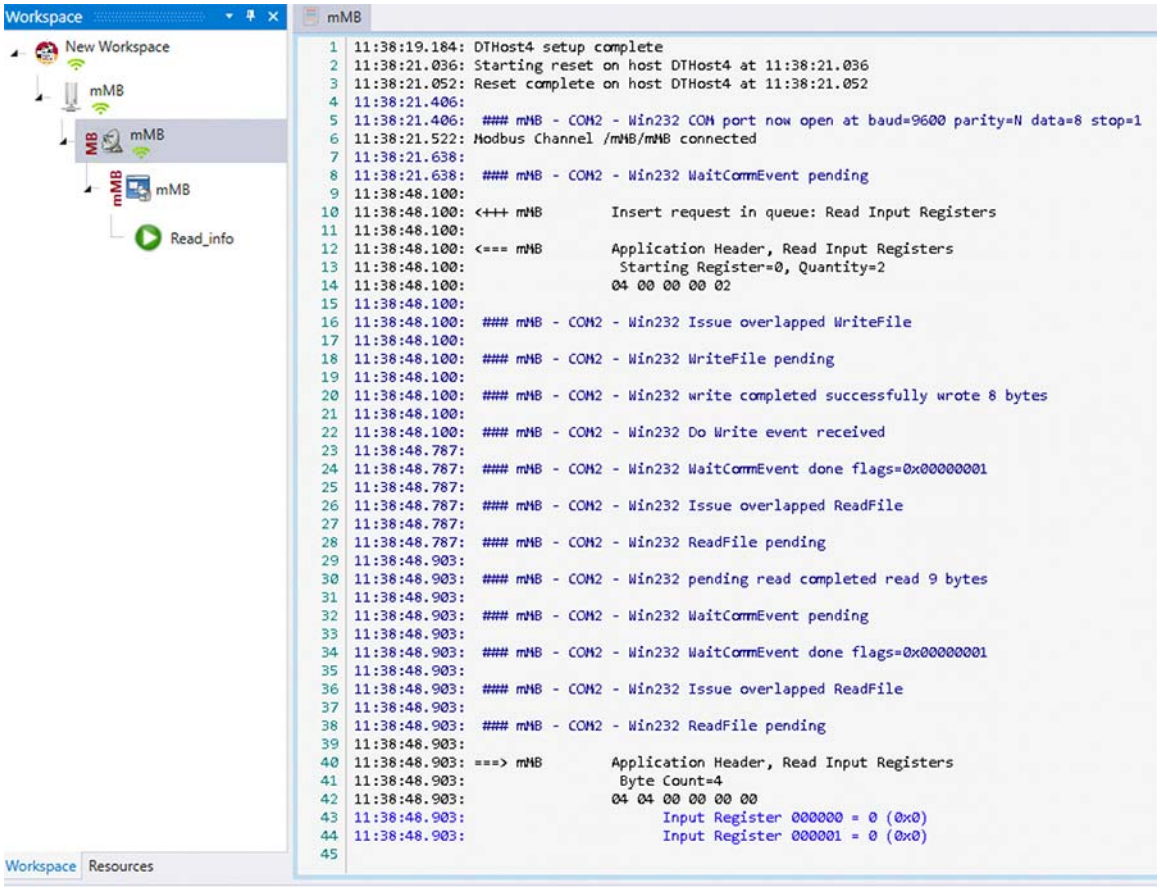


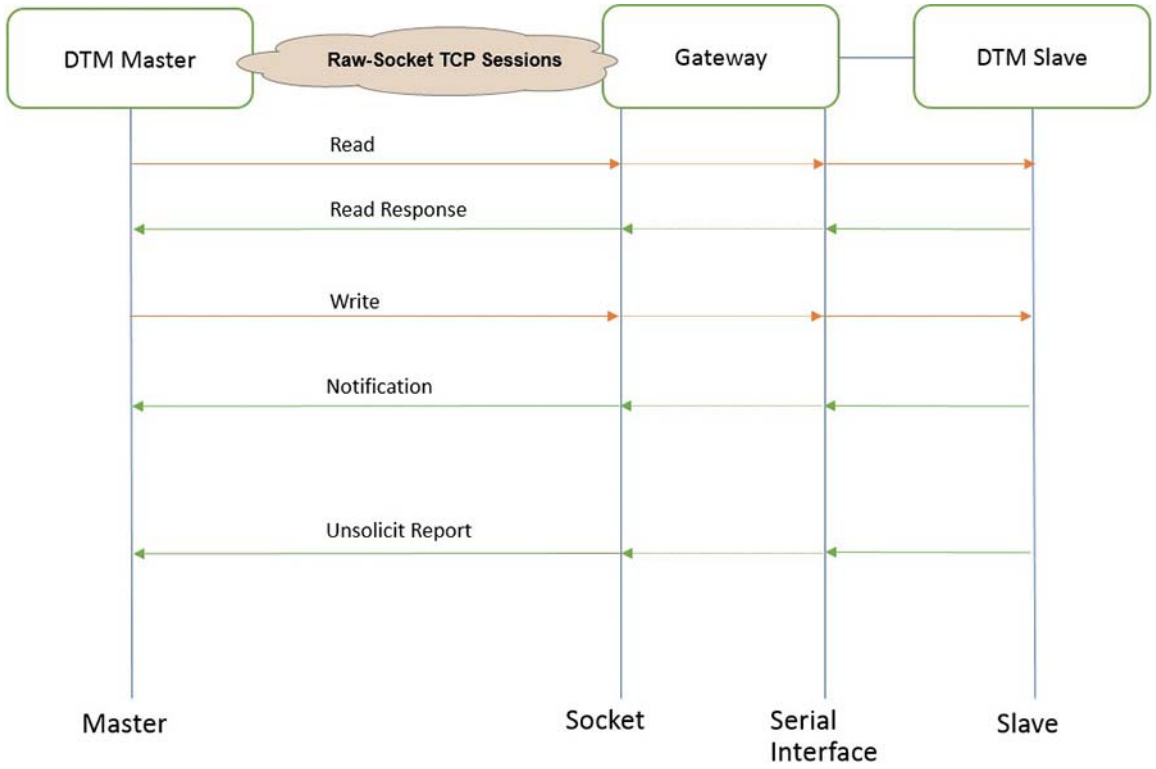
Figure 403 shows the sample images on the SCADA Remote Device (PLC/RTU) when the MODBUS connection is established.

Figure 403 SCADA Operations for MODBUS IP–2

Legacy SCADA (Raw Socket TCP)—DNP3

- Protocol Validation—The protocol validated for this release is DNP3.
- MODBUS Control Flow—See the flow diagram in Figure 404.

Figure 404 DNP3 Raw-Socket Control Flow



As shown in Figure 404, the DTM Server can read and write the Client via the SCADA Gateway using TCP Raw Socket. In addition, the Client can send the Unsolicited Reporting to the DTM Server via the SCADA Gateway using TCP Raw Socket.

IR1101 SCADA Gateway Raw Socket Configuration

As per the topology, the interface connected to SCADA Remote Device (PLC/RTU) has the following configuration:

```
interface Async0/2/0
no ip address
encapsulation raw-tcp
!

line 0/2/0
raw-socket tcp client 172.16.107.11 25000 192.168.150.42 25000
databits 8
stopbits 1
speed 9600 parity none
!
```

SCADA Server and SCADA Client Configuration

For SCADA Server and SCADA Client configuration, refer to SCADA Primary/Subordinate and SCADA Remote Device (PLC/RTU) Configuration, page 486 in the above Legacy SCADA MODBUS configuration and select DNP3 Server and Client.

SCADA Operations

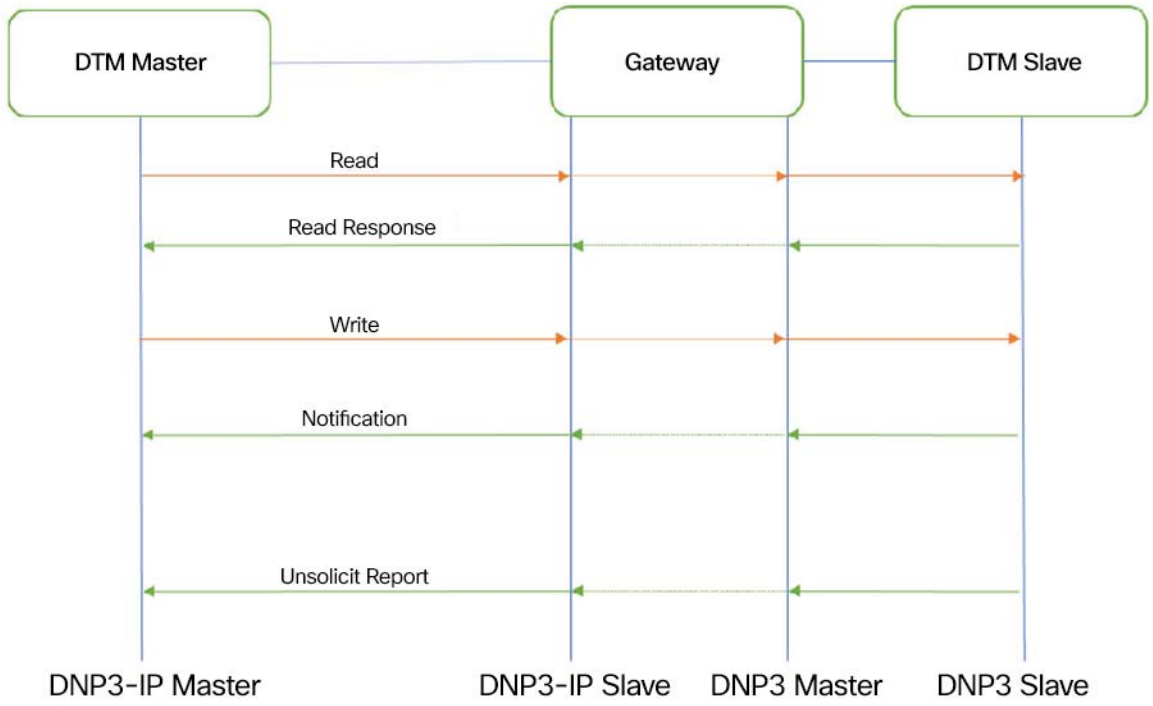
For SCADA Operations, refer to SCADA Operations for DNP3, page 472.

SCADA Gateway

- Protocol Validation—The protocols validated for this release are DNP3 and DNP3 IP.

- DNP3-to-DNP3 IP Control Flow—See the flow diagram in Figure 405.

Figure 405 DNP3-to-DNP3 IP Protocol Translation Control Flow



As shown in Figure 405, the DTM Server can read and write the Client via the SCADA Gateway using protocol translation. The Client can send the Unsolicited Reporting to the Server via the SCADA Gateway using protocol translation.

IR1101 SCADA Gateway Raw Socket Configuration

As per the topology, the interface connected to SCADA Remote Device (PLC/RTU) has the following configuration:

```
interface Async0/2/0
no ip address
encapsulation scada
!

line 0/2/0 databits 8
 stopbits 1
 speed 9600
 parity none
!

scada-gw protocol dnp3-serial
channel dnp3_ch1
 link-addr source 4
 bind-to-interface Async0/2/0
session dnp3_session1
 attach-to-channel dnp3_ch1
scada-gw protocol dnp3-ip
 channel dnp3ip ch1
  tcp-connection local-port 21000 remote-ip any
 session dnp3ip_session1
  attach-to-channel dnp3ip_ch1
  link-addr source 4
```

```
  map-to-session dnp3_session1
scada-gw enable
!
```

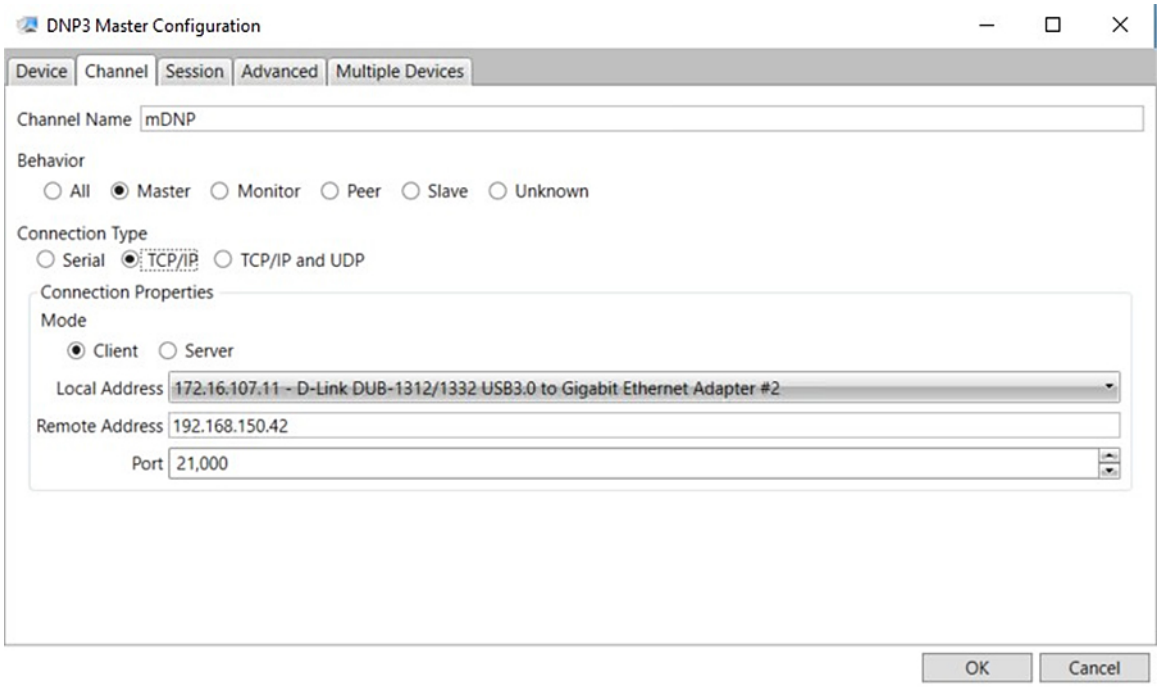
SCADA Primary/Subordinate and SCADA Remote Device (PLC/RTU) Configuration

SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate is residing in the Control Center. The following configuration is required in order for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU):

1. Open the **SCADA Primary Application** and click **Add a new DNP3 Server**.
2. From the **Channel** tab, configure the SCADA Primary/Subordinate as shown in Figure 406.
3. SCADA Primary/Subordinate (in this case configured as TCP Client), interacts with the SCADA Remote Device (PLC/RTU), which is configured to act as a TCP Server.
4. Populate the remote address field with the **Loopback IP of Cellular Gateway**.
5. Populate the port with **21000**, which is the port used in Cisco IOS Configuration.

Figure 406 SCADA Primary/Subordinate Configuration for IR1101 Gateway



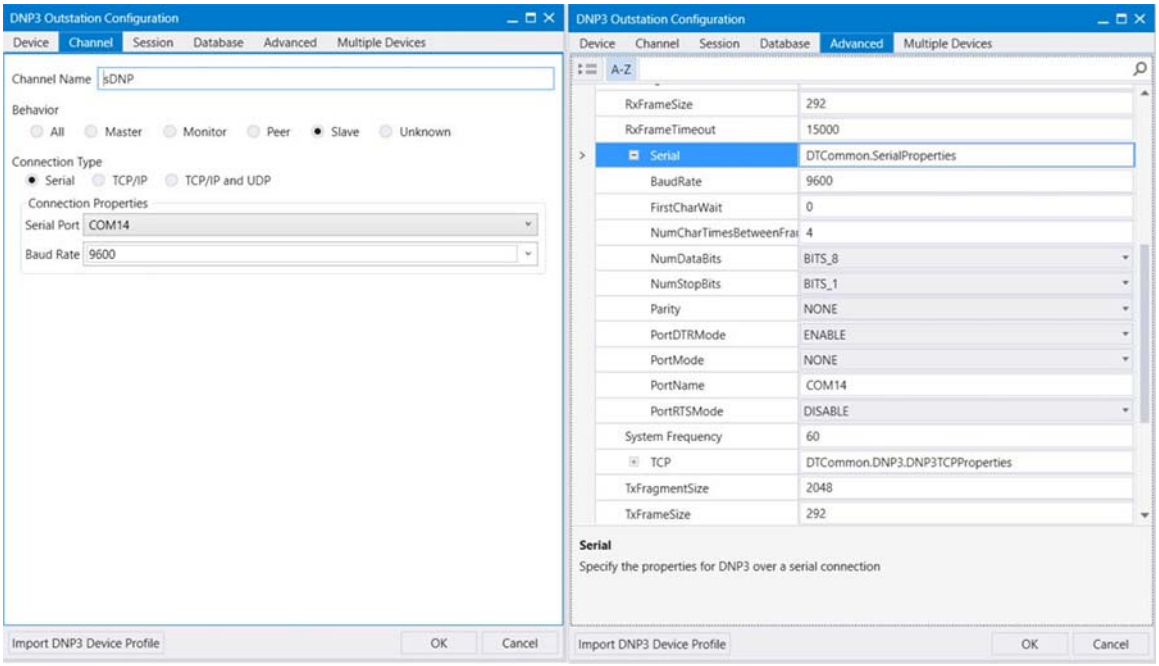
SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with SCADA Primary/Subordinate. In this implementation, we used SCADA DTMW simulator instead of a real SCADA device.

1. Open the **SCADA Remote Device Application** and click **Add a new DNP3 Client**.
2. From the **Channel** tab, configure the SCADA Primary/Subordinate, as shown in Figure 407.

3. On the **SCADA Remote Device**, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration.

Figure 407 SCADA Remote Device (PLC/RTU) Configuration



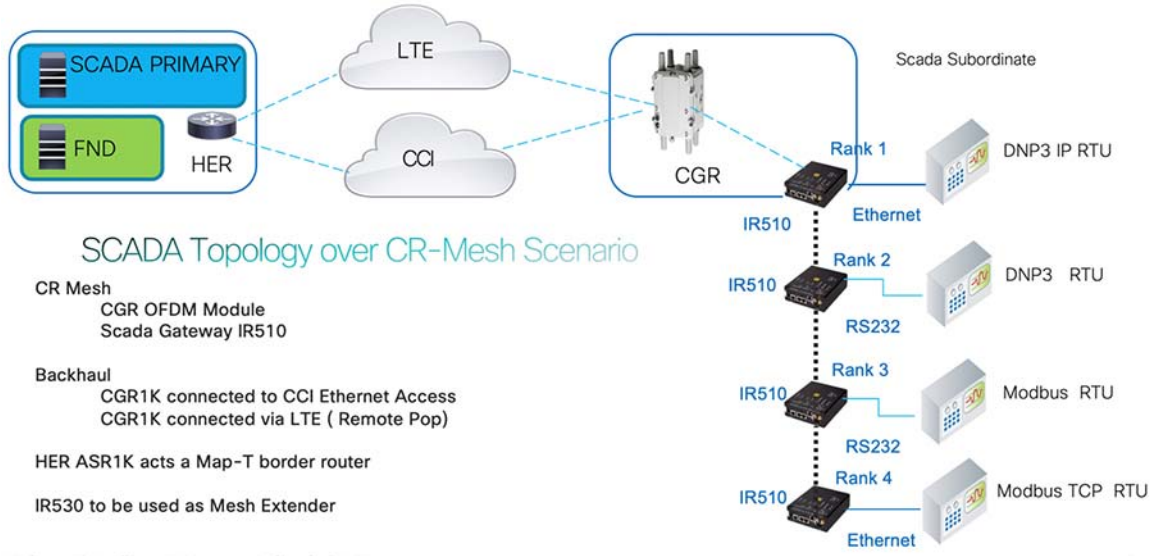
SCADA Operations

For SCADA Operations refer to SCADA Operations for DNP3, page 472.

SCADA Communication Scenarios over CR Mesh Network (IEEE 802.15.4)

In this scenario, the Control Center will be hosting SCADA applications (SCADA Primary/Subordinate). The SCADA Remote Device (PLC/RTU) is connected to the mesh node via the serial or Ethernet interface. The SCADA Primary/Subordinate residing in the Application Servers (Data Center) can communicate with the SCADA Remote Device (PLC/RTU) using the MODBUS/DNP3 protocol. IR510 acts as CR Mesh Gateway.

Figure 408 SCADA Topology over CR-Mesh Gateway



Operations that can be executed when the communication protocol is MODBUS IP, MODBUS Raw Socket are as follows:

- Read/Write Coil(s)—(Server > Client)
- Read/Write Holding Register(s)—(Server > Client)
- Read Discrete Input(s) and Input Register(s)—(Server > Client)

Operations that can be executed when the communication protocol is DNP3 or DNP3 IP are as follows:

- Poll (Primary > Subordinate)
- Control (Primary > Subordinate)
- Unsolicited Reporting (Subordinate > Primary) - Notification

The operations have been executed using a SCADA simulator known as the DTM simulator, which has the capability of simulating both the Server and the Client devices.

- If the endpoint is connected to mesh node via the Ethernet port, then it is pure IP traffic. The IP address of the SCADA Remote Device (PLC/RTU) can be NATed so that the same subnet between the SCADA Remote Device (PLC/RTU) and the Ethernet interface of the Gateway can be re-used. This approach will ease the deployment.
- If the endpoint is connected using asynchronous serial (RS-232 or RS-485), then tunneling of serial traffic using Raw Sockets must happen at the mesh node only.

This document focuses on SCADA protocol MODBUS.

For DNP3 related information refers to the section “SCADA Communication Scenarios over CR Mesh Network” (IEEE 802.15.4) in:

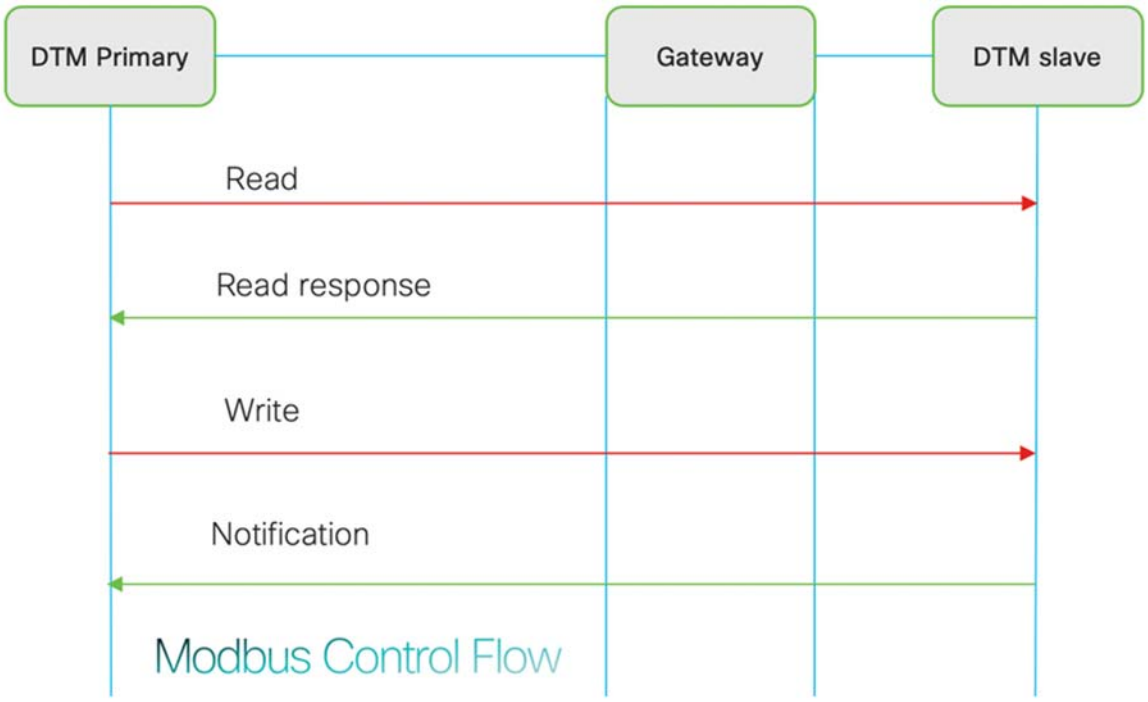
- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/IG/DA-FA-IG/DA-FA-IG.html#93131

The IR510 is implemented as a Mesh node, the CGR1240 is implemented as a FAR, and the ASR 1000s/CSR act as a HER, which terminates FlexVPN tunnels from the FAR and the HER.

IP-Enabled SCADA with MODBUS

- Protocol Validation—The protocol validated for this release is MODBUS.

Figure 409 MODBUS Control Flow for CR-Mesh Gateway



As shown in Figure 410, the SCADA Primary/Subordinate can perform a read and write operation to a remote Device via the Mesh Gateway.

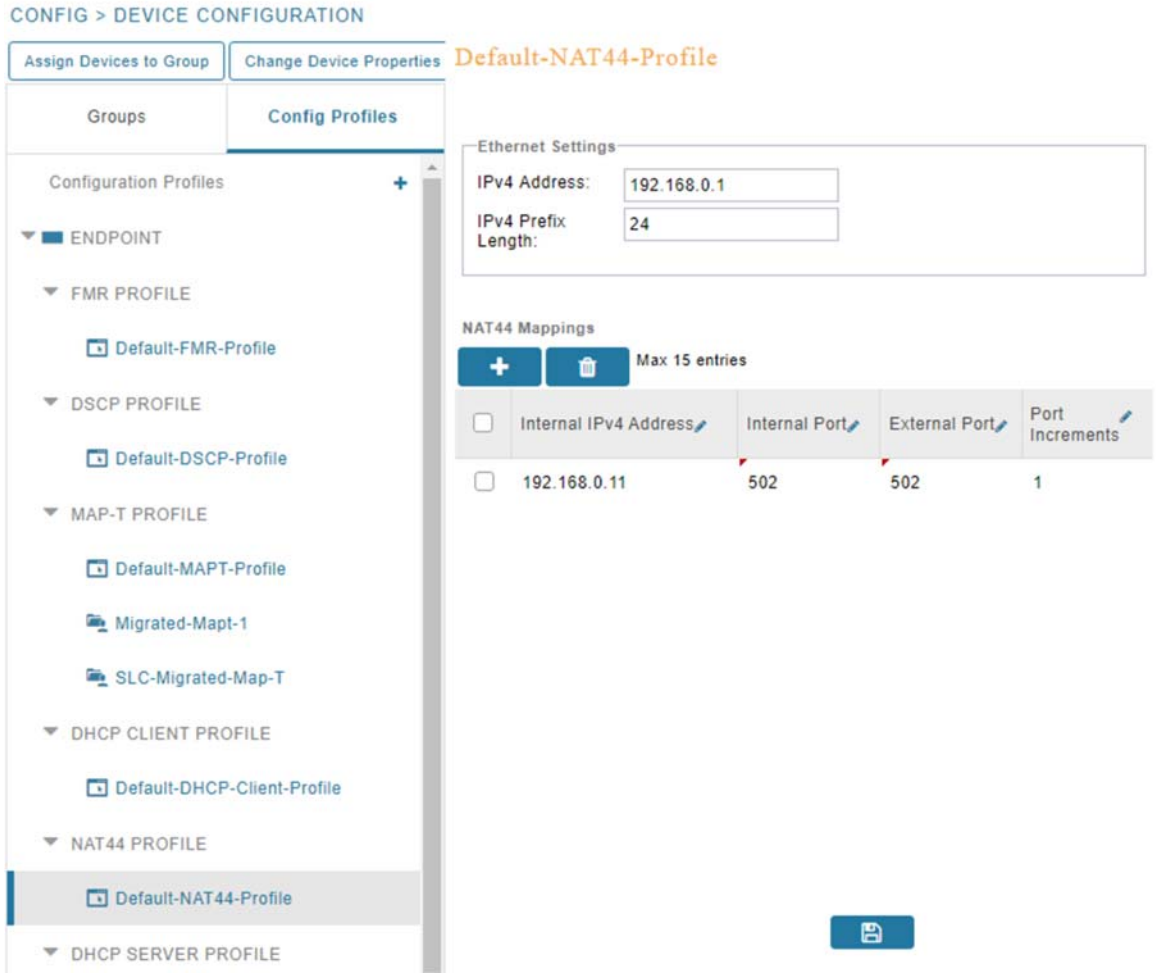
IR510 Mesh Gateway Configuration

This section describes the NAT44 configuration of the IR510 device. Basically IPv4 address assignment of the SCADA Remote Device (PLC/RTU) and the gateway IPv4 address and the port SCADA Remote Device (PLC/RTU) listens.

Note: Enable the front panel Ethernet Port on the **Configuration template** on FND.

For information on NMS management and MAP-T, refer to Enrollment of Cisco Resilient Mesh Endpoints–IR510, page 439.

Figure 410 NAT44 Configuration in FND (Config -> Device Configuration)

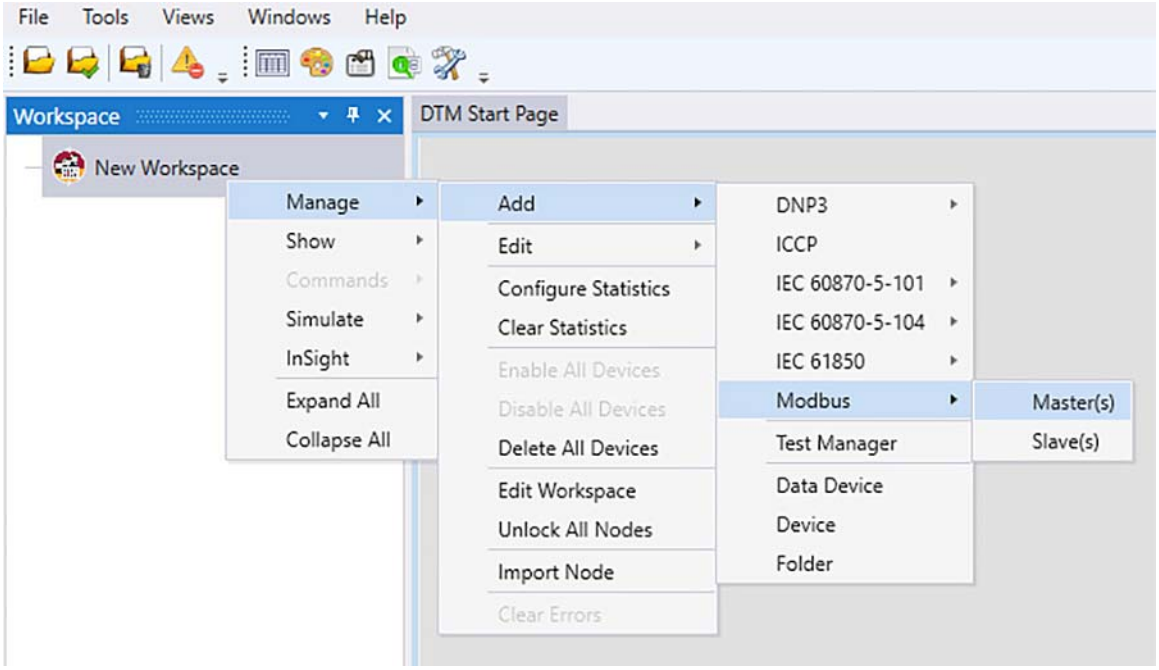


SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate resides in the Application Servers (Data Center). The following configuration must be required for the SCADA Primary/Subordinate to communicate with the SCADA Remote Device (PLC/RTU).

1. Open the **SCADA Primary Application** and click **Add a new MODBUS Server**.

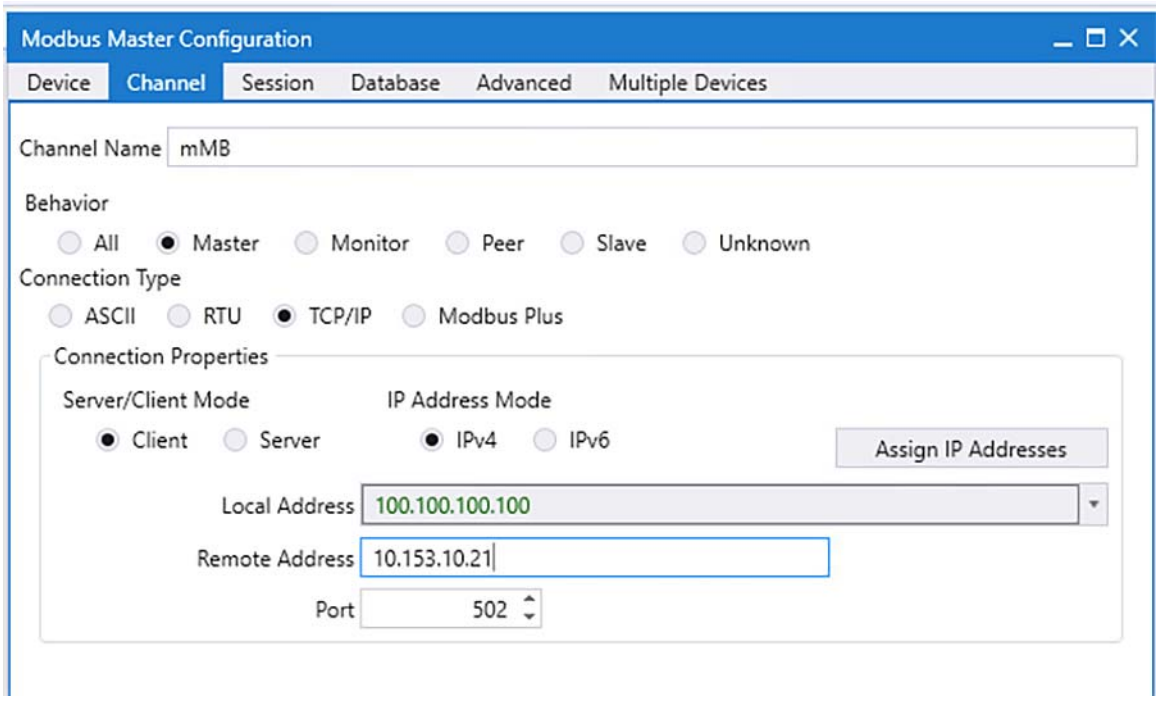
Figure 411 Creation of MODBUS Server



2. From the **Channel** tab, configure the SCADA Primary/Subordinate as shown in Figure 412.

The SCADA Primary/Subordinate, in this case, is configured as TCP Client, interacting with SCADA Remote Device (PLC/RTU), which is configured to act as the TCP Server.

Figure 412 Configuration of MODBUS Server



3. Populate the **Remote Address** field with the Map-T address of IR510.

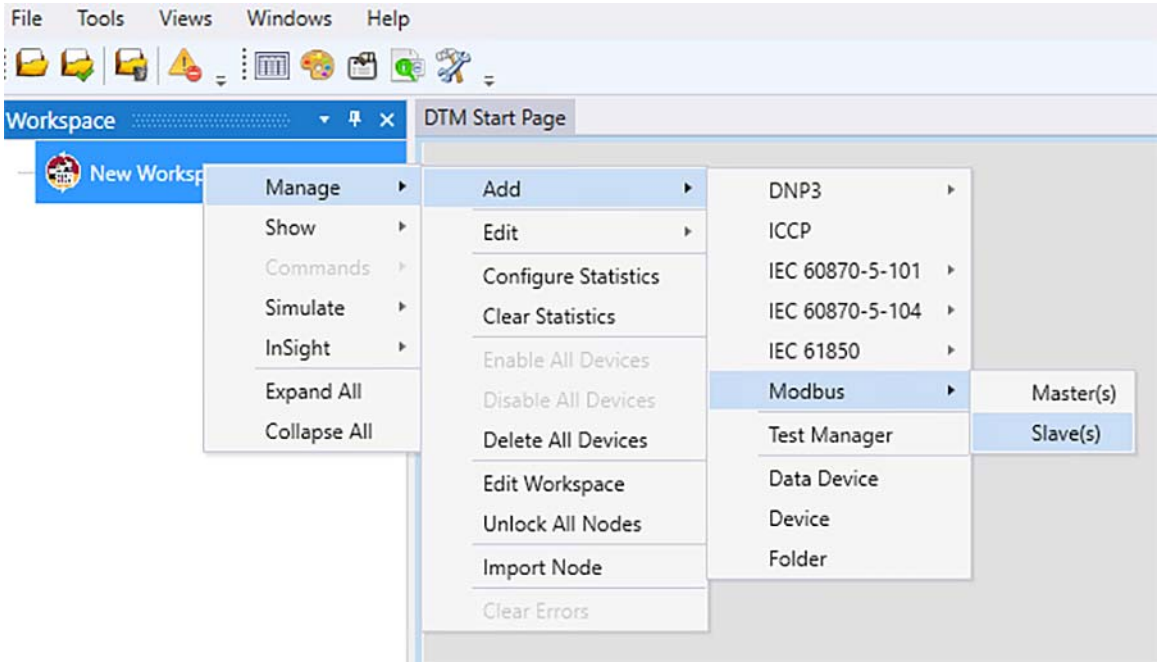
4. Populate the port with **502**, which is the port used in Cisco IOS Configuration.

SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) is residing in the field area. The following configuration is required for the SCADA Remote Device (PLC/RTU) to communicate with SCADA Primary/Subordinate.

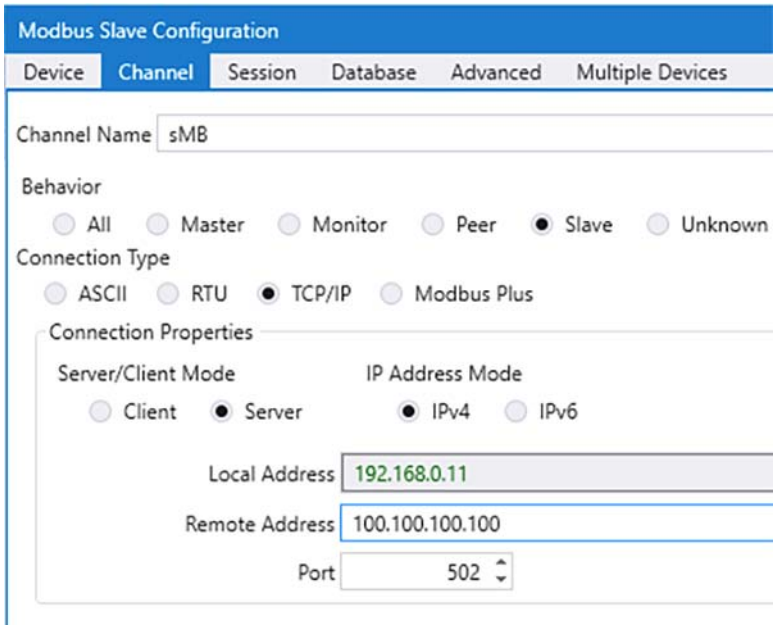
1. Open the **SCADA Remote Device Application** and click **Add a new MODBUS Client**.

Figure 413 Configuration of MODBUS Server



2. From the **Channel** tab, configure the SCADA Primary/Subordinate as shown in Figure 414.
3. Populate the **Remote Address** field with the SCADA Primary/Subordinate IP and Local Address is the SCADA Remote Device (PLC/RTU) local IP Address.
4. Populate the port with **502**, which is the port used in the SCADA Primary/Subordinate.

Figure 414 SCADA Primary/Subordinate Configuration



SCADA Operations

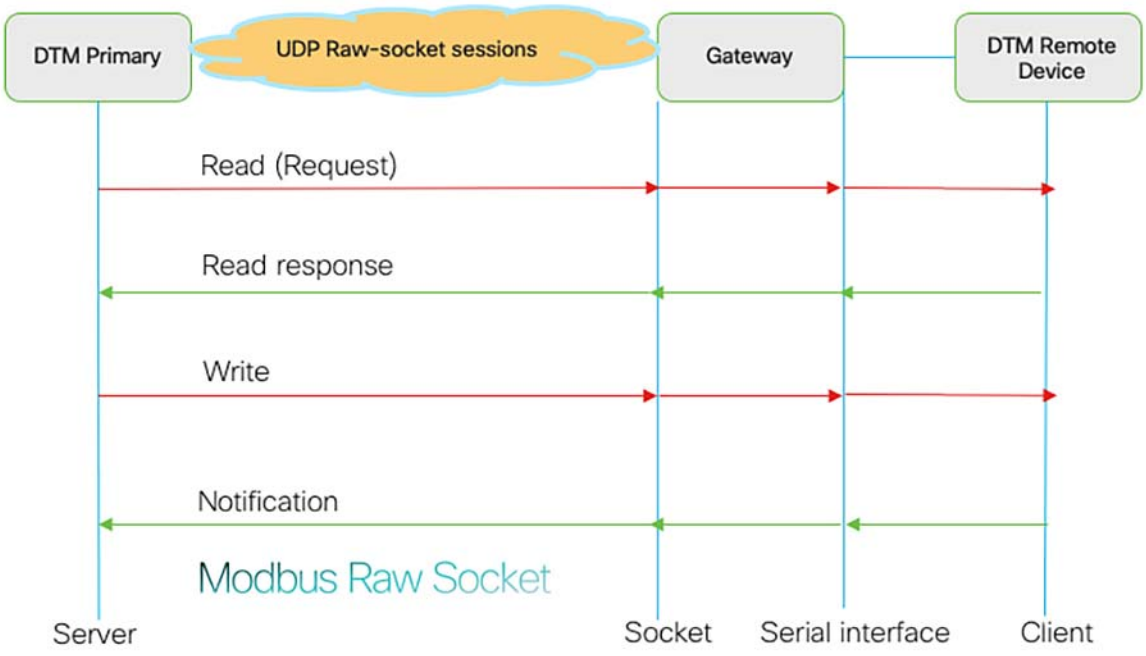
The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS, page 465.

SCADA Communication with Serial-based SCADA Using Raw Socket UDP

- Protocol Validation—The protocol validated for this release is MODBUS.

As shown in Figure 415, the SCADA Primary/Subordinate can poll and control the Remote Device via the Mesh Gateway using UDP Raw Socket.

Figure 415 MODBUS Control Flow



IR510 Mesh Gateway Raw Socket UDP Configuration

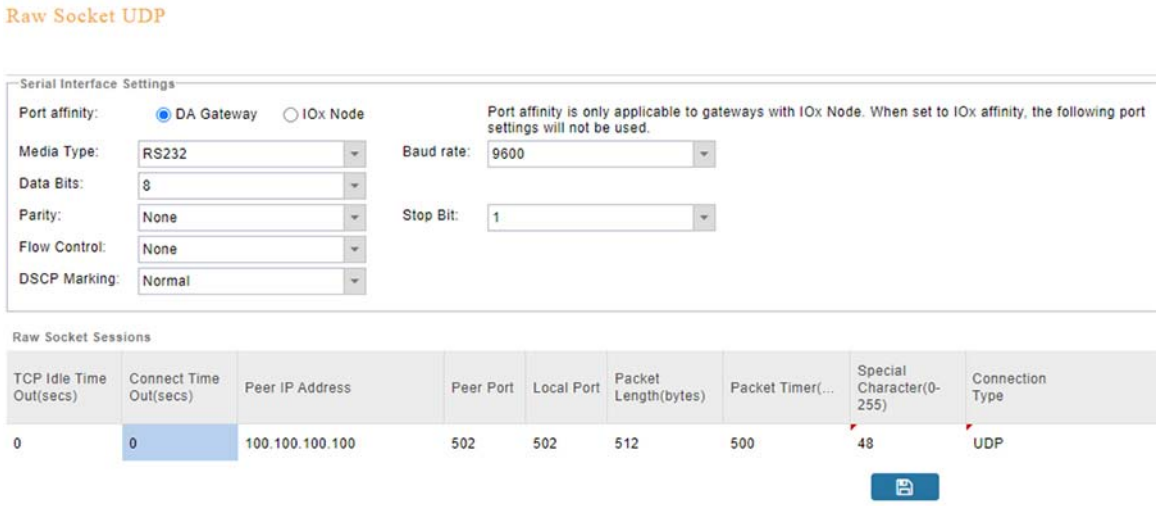
As per the topology, the SCADA Primary/Subordinate resides in the Control Center. There are three steps in the configurations on FND:

- Creation of serial profile.
- Linking of the serial profile to the configuration template.
- Configuration push to the device.

The following serial configuration profile requires the mesh node to communicate with the SCADA Primary/Subordinate.

- Peer IP Address—SCADA Primary/Subordinate IP Address.
- Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening.
- Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator.
- Packet Length and Packet Timer—Any integer value.
- Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

Figure 416 IR510 Mesh Node Raw Socket UDP Configuration

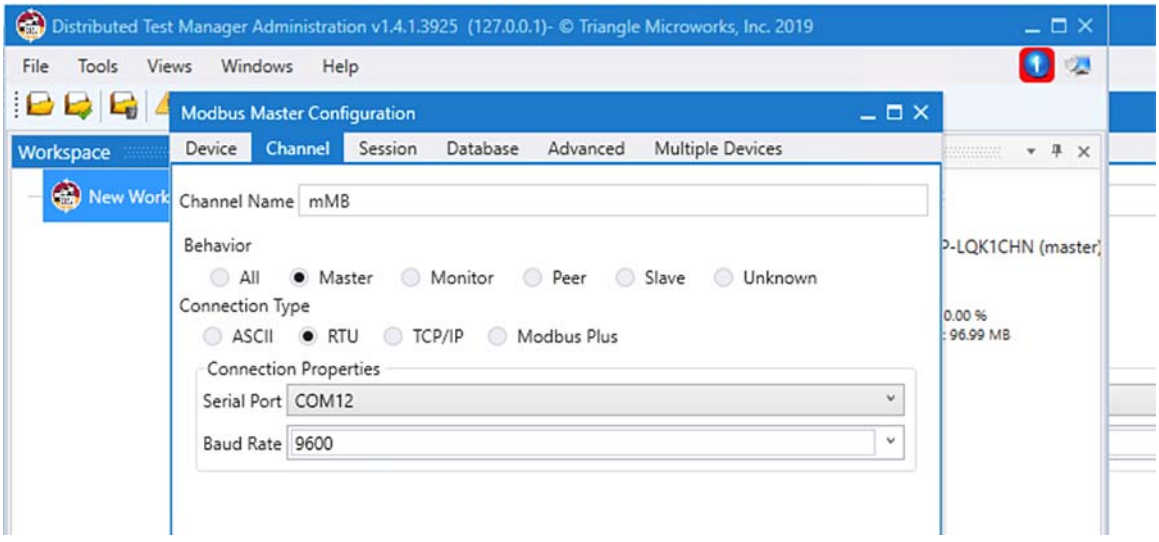


SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate resides in Control Center. The following configuration is required for the SCADA Primary/Subordinate to communicate with the SCADA Remote Device (PLC/RTU). In this implementation, MODBUS act as MODBUS Raw Socket Server. The configuration provided below is specific to MODBUS Raw socket.

1. Open the **SCADA Primary application** and click **Add a new MODBUS Server**.

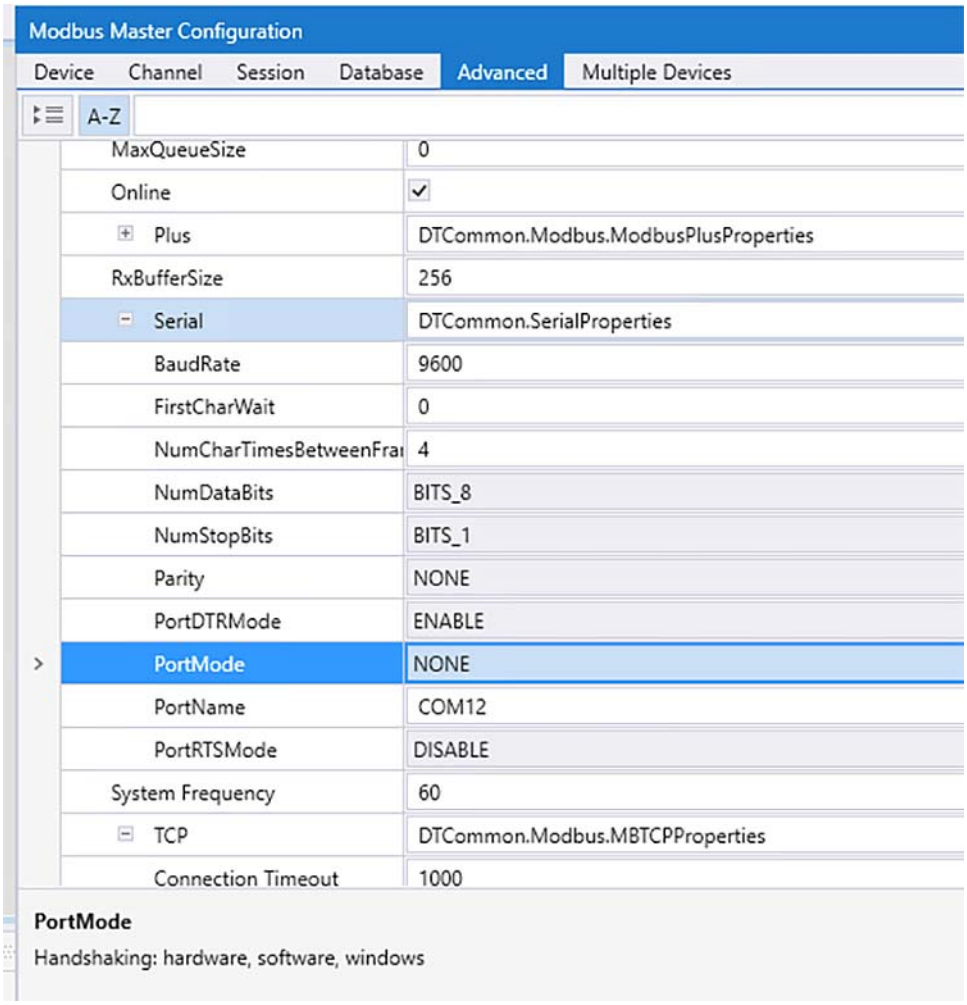
Figure 417 SCADA Primary/Subordinate Configuration



2. From the **Advanced** tab, configure the SCADA Primary/Subordinate as shown in Figure 418.

3. On the SCADA Primary/Subordinate, select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration.

Figure 418 SCADA Primary/Subordinate Details

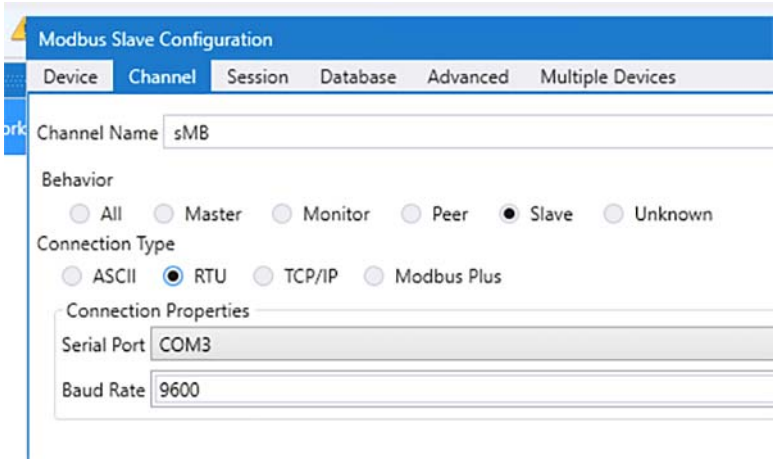


SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration is required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate. In this implementation, we used the SCADA DTMW simulator instead of a real SCADA device.

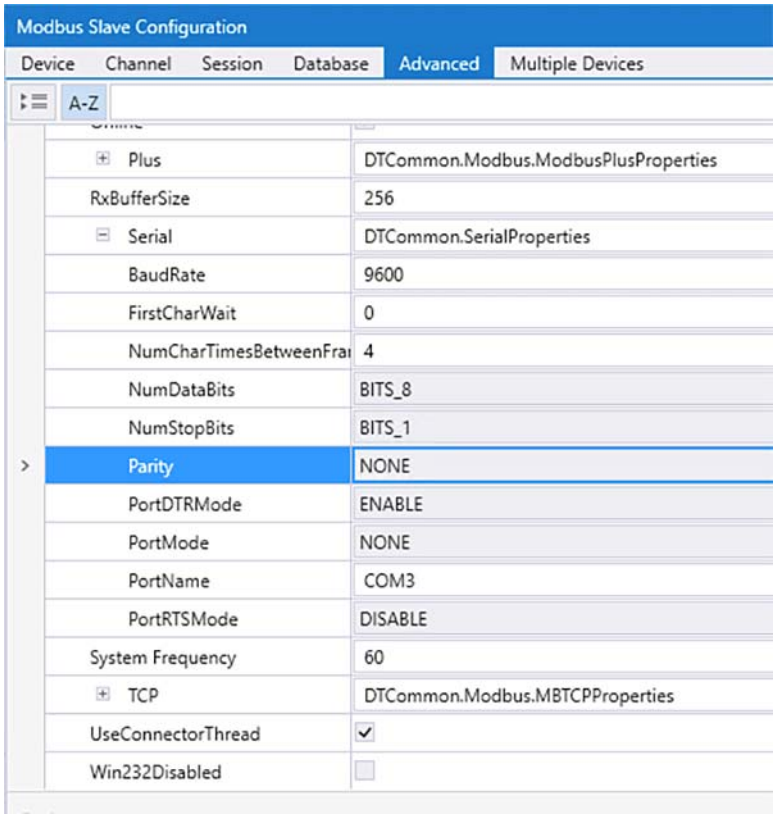
1. Open the **SCADA Remote Device application** and click **Add a new MODBUS Client**.
2. From the **Channel** tab, configure the SCADA Primary/Subordinate as shown in Figure 419.

Figure 419 SCADA Remote Device (PLC/RTU) Configuration



3. On the SCADA Remote Device (PLC/RTU), select the appropriate serial port, baud rate, data bits, stop bits, and parity matching your device configuration.

Figure 420 SCADA Remote Device (PLC/RTU) Variables Configuration



SCADA Operations

The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS, page 465.

SCADA Communication with Serial-based SCADA Using Raw Socket TCP

IR510 Mesh Gateway Raw Socket TCP Client Configuration

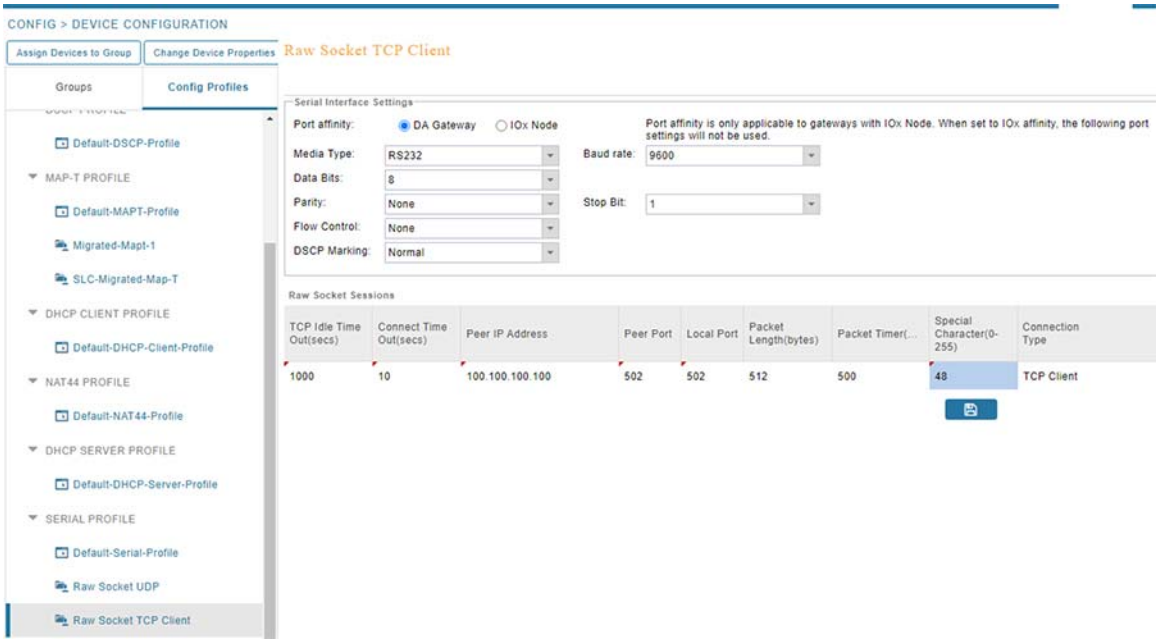
As per the topology, the SCADA Primary/Subordinate resides in the Application Servers (Data Center). There are three steps to the configuration on FND

- Creating the serial profile.
- Linking the serial profile to the configuration template.
- Pushing the configuration to the device.

The following serial configuration profile requires a mesh node to communicate with the SCADA Primary/Subordinate.

- Peer IP Address—SCADA Primary/Subordinate IP Address.
- Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening.
- Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator.
- Packet Length and Packet Timer—Any integer value.
- Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

Figure 421 Raw Socket TCP Client Configuration in FND for Serial-based SCADA Devices



IR510 Mesh Gateway Raw Socket TCP Server Configuration

As per the topology, the SCADA Primary/Subordinate resides in the Control Center. There are three steps to the configurations on FND

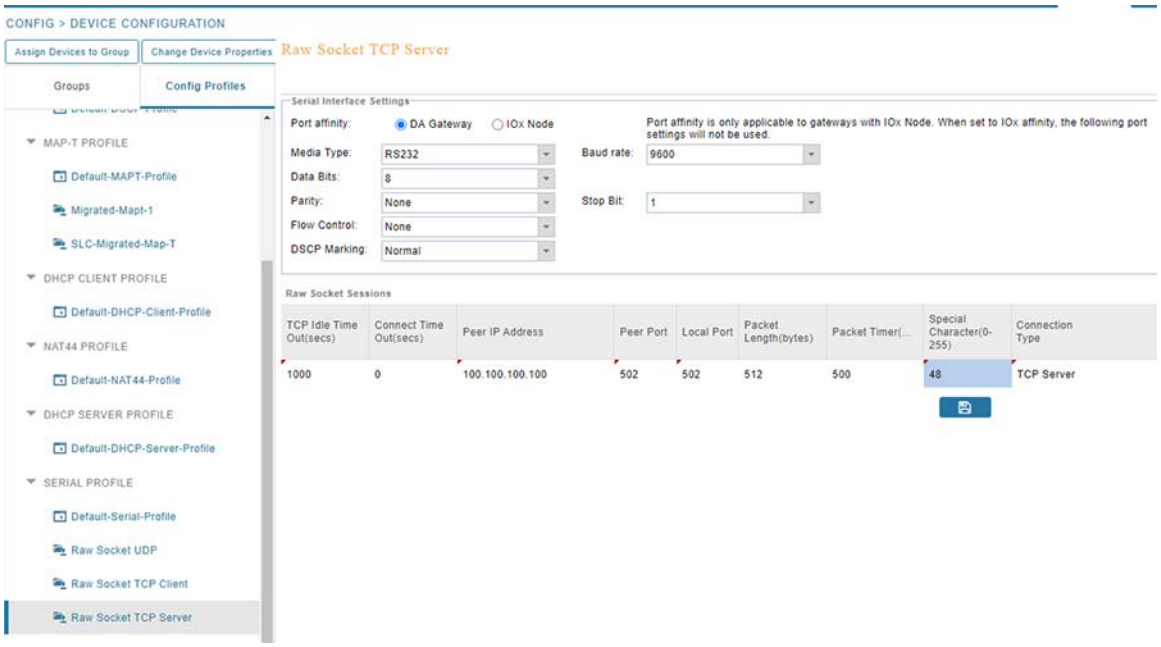
- Creating the serial profile.

- Linking the serial profile to the configuration template.
- Pushing the configuration to the device.

The following serial configuration profile requires a mesh node to communicate with the SCADA Primary/Subordinate.

- Peer IP Address—SCADA Primary/Subordinate IP Address.
- Peer Port—SCADA Primary/Subordinate Port Address, where SCADA Primary/Subordinate is listening.
- Local Port—This Port signifies the Raw Socket initiator port number. In this case, the IR510 node is the Raw Socket initiator.
- Packet Length and Packet Timer—Any integer value.
- Special Character—You can specify a character that will trigger the IR510 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR510 packetizes the accumulated data and sends it to the Raw Socket peer.

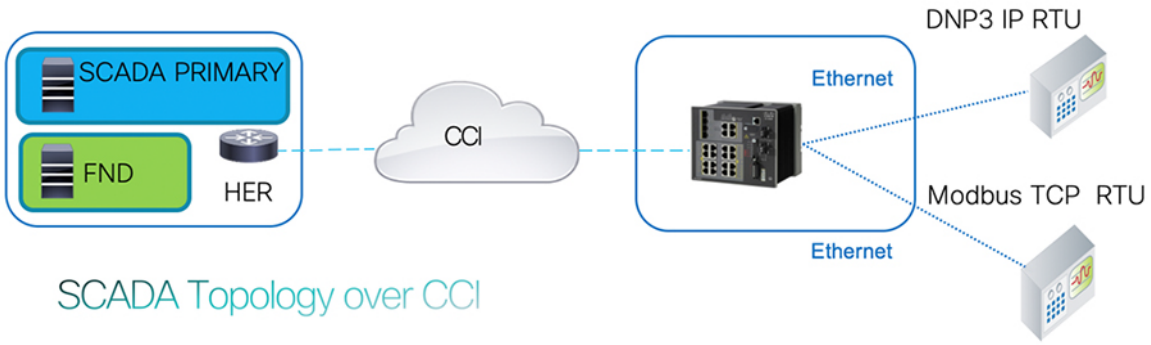
Figure 422 Raw Socket TCP Server Configuration in FND for Serial-based SCADA Devices



SCADA Communication Scenarios over CCI Network

In this scenario, the Application Servers (Data Center) will be hosting SCADA applications (SCADA Primary/Subordinate) in a Control Center. The SCADA Remote Device (PLC/RTU) is connected to IE Switch Access Ring, the transport is via CCI. The SCADA Primary/Subordinate residing in the Application Servers (Data Center) can communicate with the SCADA Remote Device (PLC/RTU) using the MODBUS/DNP3 protocol. Dot1x/MAB will be performed for end point AAA.

Figure 423 SCADA Topology via CCI Network



CCI Gateway (IE Switch) Configuration for MODBUS IP

SCADA Client is connected to CCI Access network to transport SCADA traffic over CCI and there is corresponding SCADA VLAN created.

The below address acts as Gateway IP address to connect to SCADA Primary/Subordinate via CCI:

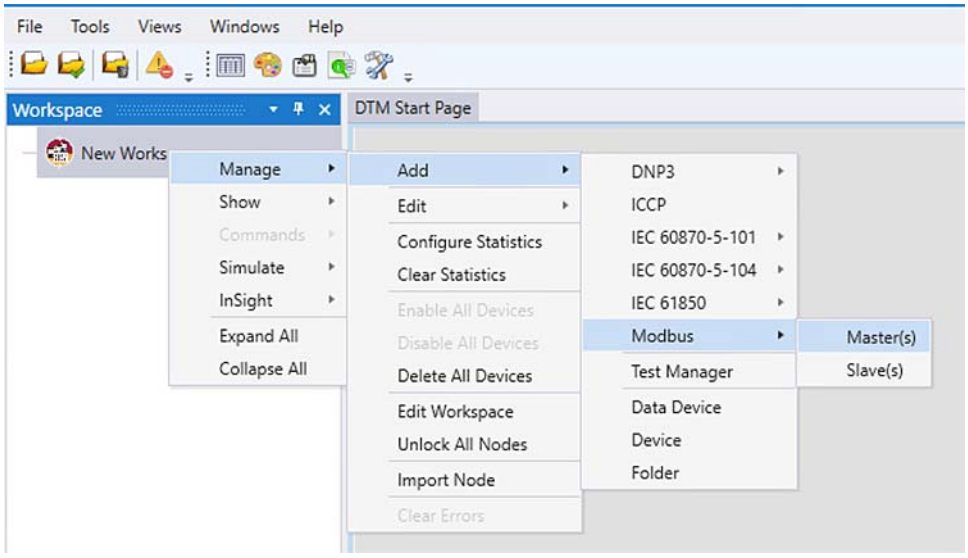
```
interface GigabitEthernet0
 switchport mode access
 switchport access vlan 125
 !
 interface Vlan125
 ip address dhcp
```

SCADA Primary/Subordinate Configuration

As per the topology, the SCADA Primary/Subordinate is residing in the Application Servers (Data Center). The following configuration must be required for the SCADA Primary/Subordinate to communicate with SCADA Remote Device (PLC/RTU).

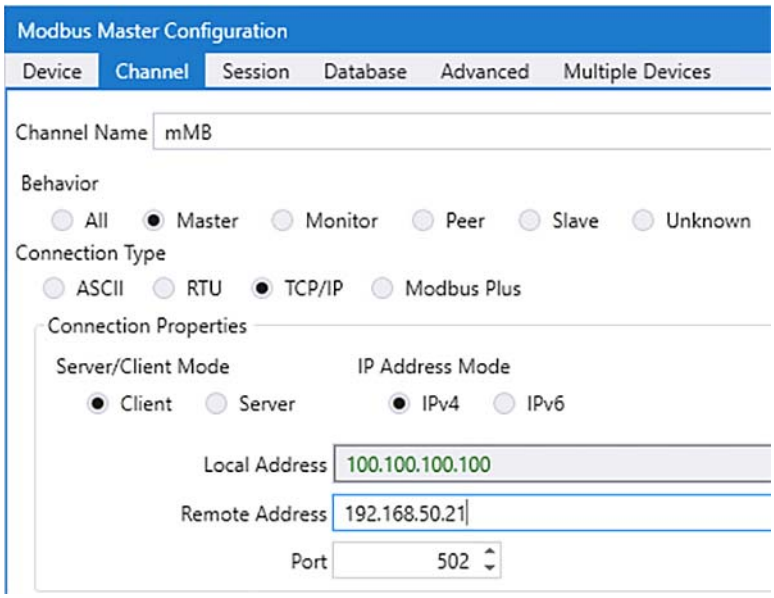
1. Open the **SCADA Remote Device application** and click **Add a new MODBUS Client**.

Figure 424 SCADA Primary/Subordinate Creation



2. From the **Channel** tab, configure the SCADA Primary/Subordinate, as shown in Figure 425.

Figure 425 SCADA Primary/Subordinate Configuration



3. SCADA Primary/Subordinate, in this case, is configured as a TCP Client interacting with the SCADA Remote Device (PLC/RTU), which is configured to act as TCP Server.

4. Populate the remote address field with the Loopback IP of the Cellular gateway (Remote Address should be loopback IP of IR1101, with NAT/PAT configuration redirecting the IP and Port to the SCADA Remote Device (PLC/RTU)).

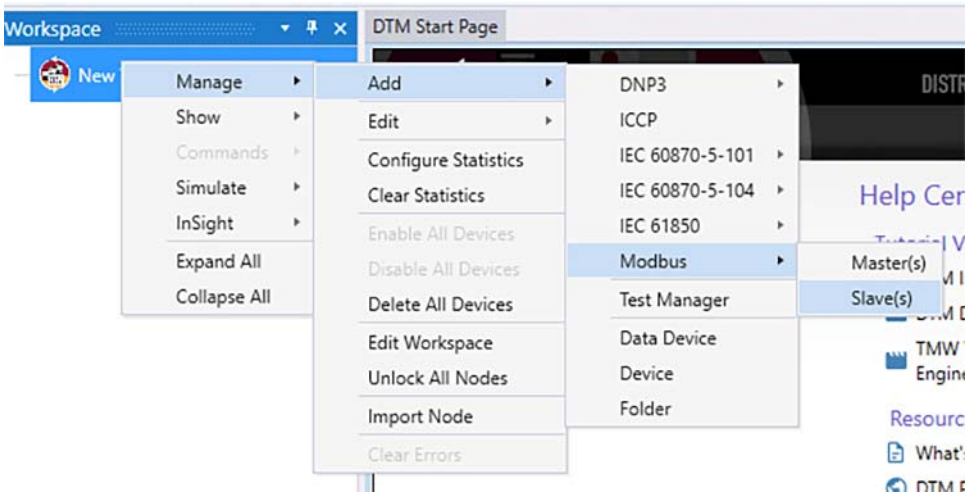
5. Populate the port with **502**, which is the port used in SCADA Primary/Subordinate.

SCADA Remote Device (PLC/RTU) Configuration

As per the topology, the SCADA Remote Device (PLC/RTU) resides in the field area. The following configuration must be required for the SCADA Remote Device (PLC/RTU) to communicate with the SCADA Primary/Subordinate.

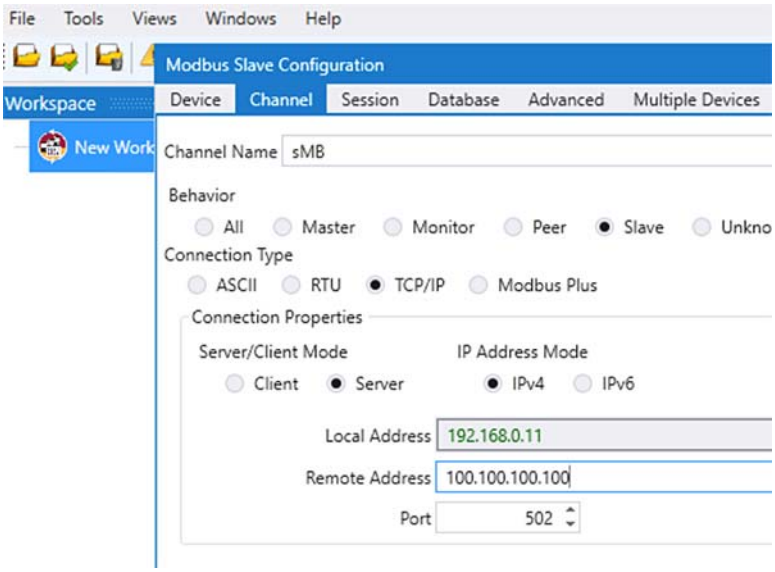
1. Open the **SCADA Remote Device application** and click **Add a new MODBUS Client**.

Figure 426 SCADA End Device Creation



2. From the **Channel** tab, configure the SCADA Remote Device (PLC/RTU), as shown in Figure 427.

Figure 427 SCADA End Device Configuration



3. Populate the remote address field with SCADA Primary/Subordinate IP and Local Address as SCADA Remote Device (PLC/RTU) IP.

4. Populate the port with **502**, which is the port used in SCADA Primary/Subordinate.

SCADA Operations

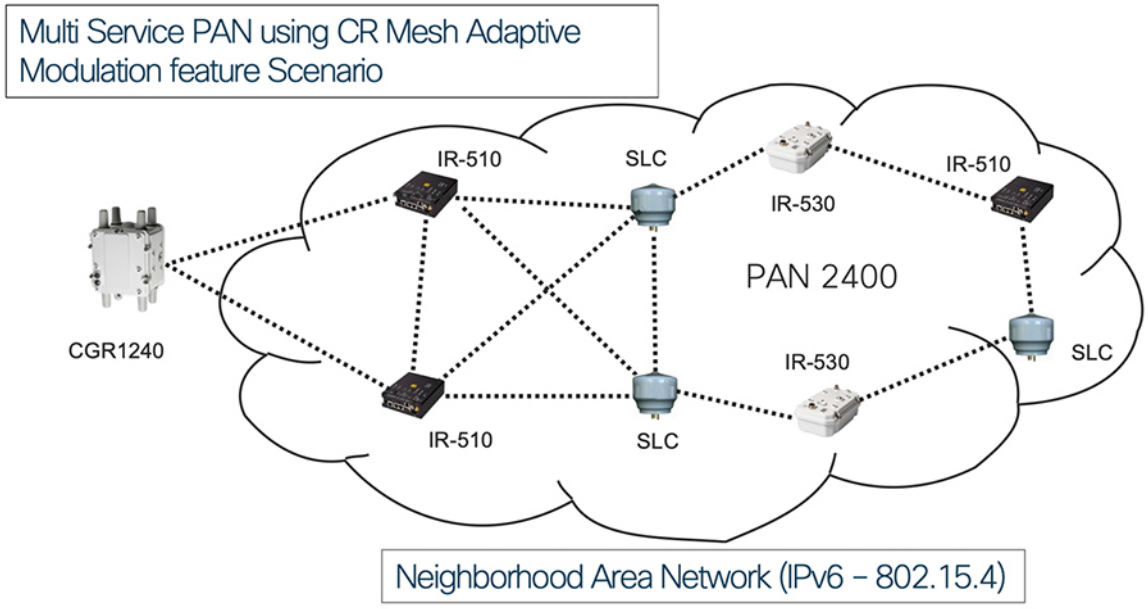
The SCADA operations are similar for MODBUS TCP. Refer to SCADA Operations for MODBUS, page 465.

Implementing Multi-Service PAN Using CR Mesh Adaptive Modulation Feature

Cisco Resilient Mesh is a sub-Gigahertz mesh capable wireless solution. Through software enhancements, Cisco resilient mesh has been enhanced so that new mesh nodes can be configured with adaptive modulation. Adaptive modulation is backward compatibility with the classic Cisco Resilient Mesh network which uses 2FSK(Frequency-Shift

Keying) modulation and improves the transmitting ability by adding OFDM (Orthogonal Frequency Division Multiplexing) modulation. Many environments will include both 2FSK and OFDM devices and will need to operate with both simultaneously as part of an ongoing strategy or as part of system migration. Operators need to understand the implications of operating both modulation types in a single environment. The Adaptive Modulation technique maximizes data transmission rate in the limited bandwidth which results in optimum utilization of frequency band and it has advantage of flexible and high data transmission rate along with utilization of spectrum.

Figure 428 Multiservice PAN Using CR-Mesh Adaptive Modulation



Note: Multi Service PAN supports OFDM option phy-mode or OFDM option plus 2FSK phy-mode. In the sample illustration we are using Cimcon SLC as 2FSK CGE and Cisco IR510 running OFDM as Mesh Gateway for connecting SCADA endpoints.

Prerequisites

IR510 and SLC are loaded with Node Certificates, FND Certificates, Root CA Certificate of ECC CA Server (User can refer to below link for how to generate the SLC Node certificate and IR510 certificate), XML and configwriter tool. Only CGR WPAN configuration is discussed in this section.

Table 36 Software Versions Tested for Adaptive Modulation

Device	Phy-mode	Version	Function
IR510	OFDM	6.2(6.2.19)	SCADA Mesh Gateway
SLC	2FSK	2.0.15	CR-Mesh End Point -Cimcon Lighting Device
Cisco CGR 1240 WPAN	OFDM Module (CGM-WPAN-OFDM/1.0/2.0)	6.2(6.2.19)	Cisco Mesh Gateway

CSMP Client Certificate Generation

Note: CSMP Client is required to load the certificates into IR-510. Refer to Enrollment of Cisco Resilient Mesh Endpoints—IR510, page 439 for CSMP Client Information.

Dot1x Authentication

IR-510 and SLC are securely authenticated through the WPAN module (Interface Wpan4/1 below) and CGR router at the edge of the network acts as Authenticator with the RADIUS Server which is located in data center. Once the dot1x authentication is succeeded (as shown below), the SLC and IR-510 will get 6Lowpan IPv6 address from DHCP Server.

```
Sep  2 13:05:39.891: %AUTHMGR-5-START: Starting 'dot1x' for client (0310.00e9.066a) on Interface
Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E
Sep  2 13:05:54.821: %DOT1X-5-SUCCESS: Authentication successful for client (0310.00e9.066a) on
Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E
Sep  2 13:05:54.821: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0310.00e9.066a) on Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E
Sep  2 13:05:54.823: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (0310.00e9.066a) on
Interface Wpan4/1 AuditSessionID C0A8C80A00000000005C8C4E
```

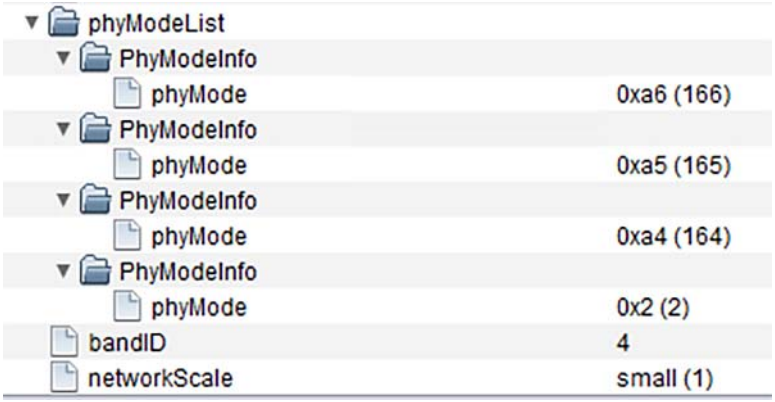
End Point Devices

Operators will want to ensure the proper channels are configured on the 2FSK and OFDM endpoints as well as the WPAN module in the CGR.

The example below shows the phy-mode configuration of the IR-510 with multiple values (Multi OFDM and Single FSK): 166,165,164,2 (Self-adapting data rates based on the channel condition). User need to post multiple phy-modes for OFDM device using CSMP client.

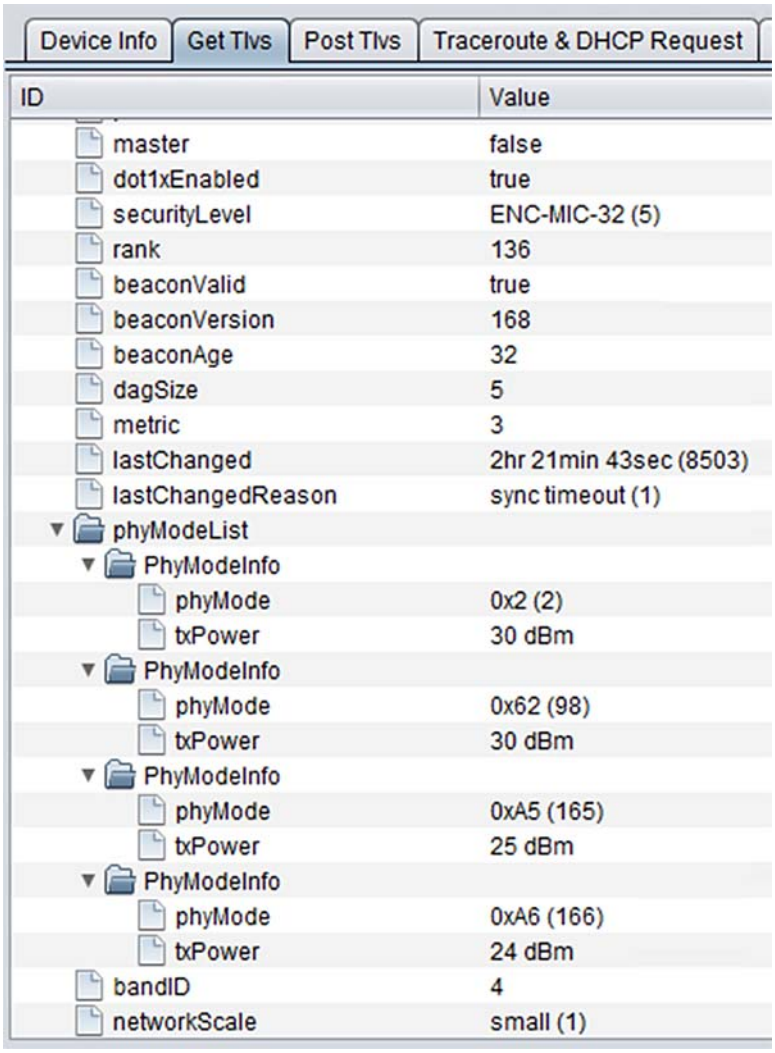
User can verify this IR-510 console (CSMP Client) and select post TLV 35 to configure multiple phy-mode values as shown in Figure 431. (This step is mandatory to configure multiple values in IR-510.)

Figure 429 Showing Multiple phy-modes in CSMP Client GUI



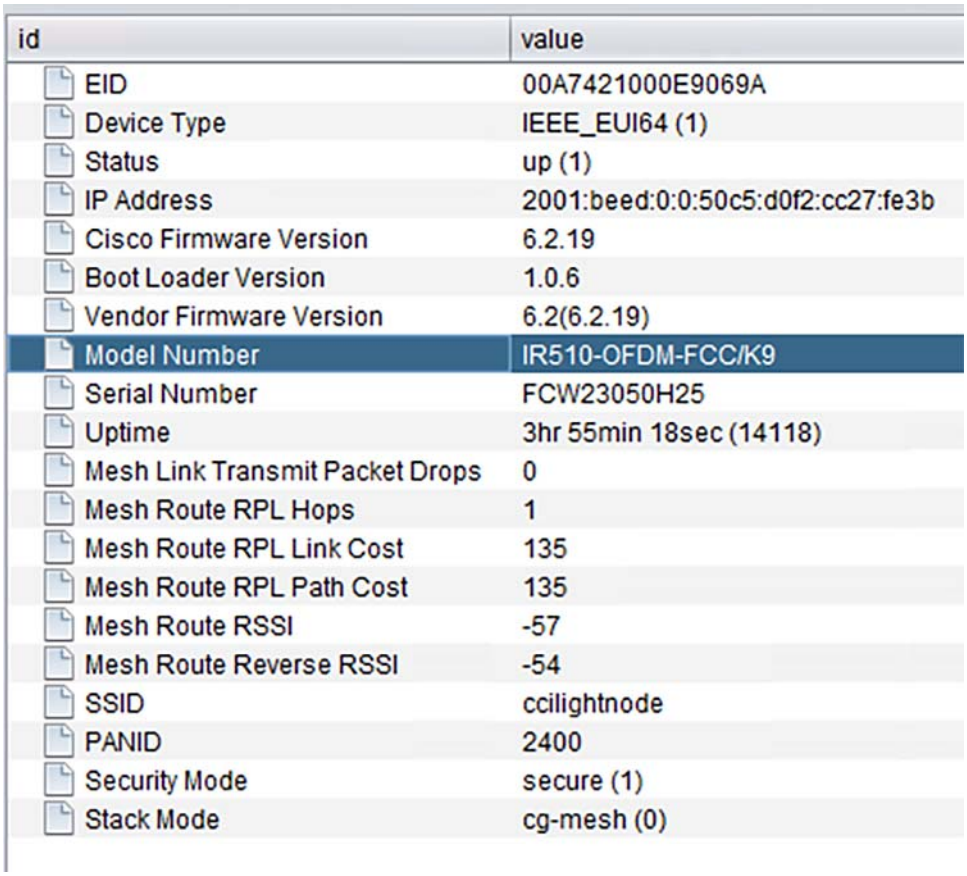
Phy-Modes in IR-510

Figure 430 Showing Details of dot1x and Multiple phy-modes in CSMP Client GUI



IR 510 Configuration Settings

Figure 431 Showing Details of IR510

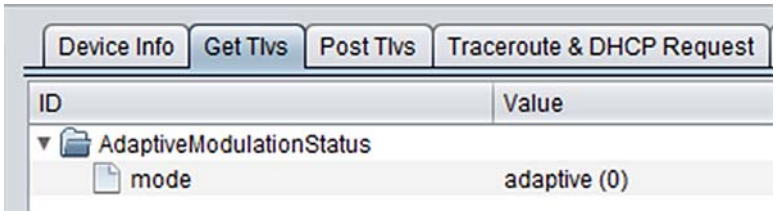


id	value
EID	00A7421000E9069A
Device Type	IEEE_EUI64 (1)
Status	up (1)
IP Address	2001:beed:0:0:50c5:d0f2:cc27:fe3b
Cisco Firmware Version	6.2.19
Boot Loader Version	1.0.6
Vendor Firmware Version	6.2(6.2.19)
Model Number	IR510-OFDM-FCC/K9
Serial Number	FCW23050H25
Uptime	3hr 55min 18sec (14118)
Mesh Link Transmit Packet Drops	0
Mesh Route RPL Hops	1
Mesh Route RPL Link Cost	135
Mesh Route RPL Path Cost	135
Mesh Route RSSI	-57
Mesh Route Reverse RSSI	-54
SSID	ccilightnode
PANID	2400
Security Mode	secure (1)
Stack Mode	cg-mesh (0)

Adaptive Modulation Settings in IR 510

User can verify it by selecting the TLV -157.

Figure 432 Showing Details of IR510 Adaptive Modulation Options



Cimcon Street Light Controller

In this use case Cimcon SLC operates on 2FSK Mode and Phy-Mode Configured : 98. User can configure phy-mode as 2 for 2FSK (Classic 2FSK Mode).

[98:Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz]

Version Compatibility:

The below versions are tested in the use case. The user can go with the versions below or higher recommended version:

- CGR Version Tested (make sure CGR Version must be greater than 15.8(3)M):

```
CGR1240_ FTXXXXXX #show version
Cisco IOS Software, cgr1000 Software (cgr1000-UNIVERSALK9-M), Version 15.9(3)M2, RELEASE SOFTWARE
(fc1)
```

- WPAN Version Tested:

```
CGR1240_FTXXXXXX#show wpan 4/1 hardware version
firmware version: 6.2(6.2.19), cg-mesh-bridge, origin/master, 1bf449d, Jan 22 2020
```

- IR-510 Version Tested:

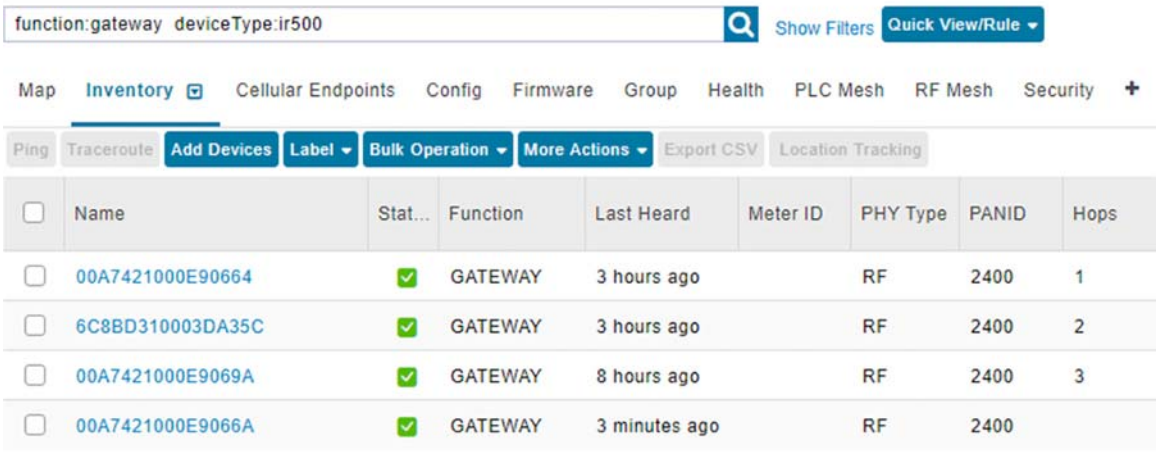
  Cisco Firmware Version 6.2.19

IR-510 Onboarding into FND

For onboarding IR-510 into FND, refer to Enrollment of Cisco Resilient Mesh Endpoints–IR510, page 439.

Once onboarding is completed, user is able to see IR510 as shown in Figure 433.

Figure 433 Display of IR510 in FND



SLC Nodes Displayed in FND

Refer to Secure Onboarding of Mesh Nodes into CR Mesh, page 444 to display SLC Nodes into FND:

Figure 434 Display of SLC Nodes in FND

Name	Stat...	Function	Last Heard	Meter ID	PHY Type	PANID	Hops
00173B140023004D	✓	CGE	17 minutes ago		RF	2400	2
00173B1400180043	✓	CGE	2 hours ago		RF	2400	2
00173B110023002A	✓	CGE	2 hours ago		RF	2400	2

CGR PAN Aggregator Configuration (WPAN Configuration)

CGR OFDM WPAN should be configured to 166, 165, 164, 2. Cisco supports OFDM and single FSK phy-mode.

```
CGR1240_FTXXXXXXW#show run int wpan 4/1
Building configuration...

Current configuration : 709 bytes
!
interface Wpan4/1
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 load-interval 30
 ieee154 phy-mode 166 165 164 2 << User can configure multiple phy-modes
 ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
 ieee154 dwell window 12400 max-dwell 400
 ieee154 panid 2400
 ieee154 ssid ccilightnode
 ieee154 txpower 25
 ieee154 beacon-ver-incr-time 15
 outage-server 2001:DB8:16:110::151 << FND IP Address
 rpl dag-lifetime 60
 rpl dio-dbl 2
 rpl dio-min 14
 rpl version-incr-time 10
 authentication host-mode multi-auth
 authentication port-control auto
 ipv6 address 2001:BEED::1/64
 ipv6 enable
 ipv6 dhcp server man-dhcpd6 rapid-commit
 no ipv6 pim
 dot1x pae authenticator
 mesh-security mesh-key lifetime 259200
end
```

CGR WPAN Neighbor Table:

```
. CGR1240_FTXXXXXXW#show wpan 4/1 link-neighbors table
------------------------- WPAN LINK NEIGHBOR TABLE [4] --------------------

EUI64              RSSIF RSSIR LQIF LQIR FIRST_HEARD LAST_HEARD  MODF MODR
00173B110023002A   -72   -68   12   66   13:16:21    13:21:31    2     2
00173B1400180043   -66   -63   15   61   13:14:13    13:21:32    2     2
00173B140023004D   -73   -66   8    64   13:15:28    13:21:30    2     2
00173B1400410042   n/a   -76   n/a  74   13:20:44    13:23:10    n/a   n/a
00A7421000E9066A(IR)-87   -90   84   86   13:05:39    13:12:42    166   166
00A7421000E9069A   -50   -57   51   55   13:13:50    13:24:11    2      2
Number of Entries in WPAN LINK NEIGHBOR TABLE: 6
```

RPL Tree Formation:

```
CGR1240_FTX2233G00W#show wpan 4/1 rpl tree
---------------------------- WPAN RPL TREE FIGURE [4] --------------------

  [2001:BEED::1] (5/6)
          \--- 2001:BEED::50C5:D0F2:CC27:FE3B (1) << IR 510
                  \--- 2001:BEED::3080:135:63C5:940E << SLC Node
          \--- 2001:BEED::CC3:8BE3:254D:96F4
          \--- 2001:BEED::D0C2:3233:DF13:D8ED
          \--- 2001:BEED::E119:434D:E8C8:6C30
          \--- 2001:BEED::E5BA:B8F9:AD9:96F6

RPL TREE: Num.DataEntries 6, Num.GraphNodes 7

CGR1240_FTX2233G00W#show wpan 4/1 rpl etree
---------------------------- WPAN RPL EUI64 TREE [4] --------------------

  [78725D1000BA6D59]
          \--(-71)-- 00173B110023002A
          \--(-70)-- 00173B1400180043
          \--(-70)-- 00173B140023004D
          \--(-88)-- 00A7421000E9066A
          \--(-50)-- 00A7421000E9069A << IR510
                  \--(-37)-- 00173B1400410042 << SLC Node

RPL EUI64 TREE: Num.DataEntries 6, Num.GraphNodes 7

RPL WPAN Configuration:

CGR1240_FTX2233G00W#show wpan 4/1 config
Module Type:    RF-WPAN (IEEE 802.15.4e/g RF OFDM)
ssid:           ccilightnode
panid:          2400
phy_mode:       166 165 164 2
band-id:        4
transmit power: 25
channel:        254
dwell:          window 12400 max-dwell 400
fec:            n/a
beacon async:   min-interval 15 max-interval 60 suppression-coefficient 1
security mode:  1
test mode:      0 (test firmware only)
admin_status:   up
rpl prefix:             2001:BEED::1/64
rpl route-poisoning:    off
rpl dodag-lifetime:     60
rpl dio-dbl:            2
rpl dio-min:            14
rpl version-incr-time:  10
rpl pon instance:       off
detach bridge:          no
bootloader mode:        no
mcast-agent:            FF38:40:2001:BEED::1 61624 61628 1153
firmware version:       6.2(6.2.19)
slave mode:             no
wisun mode:             no
ieee154 bv: 466 bv/4: 116
ieee154 beacon ver incr time: 15 seconds
```

Hardware Configuration of WPAN:

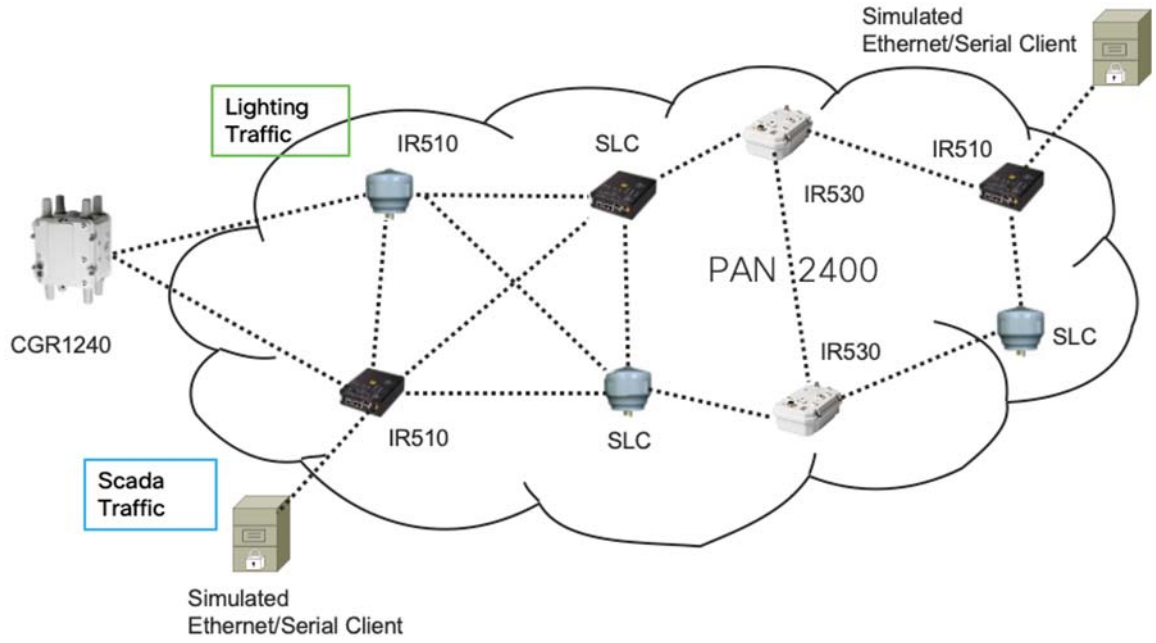
```
CGR1240_FTXXXXXXX#show wpan 4/1 hardware config
<- Removed Cisco Device Specific information->
ssid:           ccilightnode
panid:          2400
phy-modes:      2 164 165 166
band-id:        4
transmit power: 30  (<-txpower_reg 0x18)
channel:        254
channel notch:  none
dwell:          window 12400 max-dwell 400
fec:            n/a
beacon async:   min-interval 15 max-interval 60 suppression-coefficient 1
security mode:  1,  frame counter mode: 1
admin_status:   up
wisun mode:     0
```

Traffic Simulation from SCADA and Lighting Applications

Traffic testing (sending and receiving) from SCADA and lighting applications are happening at the same time.

In this scenario, the Adaptive Modulation technique is used to communicate with both OFDM devices and 2FSK devices as shown in the Figure 435.

Figure 435 Simultaneous Traffic Flow with SCADA End Point and Lighting Node

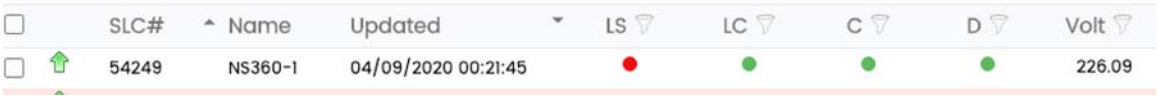


Step 1: Go to the **Cimcon Lighting Dashboard** and select the **Status** option, which will display all the lights.

Figure 436 Cimcon Status of Lights Dashboard

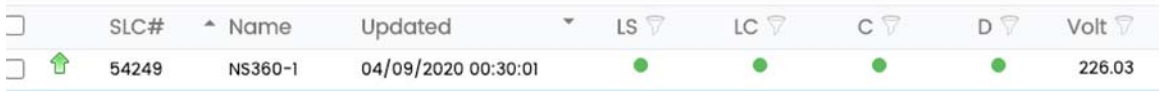
Step 2: Select the particular light(s) and go to the commands drop-down menu and select **Turn On/Off** (or vice versa). The command will be sent to the device.

Figure 437 Communication of Lights when in OFF State



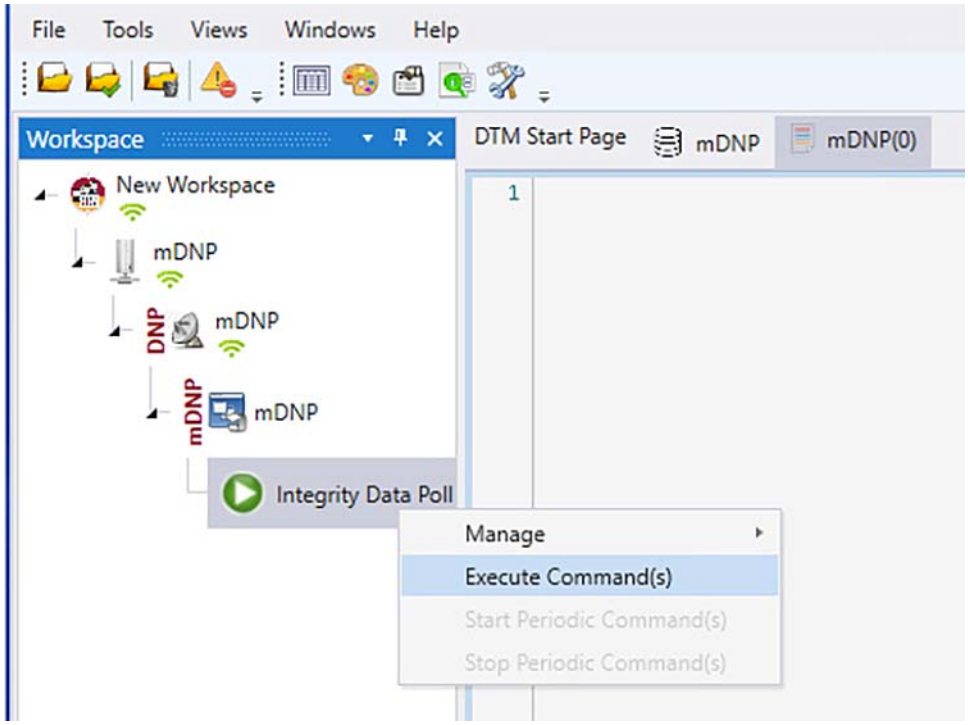
Step 3: Device got Powered On. The 2FSK communication is occurring.

Figure 438 Communication of Lights when in ON State



Step 4: This is an example of DNP3 IP Poll-Send Polling Request (Integrated Data Poll) from the SCADA Primary/Subordinate to Client.

Figure 439 DNP3 Data Polling from DNP3 Remote Device



SCADA Server showing results for IDP-Integrated Data Polling (Server polls the data from Client).

Figure 440 DNP3 Server Polling Request and Response

```
14:50:01.285:
14:50:01.285: <+++ mDNP       Build DNP3 Message: Class Data Poll
14:50:01.285:
14:50:01.285:                 Tx Object 60(Class Data), variation 2, qualifier 0x06(All Points)
14:50:01.285:
14:50:01.285:                 Tx Object 60(Class Data), variation 3, qualifier 0x06(All Points)
14:50:01.285:
14:50:01.285:                 Tx Object 60(Class Data), variation 4, qualifier 0x06(All Points)
14:50:01.285:
14:50:01.285:                 Tx Object 60(Class Data), variation 1, qualifier 0x06(All Points)
14:50:01.285:
14:50:01.285: <+++ mDNP       Insert request in queue: Class Data Poll
14:50:01.285:
14:50:01.285: <=== mDNP       Application Header, Read Request
14:50:01.285:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 7
14:50:01.285:                 c7 01 3c 02 06 3c 03 06 3c 04 06 3c 01 06
14:50:01.285:
14:50:01.285:
14:50:01.285:  ### mDNP - 153.153.10.23:20000 - TCP transmit 27 bytes
14:50:01.441:
14:50:01.441: ===> mDNP       Application Header, Response
14:50:01.441:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 7
```

SCADA Client Response for the above IDP (Client sends the date to server).

Figure 441 DNP3 Client Response

```
07:30:02.016:                28 02 00 00 18 01 00 00 01 00 00 01 00 00 01 00
07:30:02.017:                00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00
07:30:02.017:                01 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01
07:30:02.017:                00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00
07:30:02.017:                00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00
07:30:02.017:
07:30:02.017:
07:30:02.017:  ### sDNP - 100.100.100.100:20000 - TCP transmit 292 bytes
07:30:02.017:
07:30:02.017:  ### sDNP - 100.100.100.100:20000 - TCP transmit 292 bytes
07:30:02.017:
07:30:02.017:  ### sDNP - 100.100.100.100:20000 - TCP transmit 243 bytes
```

For SCADA testing using IR 510, user needs to configure Map-T based configurations on CGR, HER, FND, and IR 510. Refer to IoT Gateway Onboarding and Management, page 437 for the configurations and procedure.

References

- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/modules/wpan_cgmesh/b_wpan_cgmesh_IOS_cfg.html
- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/modules/release_notes/b_cgmesh_rn_6_0.html
- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/DG/DA-FA-DG.pdf

Frequently Asked Questions

- Do users have to configure all four Phy-modes on WPAN module for Adaptive modulation to operate?

  Not necessarily, 166 165 2 it is also working configuration. Adaptive modulation supports multiple phy-modes of OFDM. The user has the flexibility to configure two OFDM phy-modes instead of three depending on requirements, but only one 2FSK mode.

- If only one phy-mode is defined (i.e., 149) on a CGR WPAN module, will adaptive modulation operate?

  If Phy-mode is set to 149 only adaptive modulation is disabled. With phy-mode set to 149, an operator may see IR510/SCADA but not see SLC-2FSK devices.

- Why is my mesh network not working when I set my phy-mode to 166,165,98,2?

  Cisco only support multiple OFDM and single one FSK phy-mode. If you want to use 150k FSK FEC, your phy-mode settting should be 166 165 164 2. 166 165 98 2 is not a valid configuration.

FlashNet Lighting Use Case Implementation over LoRaWAN

FlashNet is a LoRaWAN-based smart street lighting control device and application. FlashNet has adopted inteliLIGHT, which provides interoperability with different IoT communication technologies and platforms. For more information refer to:

- https://www.FlashNet.ro/project/intelilight/

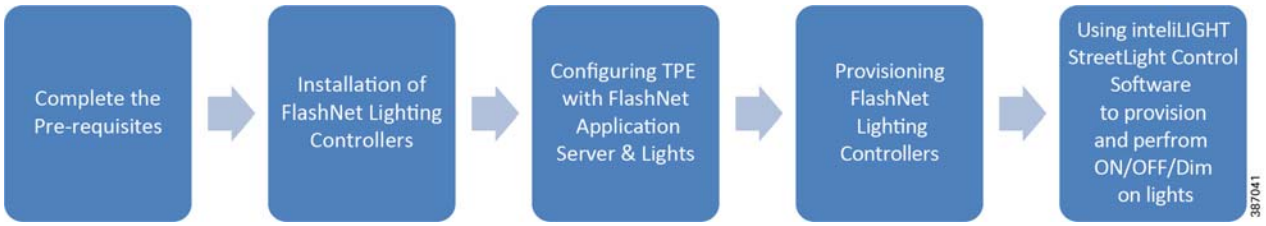
inteliLIGHT® StreetLight Control is the lighting management software used for controlling the FlashNet lights. As part of the integration steps, the software will be integrated with TPE provisioned in the CCI solution by FlashNet support.

More details on the inteliLIGHT® StreetLight Control software can be found at:

- https://intelilight.eu/intelilight-streetlight-control-software/

The flow diagram in Figure 442 shows the sequence of steps to be completed for provisioning the FlashNet solution use case.

Figure 442 Sequence of Steps for FlashNet Lighting Implementation



Prerequisites

Before beginning light provisioning, the following prerequisites must be completed in order to complete the integration of FlashNet's inteliLIGHT StreetLight Control Software with TPE:

1. The Actiility ThingPark Enterprise (TPE) and IXM Gateway must be installed and provisioned for the CCI solution. An On Customer Premise (OCP) instance of TPE is installed in Lorawan_VN network.
2. The following documents must be obtained from the FlashNet support (mail ID: support@flashnet.ro) for detailed steps on installation and provisioning of FlashNet lights:
   - Deployment Manual for intelliLight StreetLight End Nodes v1.7.pdf
   - CMS User Manual v 2.2.7 full version .pdf
3. Application Server details for FlashNet lights can be obtained from FlashNet support:
   - Application URL
   - Application type

The Application server of FlashNet is a cloud-based application.

4. Public IP that will be used by FlashNet Application Server—This IP will be used to configure Static NAT on Firepower as well as to allow the secure communication between FlashNet Application and TPE using Access Policy. Details are described in Implementing Firewall Using Firepower for CCI Network, page 369.
5. The following details pertaining to the installed TPE instance must also be shared with the FlashNet support in order to complete the integration.
   a. Permanent DX-API Access Token

This can be generated from DX-API admin by visiting the following page on the machine that is used to access the TPE instance:

https://<Hostname_Of_Your_TPE>/thingpark/dx/admin/latest/swagger-ui/index.html?shortUrl=tpdx-admin-tpe-api-contract.json

The following is an example:

https://enterprise.thingpark.com/thingpark/dx/admin/latest/swagger-ui/index.html?shortUrl=tpdx-admin-tpe-api-contract.json

After visiting the page, generate a token with infinite validity (by selecting infinite as validity period from the renew drop-down menu) by clicking **Token generation** as shown in Figure 443.

Figure 443 Generating DX-API Token for OCP TPE Instance

In Figure 443:

- The grant_type is login id.
- The client_id is tpe-api/<login_id_of_TPE>.
- The client_secret is the login password for the TPE login.

b. Public IP of the CCI Network and TPE hostname

Public IP is used by the solution for Static NATting configuration on FPR to enable the FlashNet-TPE integration and the host name that the TPE instance is using. The host name of the TPE and the public IP will be used by FlashNet support to create a DNS entry at their end for the OCP instance of TPE so as to enable the communication between FlashNet AS platform and the TPE instance.

The following is the format of the URL created:

https://<TPE_Instance_HostName_created_againt_PublicIP>>/thingpark/dx/core/latest/swagger-ui/index.html?shortUrl=tpdx-core-tpe-api-contract.json#!/Message/post_devices_device_downlinkMessages

6. After the completion of steps 1 to 5, the login details of the provisioned inteliLIGHT® StreetLight Control Software must be obtained with the license already preprovisioned by FlashNet support.
7. A list of the DevEUI, JoinEUI, and AppKey for each of the FlashNet lights received from the team.

Installation of FlashNet Lighting Controllers

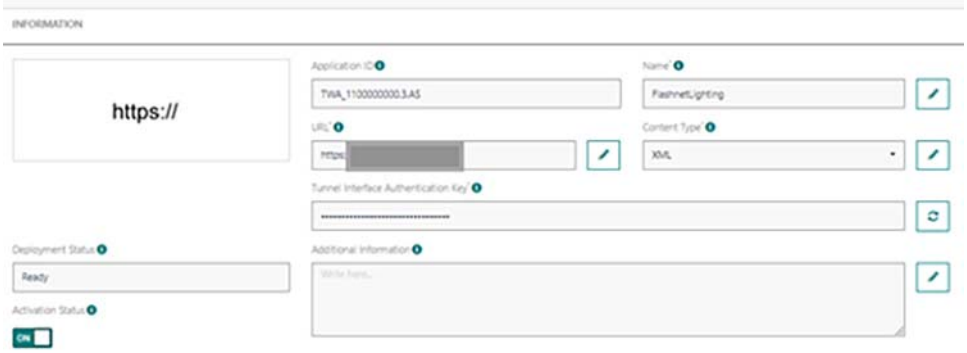
For the installation of FlashNet lights refer to the document Deployment Manual for intelliLight StreetLight End Nodes v1.7.pdf obtained from FlashNet support.

Configuring TPE with FlashNet Application Server and Lights

An application must be created before provisioning a FlashNet light as a device on TPE by following these steps:

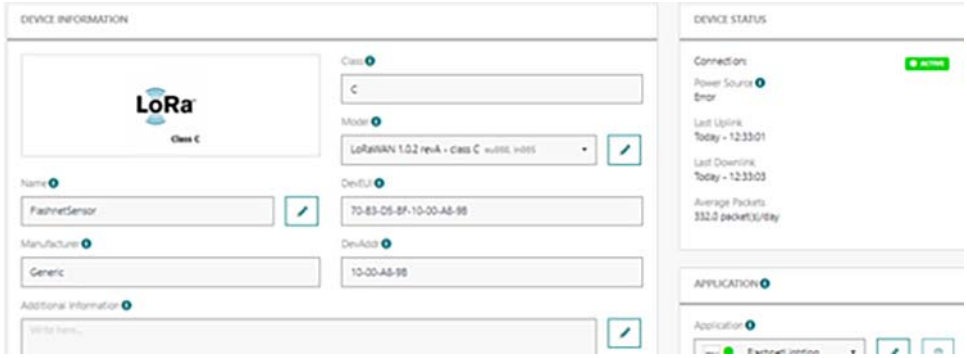
1. Log into TPE and create the application to use with FlashNet light by going to **application -> Generic Application** and entering the URL and content type obtained from FlashNet support (in pr-requisites). The created solution will look like Figure 444.

Figure 444 Added Application in TPE



2. Next go to **Devices** and click **Create** from the drop-down menu.
3. Choose **Generic** as the Device Manufacturer.
4. Select the model as **1.0.2 rev A -class C**.
5. Enter the desired name with which you would like to identify the device under the name.
6. Enter the DevEUI, JoinEUI, and AppKey of the device. They are obtained from FlashNet support when you receive the FlashNet devices.
7. Under the Activation mode choose **Activation-By-Personalization (ABP)** from the drop-down menu.
8. Select the Application created in step 1. Enter the location of the device.
9. Enter the location of the device and click **Save**.
10. The device will be now be created and can be seen under the **List of Devices**.

Figure 445 Added Device



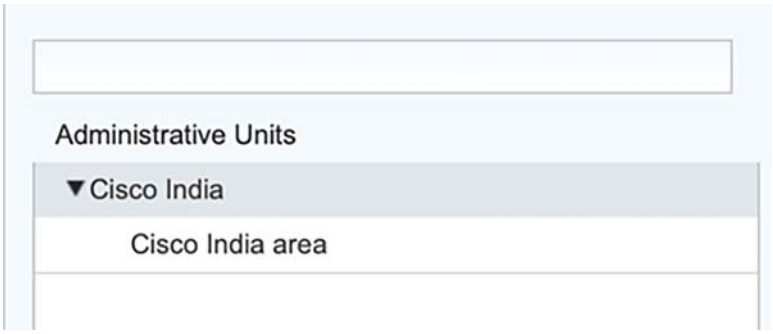
Provisioning FlashNet Lights from inteliLight StreetLight Control

Detailed steps for provisioning the lights using the software can be found in the CMS User Manual v 2.2.7 full version .pdf (obtained in prerequisite step).

A brief summary of the steps are listed below:

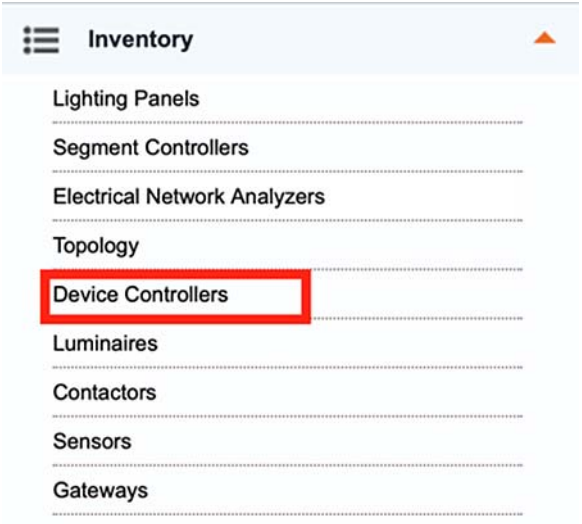
1. Log in to the inteliLIGHT StreetLight Control software and ensure that the administrative unit (appearing at the top left) is set to the main Administrative unit.

Figure 446 Setting Administrative Unit to Main Unit



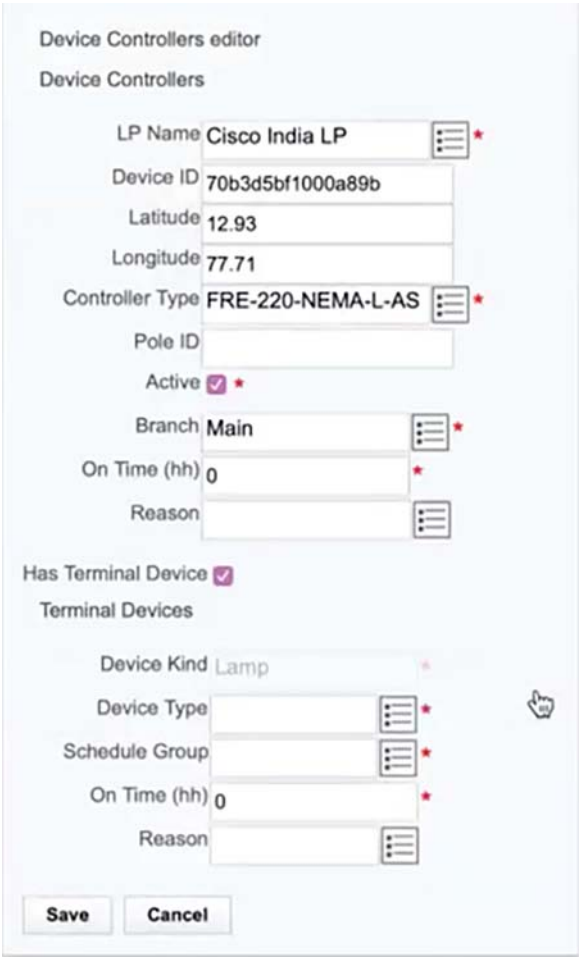
2. Add device controllers from **Inventory->Device controller**.

Figure 447 Adding Inventory



3. Enter the details as shown in Figure 448 and click **Save**.

Figure 448 Adding Device Controller



4. The device will appear as shown in Figure 449.

Figure 449 Added Device

5. Ensure that the communication device is set as shown in Figure 450.

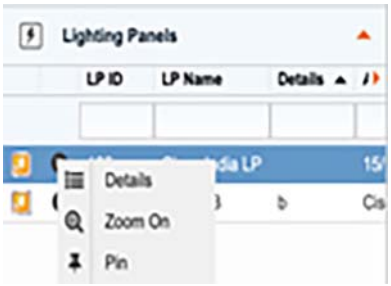
Figure 450 Adding Lighting Panel

Controlling the Light Intensity from intelliLIGHT StreetLight Control Software

The steps for controlling the lights via intelliLight StreetLight Control are:

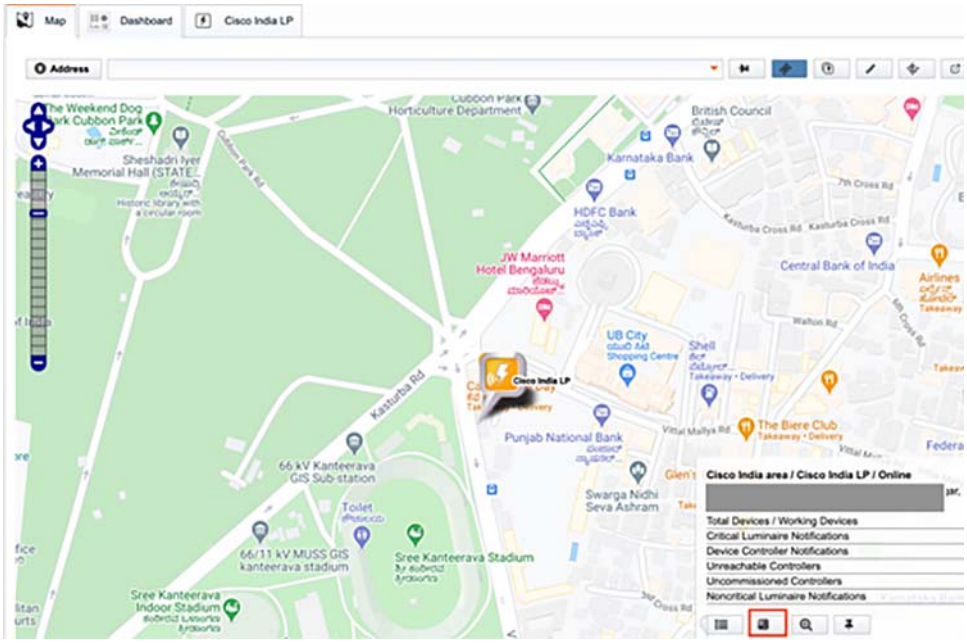
1. To control ON/OFF and dim levels, select **Lighting Panels** from left menu and click the down arrow next to the Luminaire and select **Details**.

Figure 451 Controlling ON/OFF Dim



2. Access manual commands by selecting the **Commands** button on the Detail Box, as shown in Figure 452.

Figure 452 Controlling ON/OFF Dim

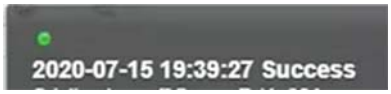


3. The state of the light is reflected on the map when command ON/OFF is executed along with a Success message at the bottom right corner as shown in Figure 453, Figure 454, and Figure 455.

Figure 453 Status When Light is ON

Figure 454 Status When Light is OFF

Figure 455 Success Command Received after Command Execution



This completes FlashNet Lighting use case implementation over LoRaWAN.

Roadways

In this section, how to configure the DNAC to securely onboard the roadside devices is discussed. These devices include the Traffic Signal Controller (TSC), pedestrian video detector, Dynamic Message Sign (DMS), Road Weather Information System (RWIS), Roadside Unit (RSU), and roadside cabinet. This description includes DNAC onboarding and device management. Detailed installation instructions are specific to the devices and usually require assistance from the device manufacturer, therefore they are not included in this guide.

Cisco DNAC

Similar to other services on the CCI network, the roadside devices must be assigned to a Virtual Network with an IP pool for each fabric site. When attaching a Virtual Network to a fabric site and assigning IP pools, Choosing a VLAN name that can be used across sites is recommended. When doing so, an end device can be onboarded through ISE and then assigned to the correct VLAN without ISE explicitly knowing the VLAN number used at the site. This capability in ISE is enabled with the authorization profile.

Figure 456 Fabric Site Virtual Network

	VLAN Name ▲	IP Address Pool	VLAN	Traffic Type
☐	Roadside	Edge2_Roadside 172.16.12.128/26	1036	Data

Figure 457 ISE Authorization Profile

Traffic Signal Controller

The traffic signal controller (TSC) is responsible for controlling the timing of the signal lights at an intersection. It must work with numerous types of detectors to sense vehicles, pedestrians, and bicycles. It also frequently works with pedestrian signals to provide walk / don't walk indicators. Because of its importance in providing an efficient and safe intersection, it is important to provide network and physical safety for the TSC. Discussion of physical safety is part of the physical cabinet section in this guide. In this guide, the TSC is an Econolite Cobalt unit. The recommended management system for the Econolite Cobalt TSC is to use the cloud application provided by the Econolite cloud application called Centracs Mobility. This is the only management system documented in this guide. This guide also does not go into the details of configuring signal phases or other intersection details except what is necessary to incorporate the TSC into the CCI network.

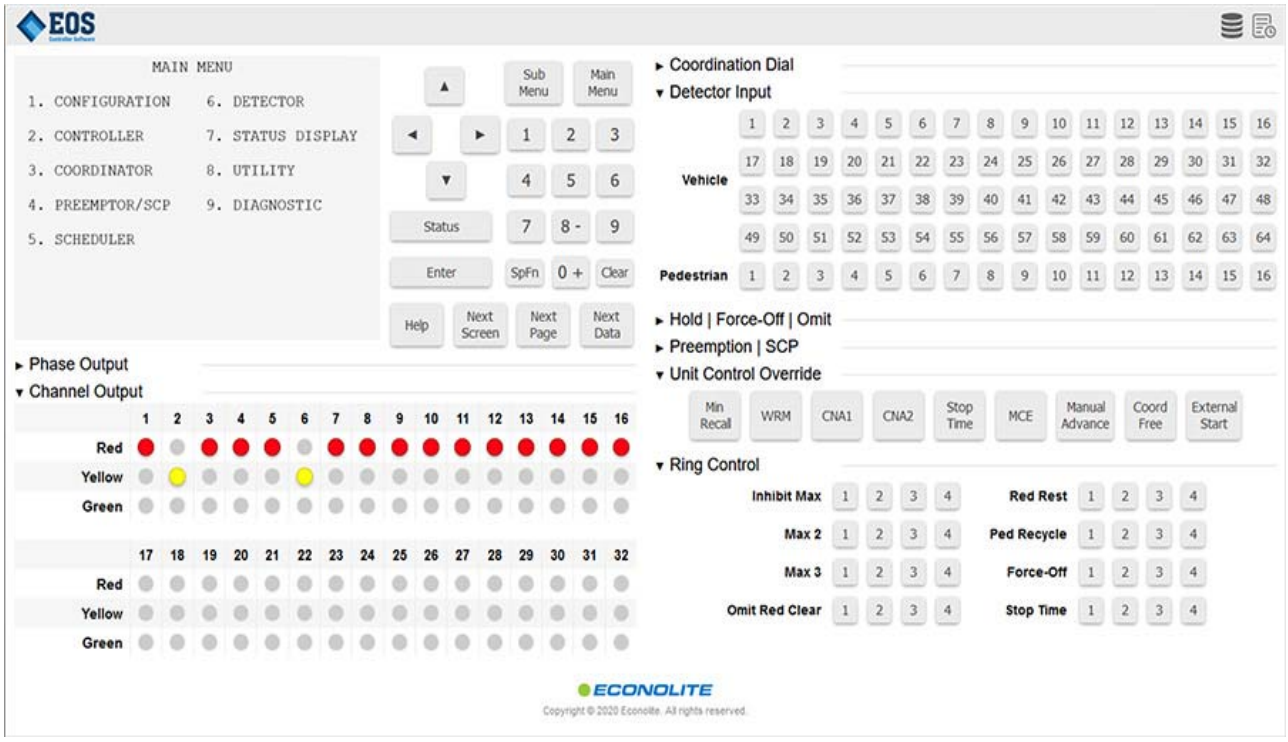
CCI Integration

The TSC does not support 802.1X, so the next most secure method is by using MAB authentication which is described in the <MAB authentication> chapter. Because the TSC must communicate with other roadside devices to form a complete picture of the intersection, Putting the TSC in the same VN as other roadside devices is recommended.

Management

Managing the TSC can be done in several ways, by physical access or remote access. It is recommended to assign a static IP address to the TSC is recommended for ease of management. This can be done using the front keypad and graphical interface. Depending on the model, it could be text driven with physical buttons or use a graphical touchscreen interface. After an IP address is assigned, the TSC can also be managed using a web browser. The Econolite Cobalt TSC supports web management on port 8081.

Figure 458 Econolite Web Management

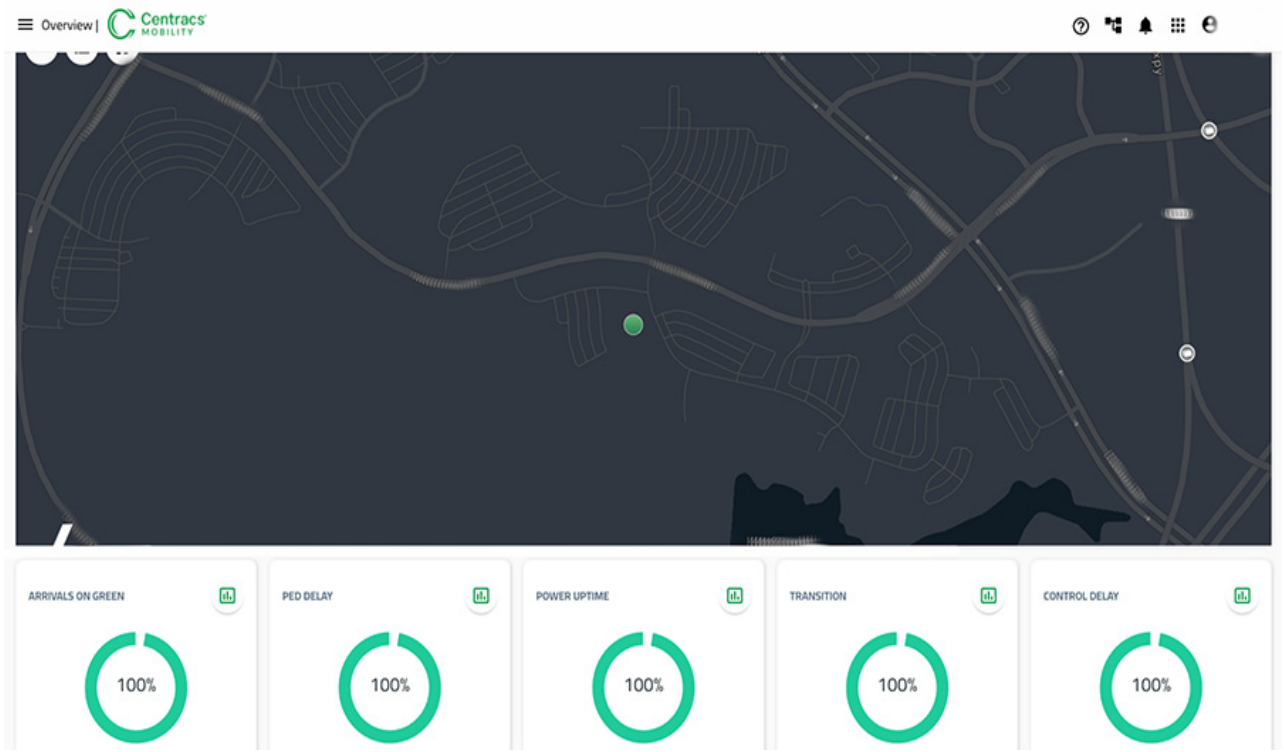


To manage more than a few intersections, it is recommended to use a centralized management system is recommended. Econolite offers numerous on-premise management systems based on their Centracs Advanced Traffic Management System (ATMS) and their cloud-based offering called Centracs Mobility. Only the Centracs Mobility is documented in this guide.

Because Centracs Mobility is cloud based, a separate Device Manager is installed in the datacenter as the proxy between the TSC and Centracs Mobility. The Device Manager communicates directly with the TSCs and Centracs Mobility. This reduces the size of the attack surface in the network because the TSCs are not directly communicating with the Internet. The Device Manager is installed as a Docker container in the datacenter and is configured to communicate with all the TSCs. The Device Manager configuration is based on the number and types of TSCs installed. The details of this installation are outside the scope of this guide.

After the Device Manager is successfully communicating with Centracs Mobility and the TSCs, Centracs Mobility will receives the status of all the devices and can manage them and perform traffic analytics.

Figure 459 Centracs Mobility



Video Detector

To increase the safety and efficiency of an intersection, numerous types of detectors can be used which can be used as inputs into the TSC. Examples include loop detectors embedded in the road to detect vehicles, video analytics to detect pedestrians, vehicles, and bicycles, or even Lidar which can form a 3D map of an intersection. In this guide, the Iteris Vantage Next video detection system will be documented which can detect and count perform pedestrians, vehicles, and bicycle detection and countings. This video can be used as a means of surveillance, or with the built-in computing capabilities, analyzed and used as an input into the TSC as a detector. Using their cloud based application, VantageLive!, this data can also be analyzed at an overall system level to see larger trends.

This video detection system is two main components, the video processor, and the cameras.

Figure 460 Iteris Vantage Next

The video processor is typically located inside the roadside cabinet and has an Ethernet connection to the CCI network. Up to 4 cameras can be connected using standard RJ-45 connectors. If desired, the video processor can be connected to the TSC using the SDLC connector for TS-2 applications.

CCI Integration

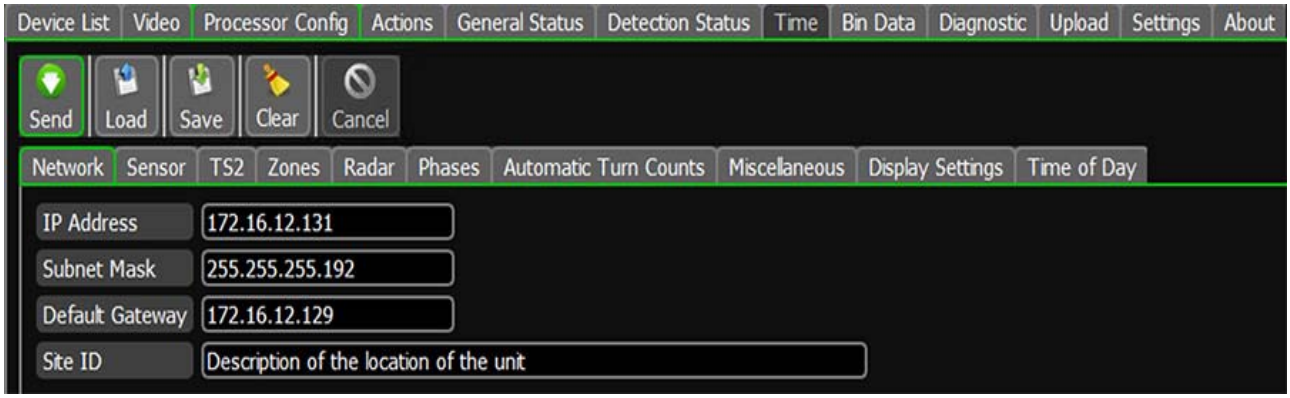
Iteris Vantage Next does not support 802.1X so the next most secure method is by using the MAB authentication which is described in the <MAB authentication> chapter. The Vantage Next has numerous communication methods depending on the applications needed. When performing as video surveillance, it can stream RTSP to a viewer in the datacenter. In this configuration, the Vantage Next can be placed in a VN that is specific to that function. If Vantage Live! is used, the Vantage Next is put into a VN that has Internet access through the datacenter. Communicating with the TSC using the SDLC connector and requires no network configuration. For simplicity of management, the Vantage Next can be placed in a common VN used exclusively for roadside devices.

Management

The Iteris Vantage Next system comes configured with a the default IP address of 192.168.1.2 and is configured using their included Windows compatible application. This software is required to perform any maintenance task on the system. These tasks primarily include setting up the detection zones in an intersection, configuring the communication with an attached TSC, and administrative tasks such as capturing logs and upgrading software.

After logging into the system for the first time, it is important to remember to change the IP address to one consistent with the configured VN.

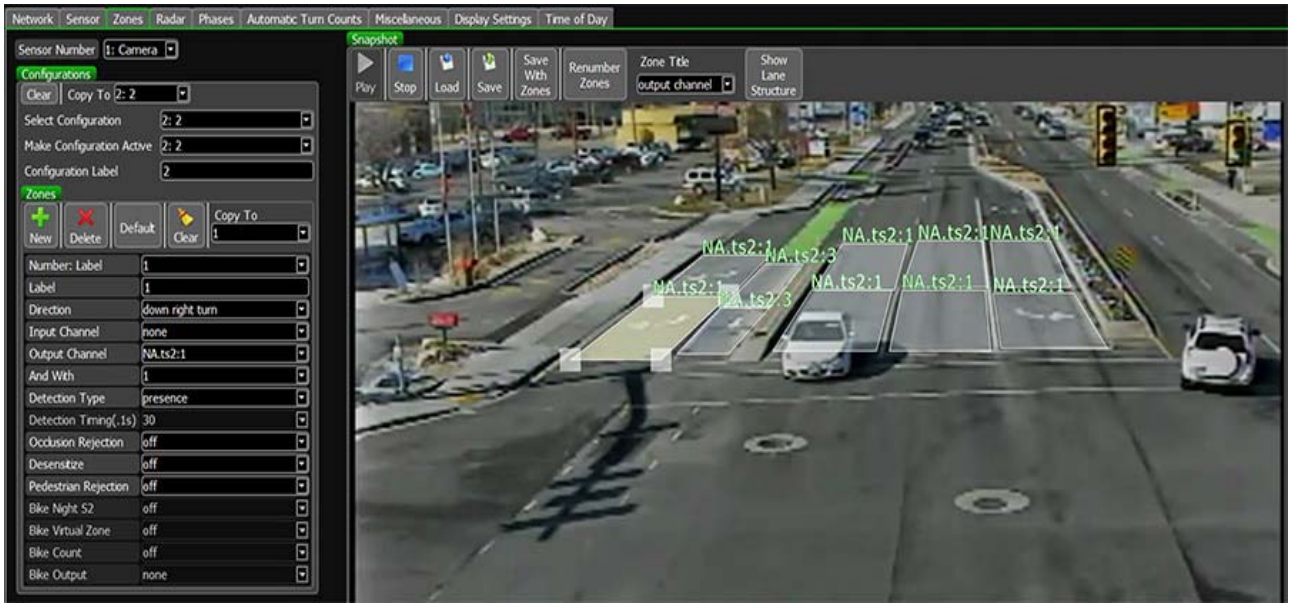
Figure 461 Network Settings



After the IP address is changed, and the Send button is pressed, and the device now has the new IP address.

Below is an example of configuring detection zones.

Figure 462 Detection Zones



Below is an example of the live video with analytics overlaid.

Figure 463 Live Video

When using VantageLive! for analytics, it must be able to collect the data from all the video processors in the system. To accomplish this, a server is configured in the datacenter to communicate with all the video processors and send the telemetry data to VantageLive! residing in the cloud. The details of installing this server are outside the scope of this document and require technical assistance from Iteris.

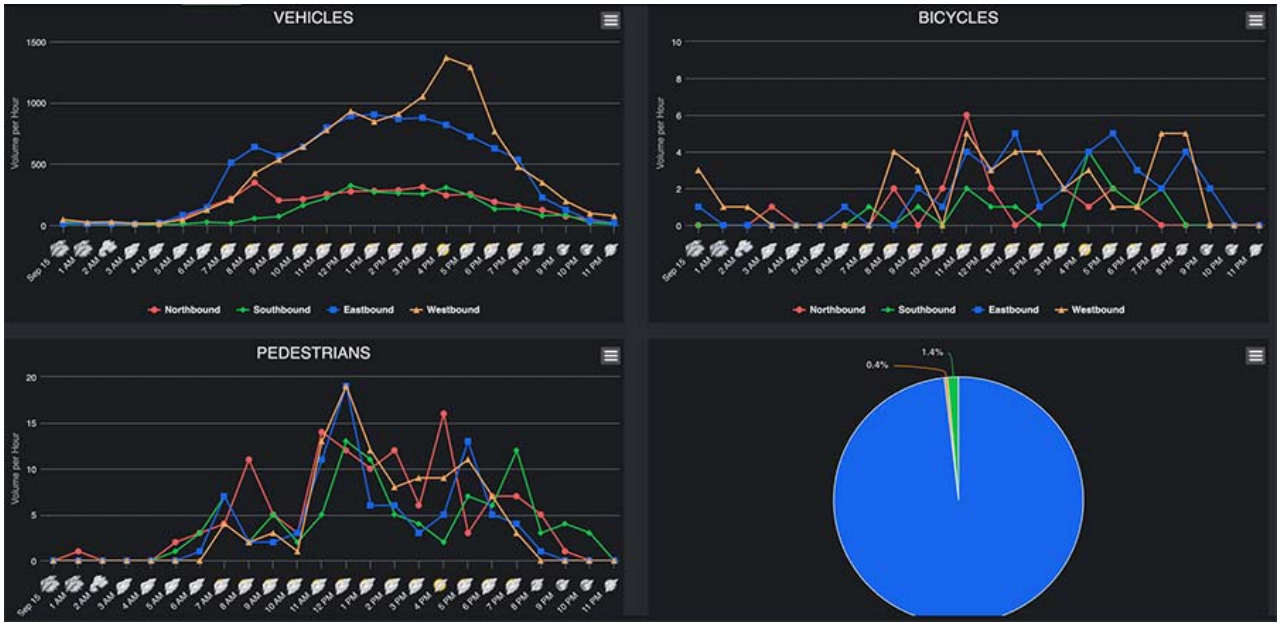
Video Considerations

Because the video processor is designed to function at the roadside alongside potentially hundreds of other cameras, the bandwidth requirements must remain small to not saturate the network. It also must be able to function over low bandwidth cellular links as well as a high- speed fiber network. Each Vantage Next video processor unit supports 4 cameras and each video stream is approximately 500 Kbps. This video is unicast so it is multiplied for every person viewing the video stream. The traffic is also sent with a QoS marking of Best Effort. Each camera feed can be accessed using RTSP and can be viewed using a dedication video streaming application or incorporated into a custom traffic management application.

Analytics

Using the VantageLive! cloud application from Iteris can give traffic management personnel deeper understanding into how much and what kind of traffic flows through an intersection. Having this knowledge can help capacity planning for more efficient road expansions or optimizing traffic light patterns for more efficient flow. An example of the data shown is below.

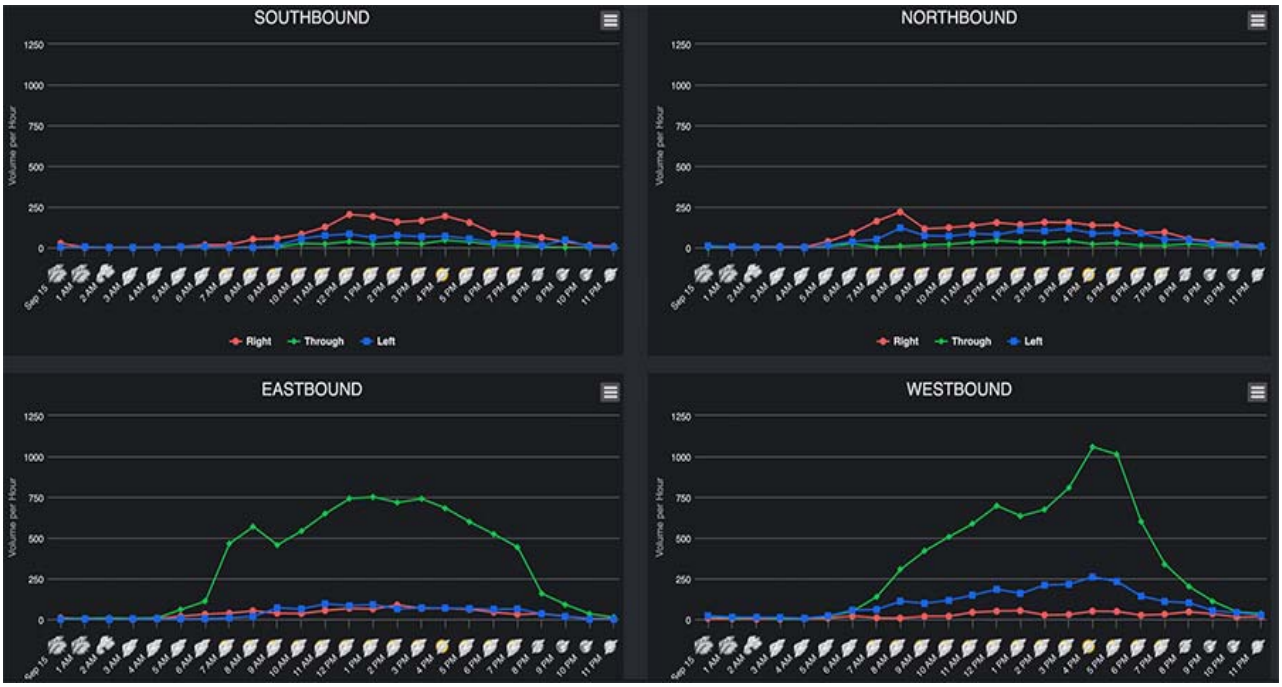
Figure 464 Sample Intersection Data



This data shows the volume per hour for vehicles, pedestrians, and bicycles broken down into direction and time of day. Depending on the observed trends seen, this data could be used to justify longer pedestrian crossing times, adding a dedicated bike lane, or expanding a road.

Looking at dedicated vehicle data will break down the traffic further into left, right, and through movements as seen below.

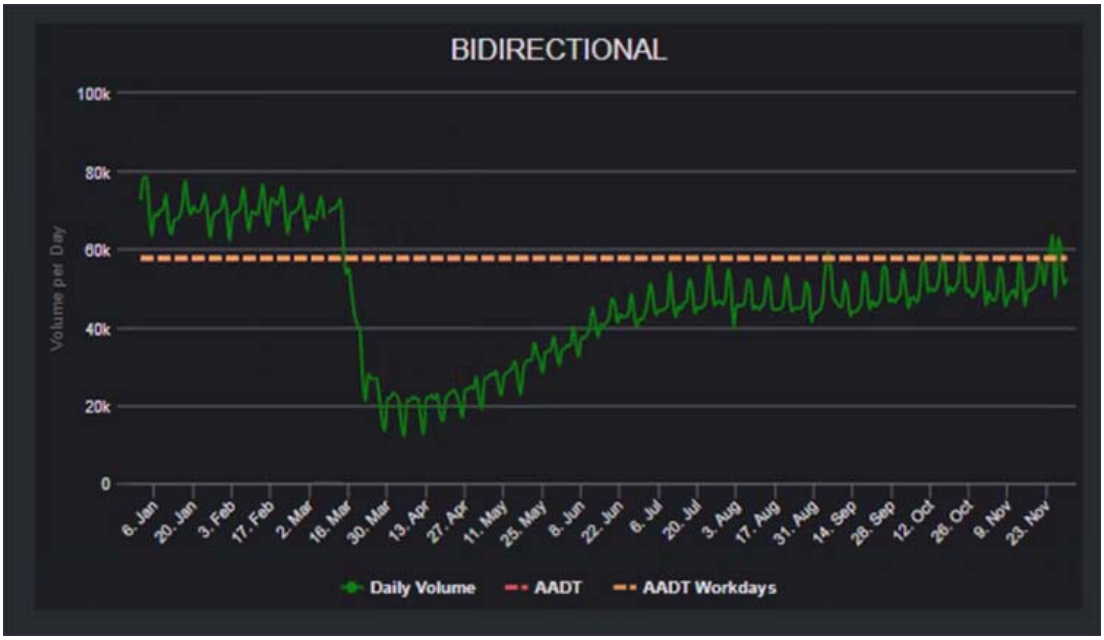
Figure 465 Vehicle Data



When planning road closures or expansions, this data can be useful to minimize disruptions and spend money where it will be most effective.

Another feature of VantageLive! is their Average Daily Travel which shows larger trends in an area over time. This can be used to see the effects of events or changes in the area.

Figure 466 Average Daily Travel



Dynamic Message Sign

A Dynamic Message Sign (DMS), which is typically seen on highway overpasses on a highway, is an very effective means of communicating with large numbers of drivers. Various alerts and route information can be displayed and changed based on circumstances. Other dynamic message signs are found on speed limit signs that can change due to various traffic conditions or times of day.

When connected to the network, the traffic management personnel can manage all the connected signs from a central location which increases security and visibility into the signs' status and operation. But because of the signs' functions, it is necessary to have secured network access to prevent rogue actors from disrupting traffic.

Figure 467 Hacked Dynamic Message Sign

In this guide, the Daktronics VFC sign controller is used.

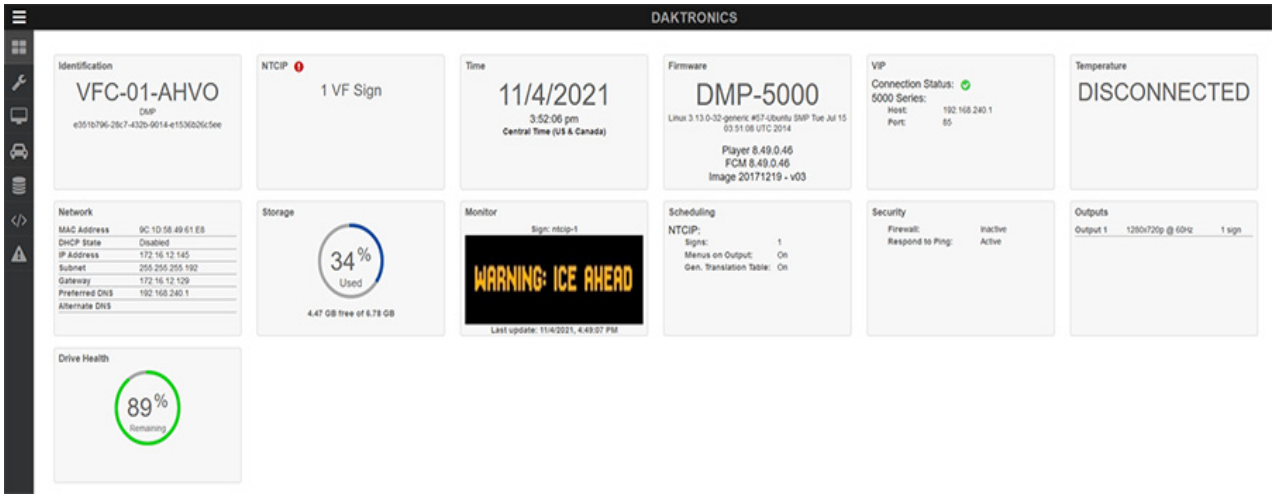
CCI Integration

The DMS does not support 802.1X so the next most secure method is by using MAB authentication which is described in the <MAB authentication> chapter. Putting the DMS in a roadside VN is recommended for ease of management with a separate SGT to restrict communication with other roadside devices. The Daktronics VFC controller supports DHCP but using a static IP address is recommended for deterministic management.

Management

The Daktronics VFC supports remote management as well as and local management using the front keypad. A traffic management administrator can remotely connect to the sign controller using the web interface or Daktronics' Vanguard v4 Control Software application. This application can be used standalone or alongside other traffic management software.

Figure 468 Daktronics Web Management - 387625



Road Weather Information System

A Road Weather Information System (RWIS) is a system of weather sensors with or without a controller that collects weather data at the site of installation. In areas with extreme weather, this data could be used to determine a safe speed limit or display a warning message that is reflected on a DMS. It may or even close a road down if it becomes impassable. When connected to the CCI network, all the sensor data can be aggregated and viewed in a single location for the traffic engineer or scientist to monitor and manage. Depending on the RWIS used, this data can be viewed in a web browser or aggregated into a large traffic management system. In this guide, only sensors connected to an ethernet-enabled controller, such as a datalogger, are supported. Alternatively, IP enabled sensors can also be supported.

CCI Integration

It is recommended to use the highest security method available when onboarding the RWIS, whether using 802.1X or MAB. It is also recommended to put the RWIS in a dedicated roadside VN with a separate SGT to limit communication with other roadside devices. If the RWIS will send data to a cloud application, this VN must also have Internet access. A static IP is also recommended for deterministic management.

Roadside Units

Roadside Units (RSU) are used as part of a V2X infrastructure. They rely on Dedicated Short-Range Communication (DSRC) or Cellular Vehicle to Everything (C-V2X) technology to communicate with Onboard Units (OBU) installed in a vehicle. This technology allows vehicles to anonymously communicate their telemetry data to the RSUs at the roadside effectively turning the vehicles into mobile sensors. The RSUs can also forward data to the vehicles such as custom alerts in the form of a Traveler Information (TIM) message or the timing of the traffic signal lights from a TSC as a Signal Phase and Timing (SPaT) message. In this guide, Cohda RSUs and OBUs are validated using DSRC technology.

CCI Integration

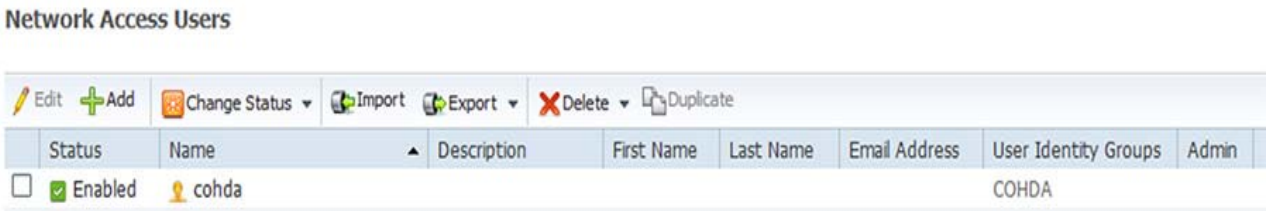
Because the RSU typically communicates with other roadside devices, it is recommended to put putting it into a dedicated roadside VN that has allowed access to the other roadside devices is recommended. Using static IP addresses or DHCP with MAC to IP mapping Fis recommended for ease of management., it is recommended to useU static IP addresses or DHCP with MAC to IP mapping.

Depending on the RSU capabilities, 802.1X may be a supported security option. The Cohda's MK5 is Linux based and supports 802.1X out of the box. Below is an example using the WPA_supplicant application in Linux along with the corresponding entries in ISE.

```
/etc/wpa_supplicant.conf
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=2
ap_scan=0
network={
key_mgmt=IEEE8021X
eap=TTLS MD5
identity="cohda"
anonymous_identity="cohda"
password="mypassword"
phase1="auth=MD5"
phase2="auth=PAP password=mypassword"
eapol_flags=0
}
```

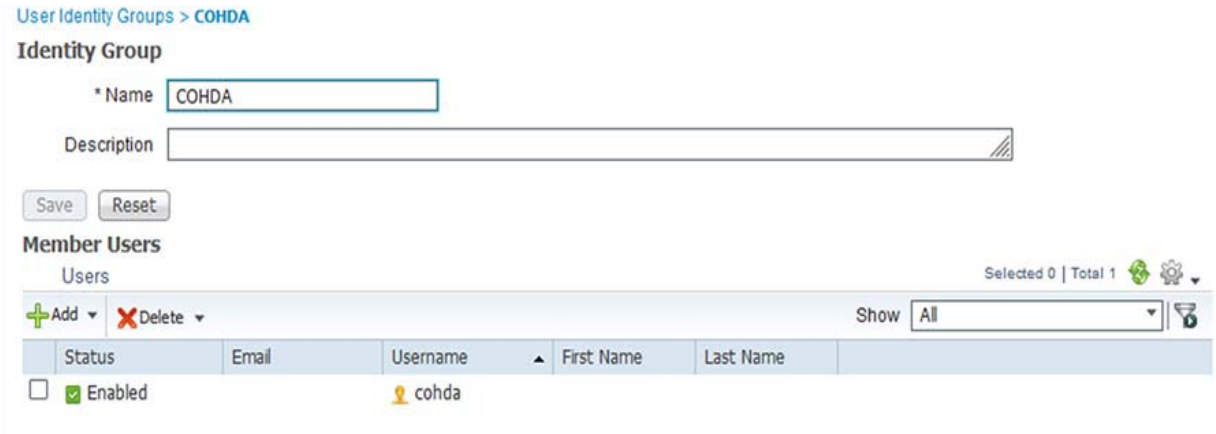
The WPA _supplicant identity is added to ISE as an access user.

Figure 469 ISE Access User



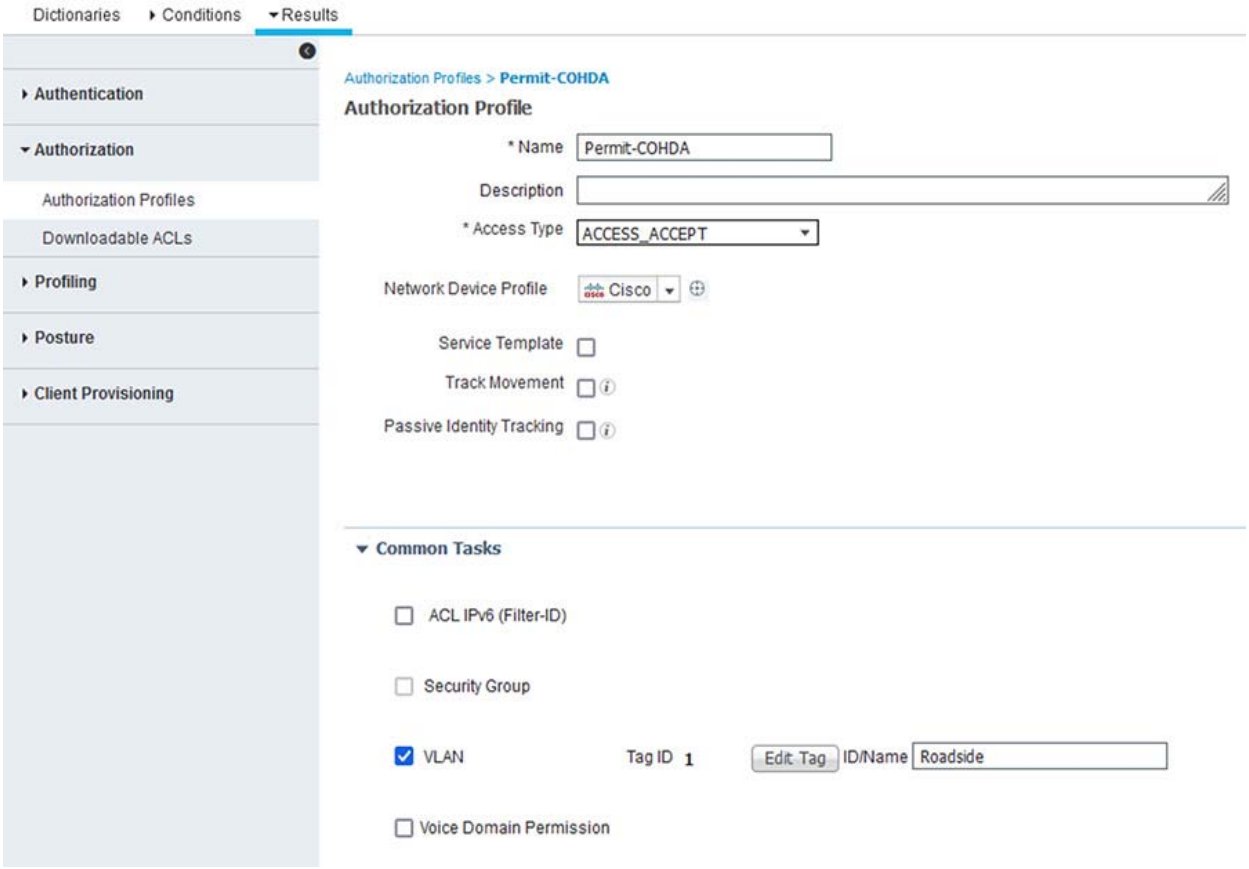
This user is also part of an identity group.

Figure 470 ISE Identity Group



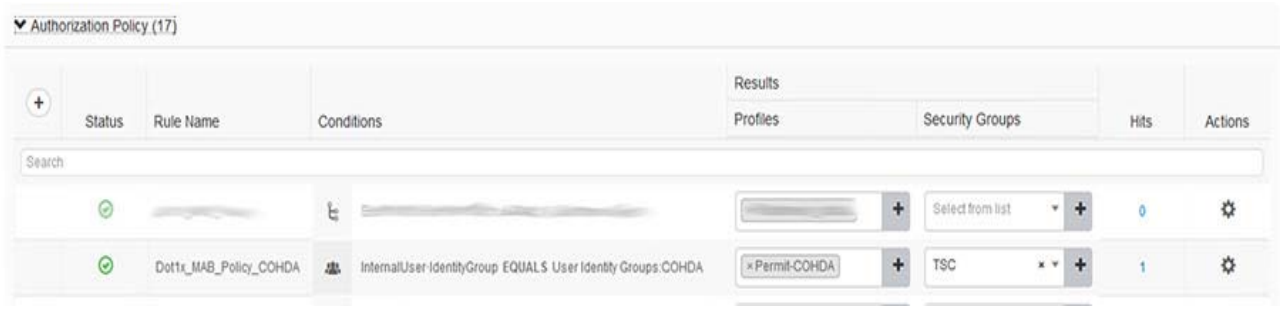
An authorization profile is created to put the Cohda RSU into the correct VLAN in the fabric site Virtual Network.

Figure 471 ISE Authorization Profile



An authorization policy is then created which permits this user to gain access to the network with the correct VLAN name and SGT assigned.

Figure 472 Authorization Policy



After a successful login, the user is seen in the live logs.

Figure 473 Successful Login

Roadside Cabinet

While not strictly a networking device, the roadside cabinet can be monitored by the network infrastructure and made smarter more useful. Network security is well known and documented, but physical security can alert the management platform about access to the cabinet and even power losses.

Contact Closure

If the cabinet door is outfitted with a contact closure, it can be connected to the alarm port on the IE switch or IR1101 router. When the door is opened, the alarm is triggered, and an SNMP message is sent to DNA-C. These messages can be further incorporated into a larger traffic management application.

After connecting the contact closure to the alarm input port according to the hardware installation guide found here, https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/b_ie2k-ip67-hig_chapter_010.html#con_1220513 , the switch must be configured to process the alarm input.

If using the IR1101 for the alarm input port, the guide is here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/b_IR1101config_chapter_010010.html .

Alarm Contact Configuration

```
alarm contact 1 description Door Contact
alarm contact 1 severity major
alarm contact 1 trigger open
```

After configuration, any alarm triggers are sent to DNA-C and viewable in the switch Event Viewer.

Figure 474 IE Switch Alarm Asserted/Cleared

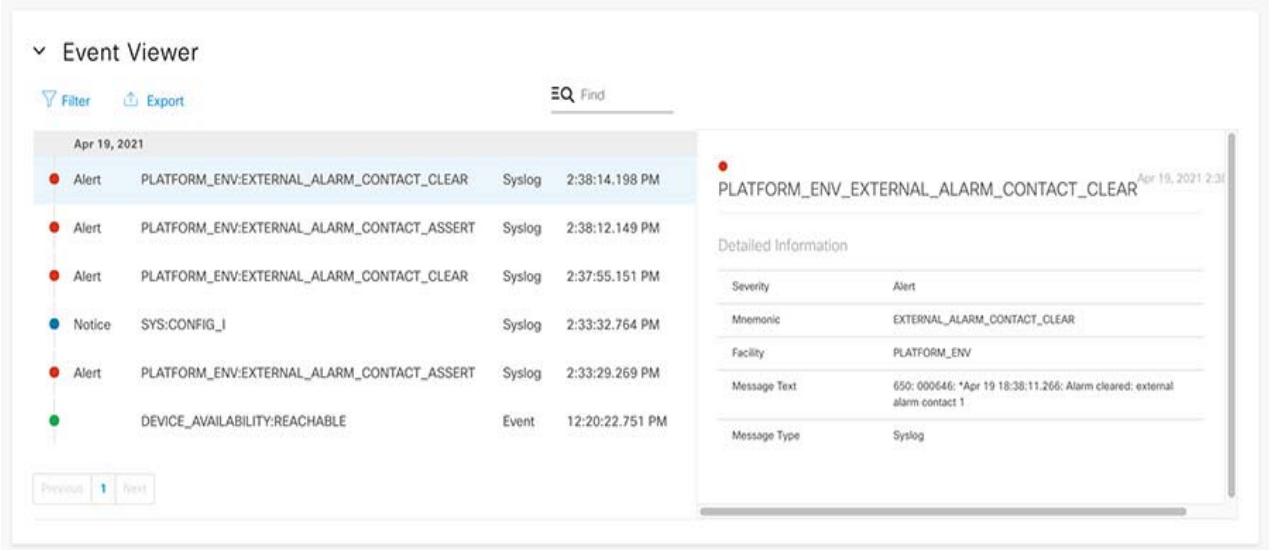
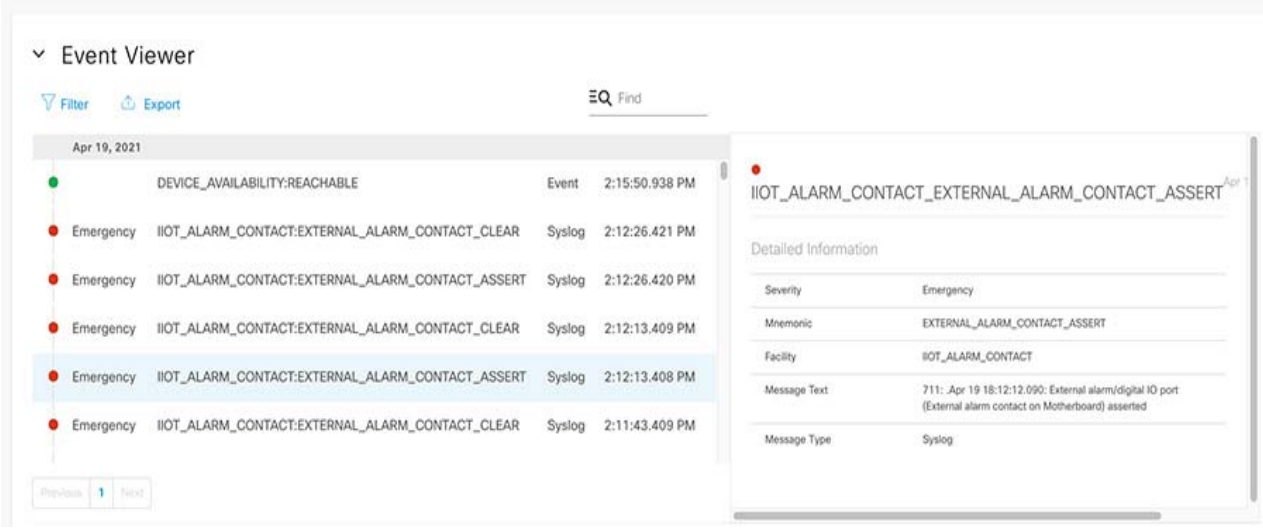


Figure 475 IR-1101 Alarm Asserted/Cleared

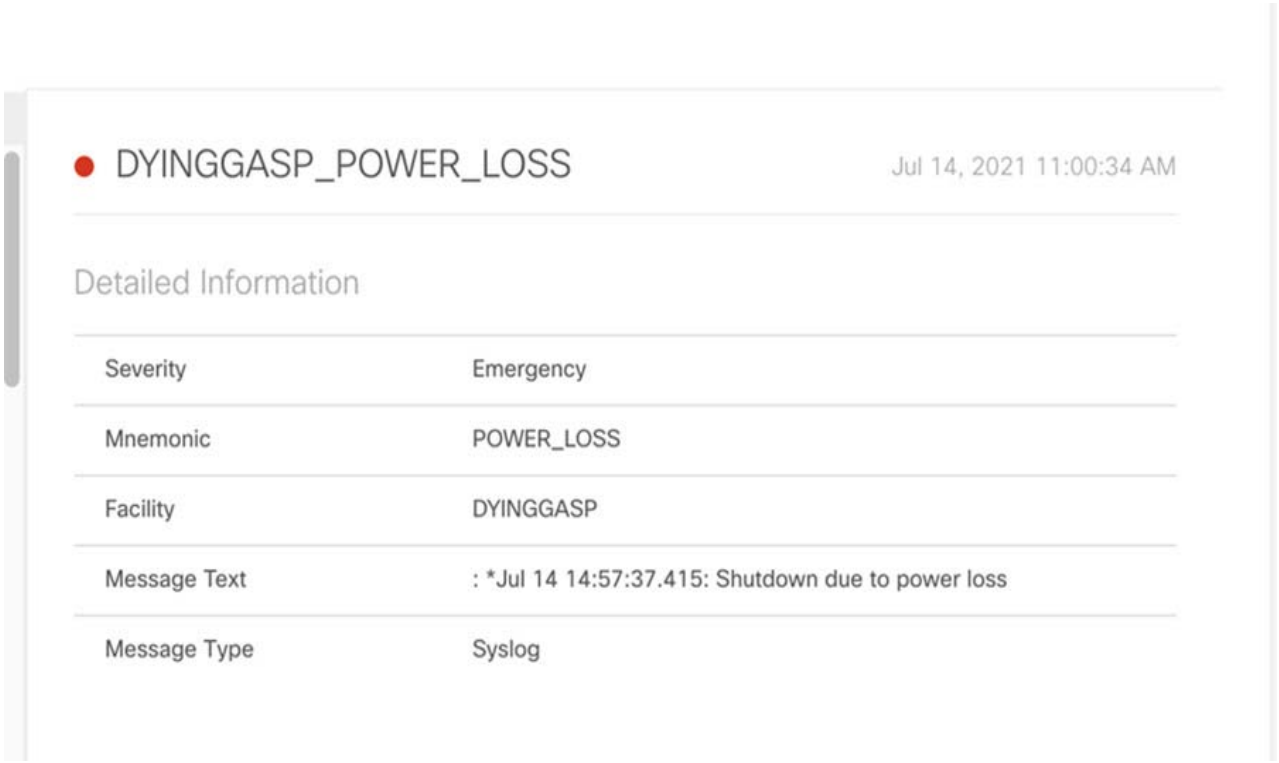


Power

When a switch loses connectivity to DNA-C, it will show as unreachable in the dashboard and the Event Viewer will show a Link Down error in the neighboring switch. If a console connection is unavailable, there won't be any way to know what the failure is without onsite support. By using the dying gasp feature on the IE switch, any power failures will be alerted to DNA-C. Once enabled, this feature will send a SYSLOG message and an SNMP Trap to the DNA-C dashboard which will be viewable in the switch Event Viewer.

```
dying-gasp primary syslog secondary snmp-trap
```

Figure 476 Dying Gasp Event

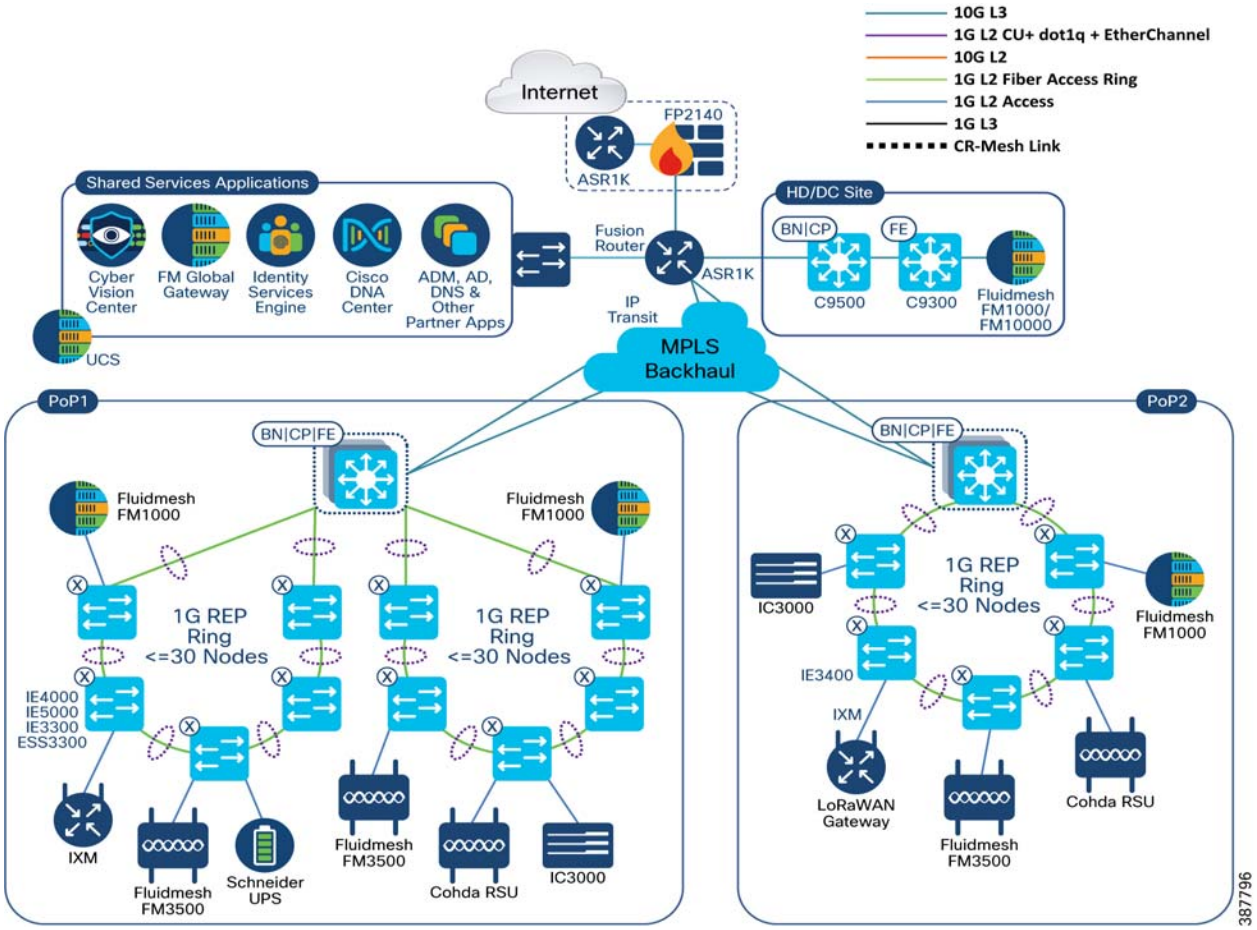


Train to Trackside Roaming

In some dense city settings, there may be one or more train lines that span the entire city. As a CCI network is built out, extending network services out to the train may be part of that plan. Since a train is a large moving network with passengers and safety equipment, high throughput, low latency, and seamless roaming are the highest priority. But since a train is constantly moving and at potentially high speeds, special considerations are necessary to meet those priorities. The primary building block of the CCI network is the Fabric Edge PoP which is at the street level. As large as a PoP may be architected, it may not be practical to cover an entire section of track with a single PoP deployment. This means a train will roam between PoPs as it travels down the track. To ensure a seamless roaming experience, a CURWB network must be built on top of the CCI network. The technology enabling this seamless roaming is called Fluidity and specifically for the CCI network, it is Layer 3 Fluidity. See the CCI Design Guide for a detailed explanation of the CURWB components, Fluidity, and the network design.

An example network showing how a CURWB network is integrated with the CCI network is shown in Figure 477. The FM 4500 train radios are not shown.

Figure 477 Example Train to Trackside Test Topology



CCI Network Integration

Cisco DNAC

Like other services supported by CCI, the CURWB devices are put into a virtual network supporting the trackside infrastructure. In this implementation, they are put into a Train2Track VN which is dedicated to the CURWB devices with subnets allocated in each fabric site. Therefore:

- In each Edge PoP, all mesh points and mesh ends (FM-3500, FM-1000) are put into the Train2Track VN.
- In the data center PoP, the global gateway (FM-1000, FM-10000) is put into the same VN.

Since the train radios and onboard gateways are mobile, they are not given addresses out of a particular Edge PoP IP Pool. An IP Pool can be created as an administration task to ensure the IP addresses are not used for a different service. More details can be found in Preparing Cisco DNA Center for PoP Site Provisioning, page 67.

When onboarding a CURWB device in Cisco DNA-C, it can be done manually through the Host Onboarding workflow, manual Day-N templates, or by using MAB since the devices do not support 802.1x. See Network Devices and Endpoints Security Implementation, page 366 for more details.

Routing Considerations

To enable seamless roaming between different Layer 3 domains, each Mesh End forms L2TP tunnels to the Global Gateway in the data center. Because the Global Gateway is the entry point into the CURWB network, all return traffic destined for the train must go through the Global Gateway. In the data center PoP, a static route is added to the Fabric in a box that points to the Global Gateway as the next hop for the train radio network as well as the onboard gateway network. This static route must be redistributed into the BGP process for the Train2Track VN. An example is shown below.

Static Route

```
ip route vrf Train2Track 192.168.10.0 255.255.255.0 172.16.14.7
```

BGP Routing Address Family

```
address-family ipv4 vrf Train2Track
  bgp aggregate-timer 0
  network 172.16.0.20 mask 255.255.255.252
  network 172.16.14.1 mask 255.255.255.255
  aggregate-address 172.16.14.0 255.255.255.192 summary-only
  redistribute static
  redistribute lisp metric 10
  neighbor 172.16.0.22 remote-as 65001
  neighbor 172.16.0.22 update-source Vlan3033
  neighbor 172.16.0.22 activate
  neighbor 172.16.0.22 weight 65535
 exit-address-family
```

Similarly, this network must also be leaked from the Train2Track VN to the Global Routing Table in the Fusion Router if resources outside the VN need to be reached. More details can be found in Configuring Fusion Router, page 97.

```
ip prefix-list train2track-to-global seq 80 permit 192.168.10.0/24
```

This will ensure that return traffic can properly reach the train networks.

Quality of Service

When the traffic from the train enters the trackside Mesh Point and is put out onto the network, it is MPLS labeled. The priority of the inner payload is copied into the EXP bits of the MPLS header. The traffic is non-IP and the access ring switches are not able to match packets based on those EXP bits, so traditional IP-based QoS will not work. Configuring a MAC ACL on these switches allows matching on the MPLS Ethertype or the MAC address of the radio attached to a switchport.

See Configuring QoS on Ethernet Access Ring, page 405 for more detailed information.

1. Create MAC ACL based on MAC address or MPLS Ethertype.

   This is an example of a MAC address-based ACL.

   ```
   mac access-list extended fm51292
    permit host 00f1.ca01.1d02 any
   ```

   This is an example of a MAC ACL using the MPLS Ethertype.

   ```
   mac access-list extended fm_mpls
    permit any any 0x8847 0x0
    permit any any 0x8848 0x0
   ```

2. Create class-maps to classify the traffic. There will be a class-map for the ingress direction that matches the MAC ACL and then another class-map for the egress direction where the traffic will be marked. This marking is dependent on the specific QoS design.

This matches on the MAC address.

```
class-map match-all fm51292
 match access-group name fm51292
```

This matches on the MPLS Ethertype.

```
class-map match-all fm_mpls
 match access-group name fm_mpls
```

This example is for the IE4000/IE5000 using qos-groups.

```
class-map match-all fm_out
 match qos-group 3
```

This example is for the IE3x00 using COS.

```
class-map match-all fm_out
 match cos 3
```

3. Create policy-maps for the input and output service policies that align with the QoS design. These statements can be part of a larger input/output policy-map statement as seen in the previously mentioned Configuring QoS on Ethernet Access Ring, page 405.

   This example is for the IE4000/IE5000 using qos-groups.

```
policy-map CCI_IE_QoS_Input_Policy
 class fm51292
  set qos-group 3
```

   This example is for the IE3x00 using COS.

```
policy-map CCI_IE_QoS_Input_Policy
 class fm51292
  set cos 3
```

   This is an example output policy for the IE4000, IE5000, or IE3x00.

```
policy-map CCI_IE_QoS_Output_Policy
 class fm_out
  bandwidth percent 30
```

CURWB Device Configuration

The CURWB devices can be configured by three different methods:

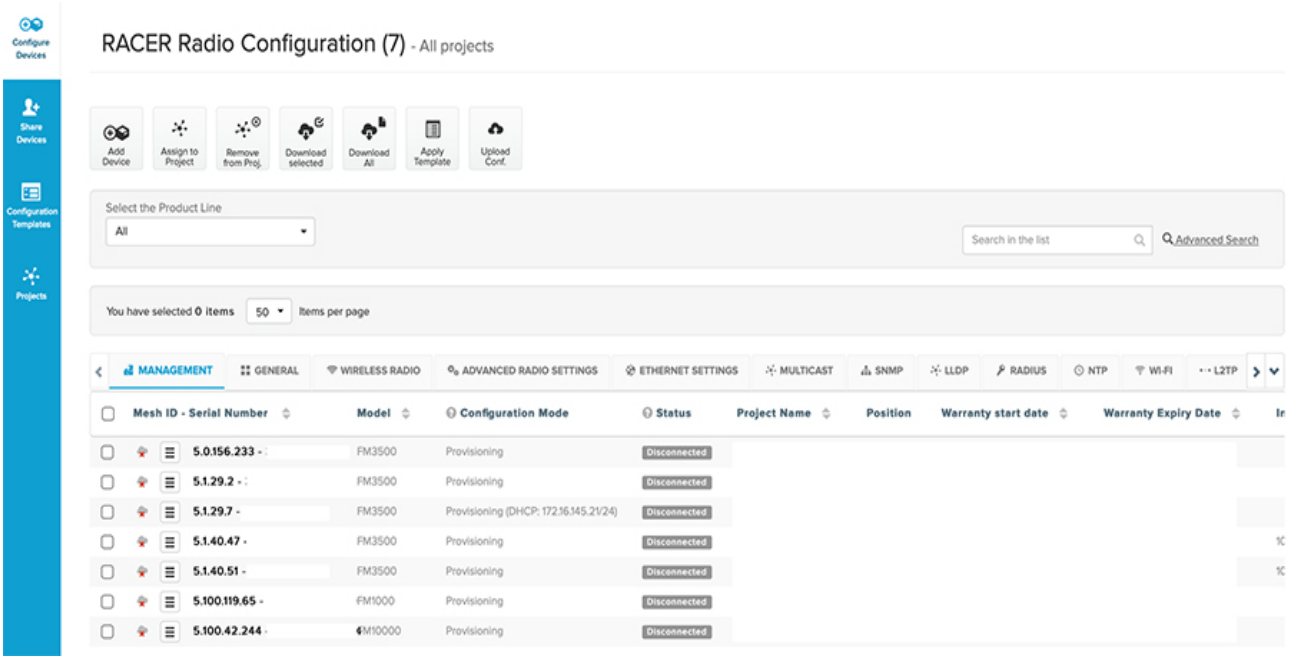
- RACER is a cloud managed tool that can create and push configurations to devices in real time if they are connected to the Internet. It can also be used in an offline mode if the devices do not have Internet access.
- Another option is Configurator, which is a web tool built into the devices. It is accessed by connecting to the device interface address.
- The final option is by CLI, either through telnet or SSH to the device interface address.

By default, a new CURWB device will start up in the provisioning state. In this state, it will attempt to get an address through DHCP and access RACER from the portal at https://partners.fluidmesh.com on port 443. If successful, the device is placed into Online mode, which allows RACER to directly push a configuration to the device. If the device cannot reach this portal, it will revert back to offline mode. In this mode the device will have an IP address of 192.168.0.10 and username/password credentials of admin/admin. Since this IP address is the same on all CURWB devices and is unlikely to match the IP pool scheme for an Edge PoP, the devices should be pre-staged before installation. In this mode, all configuration options are available except that RACER will be in an offline mode.

Using RACER in offline mode is preferable to Configurator or CLI for a medium or large deployment because RACER allows the user to create all the device configurations and then export them as a single file. This makes it a central repository for the device configurations. Within this file are all the configurations for the devices separated by Mesh ID. The file is then uploaded to the individual devices through Configurator and the device picks the correct configuration based on the Mesh ID of the unit.

An example of the RACER configuration portal is shown in Figure 478.

Figure 478 RACER Main Configuration



RACER is also the preferred method of configuration because there are some features that cannot be configured from the Configurator web tool, namely TITAN and some of the more advanced Fluidity features.

For more detailed information on RACER, see the FM RACER User Manual.

For display and documentation purposes, the Configurator tool output will be shown when possible.

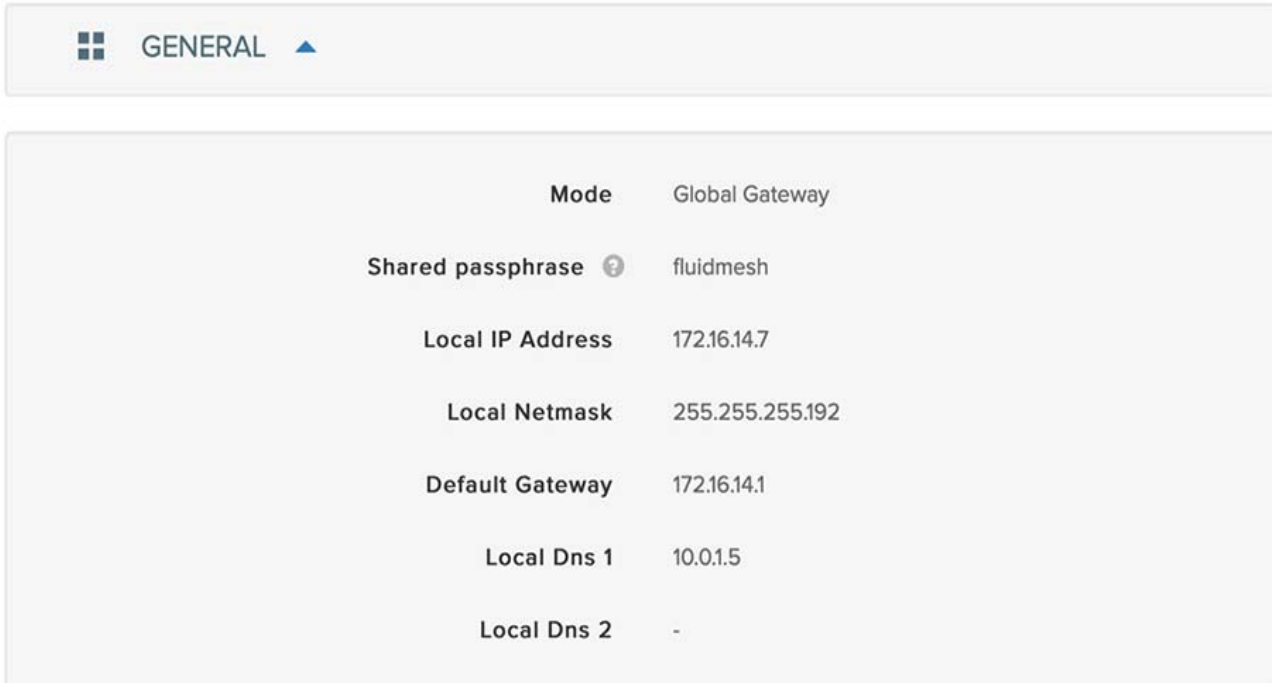
Global Gateway

The Global Gateway is located in the data center PoP or in some other centralized PoP close to the services used by the train and passengers. The following sections will describe what settings need to be configured to enable Layer 3 Fluidity. At a minimum, the General Mode section, L2TP, and Fluidity sections must be configured to enable this functionality. Both the FM-1000 and FM-10000 can serve as the Global Gateway.

General Mode

General Mode is where the Mesh role is configured as well as the IP address of the device. The Global Gateway can only be a Mesh End so there is no option to configure it. The IP address is configured manually from the Train2Track VN IP Pool in that PoP. The shared password must be the same on all the FM devices communicating with it.

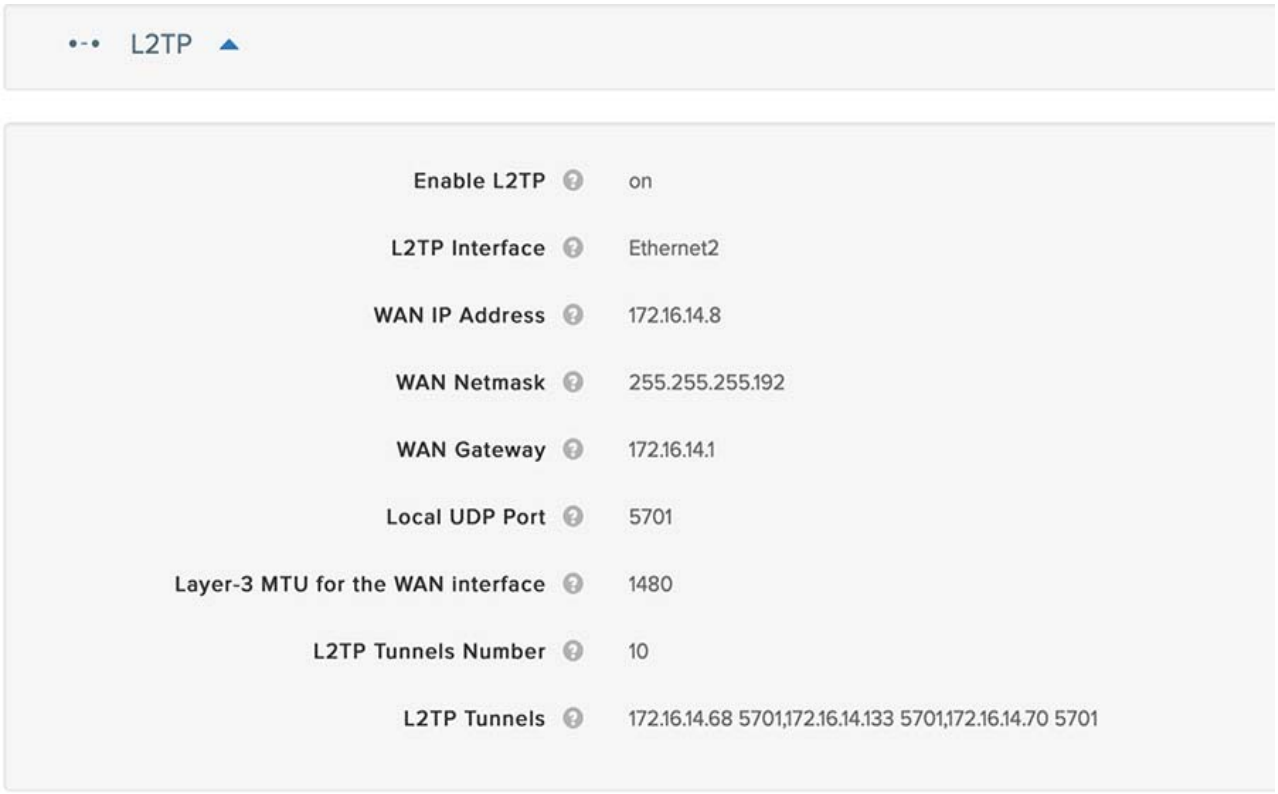
Figure 479 Global Gateway General Mode



L2TP Configuration

The Global Gateway must be configured with L2TP tunnels to every Mesh End to enable the seamless roaming between subnets. A separate IP address is configured for each end of the L2TP tunnel. In this guide, the L2TP tunnel IP addresses are configured as 1 higher than the interface address. This must be taken into account when configuring the L2TP tunnel destination IP on the Mesh Ends. The UDP port for L2TP is also required and by default it is 5701. Figure 480 is an example of the L2TP tunnels from the Global Gateway to every Mesh End.

Figure 480 Global Gateway L2TP Tunnel

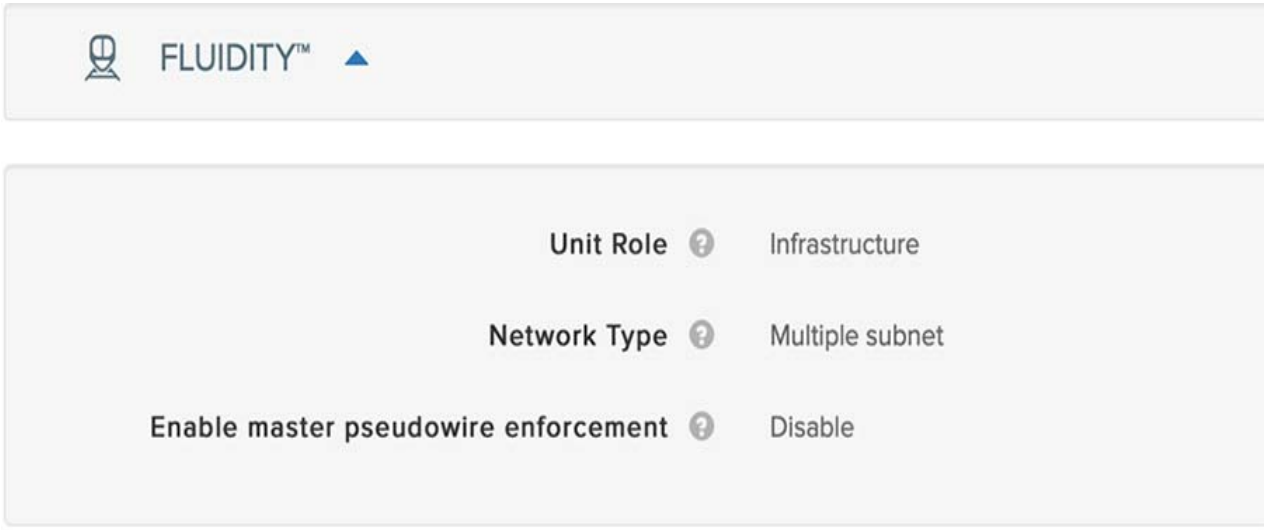


When Mesh Ends are configured in redundant mode using TITAN, the Global Gateway must point to each Mesh End.

Fluidity

The final required configuration is under the Fluidity section. To enable Layer 3 Fluidity, the network type must be “Multiple subnets” and the Global Gateway feature must be enabled.

Figure 481 Global Gateway Fluidity



Once these tasks are completed, the Global Gateway will wait for Mesh Ends to build L2TP tunnels to it.

Mesh End

Because the Mesh Ends transport all data from the train to the Global Gateway and vice versa, these devices should be located near the Fabric in a box border node in terms of network positioning. Once the train data is encapsulated in L2TP, it can quickly reach the border node and get forwarded to the Global Gateway. In this deployment, a Mesh End can be a FM 3500 or the FM 1000. Note that the FM 1000 does not have any radio functionality and should not be deployed in a wayside or roadside cabinet because of the environmental conditions.

General Mode

The configuration of a Mesh End is very similar to the Global Gateway except for the radio functions of the FM 3500. The Mesh End must be configured with an IP address in the correct IP Pool for the Edge PoP in the General Mode section. The FM 1000 can only operate as a Mesh End while the FM 3500 can operate as a Bridge, Mesh Point, or Mesh End. Examples of both configurations are shown in Figure 482 and Figure 483.

Figure 482 FM 1000 General Mode

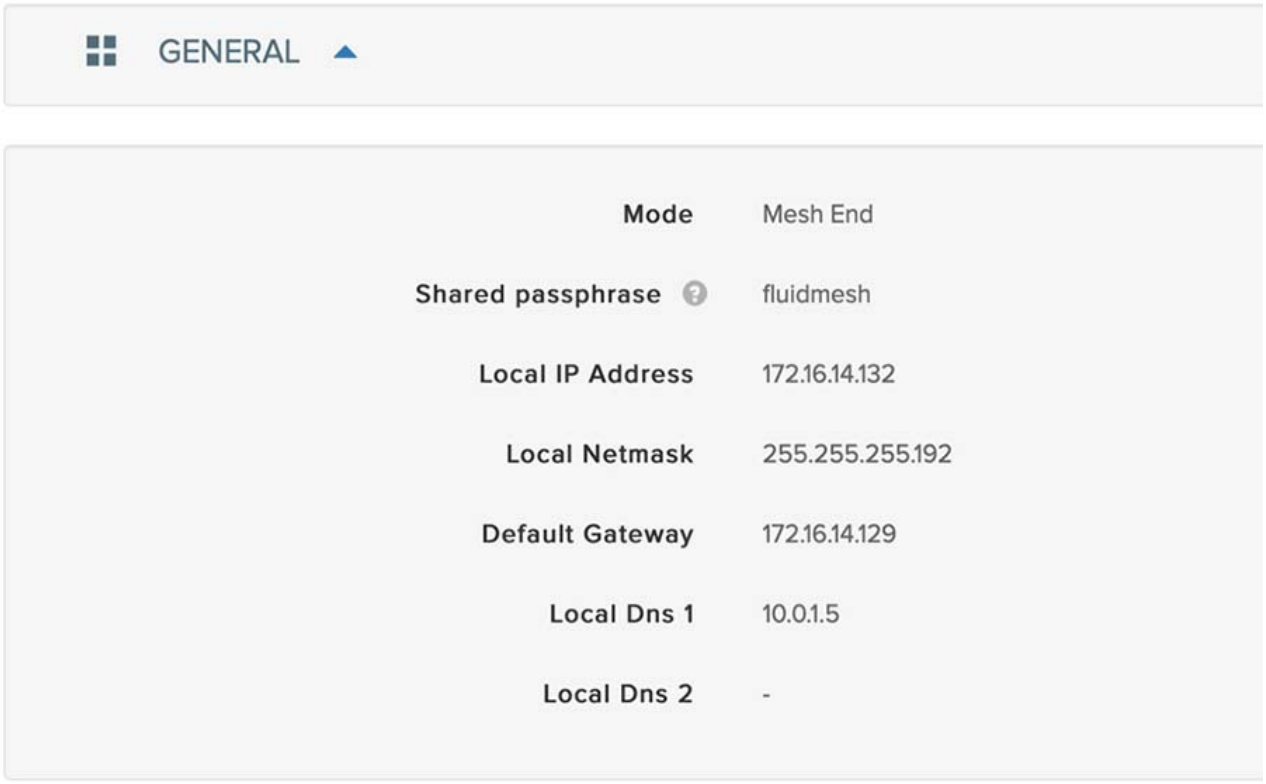
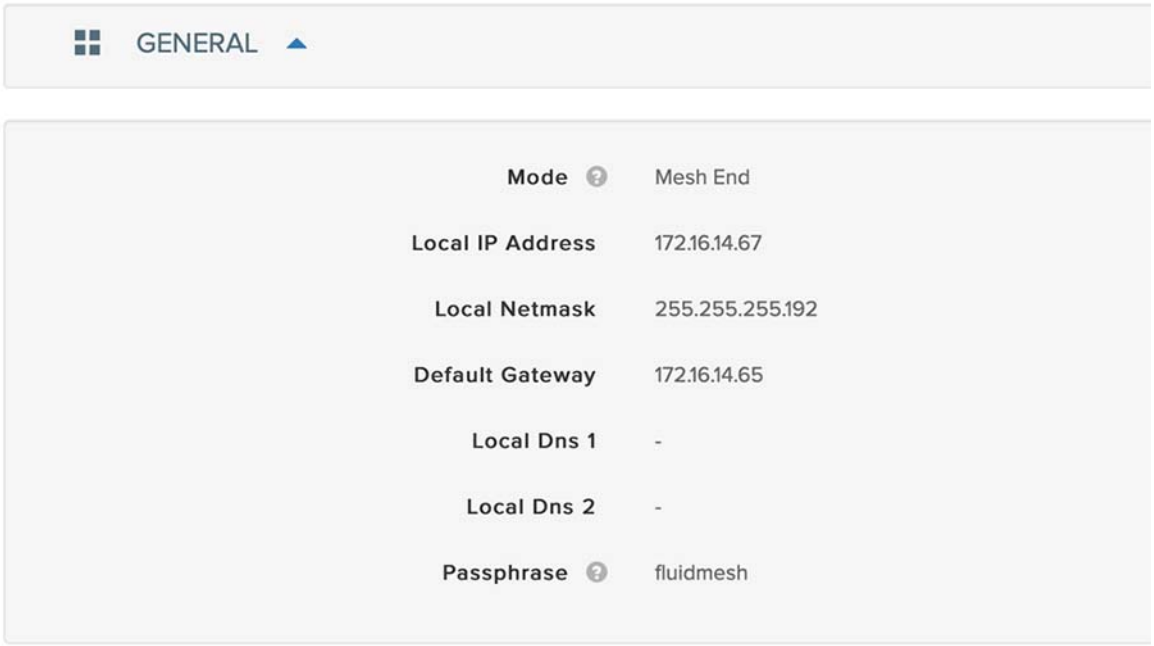


Figure 483 FM 3500 Mesh End General Mode

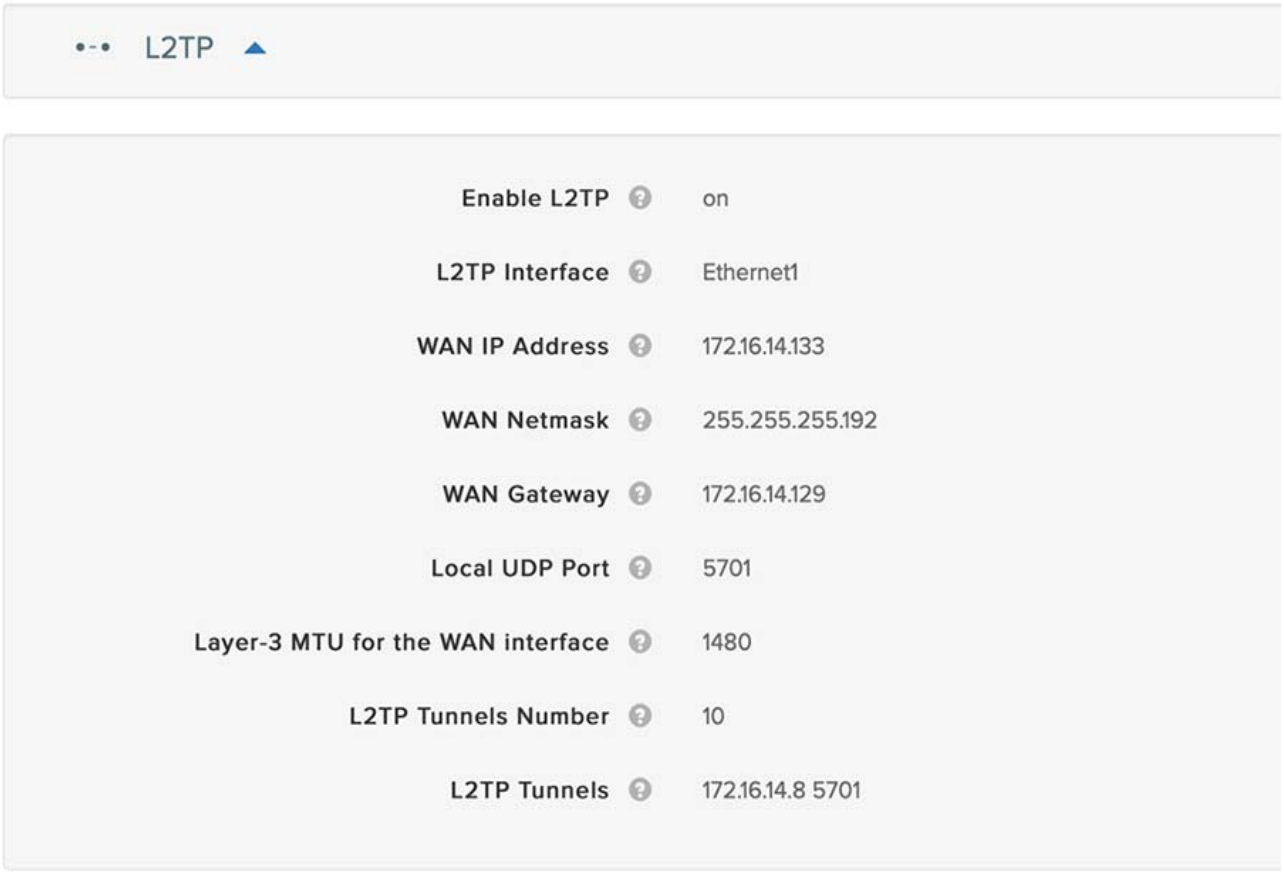


When configuring an FM 3500, there is the extra step of choosing which mode the unit will be in.

L2TP

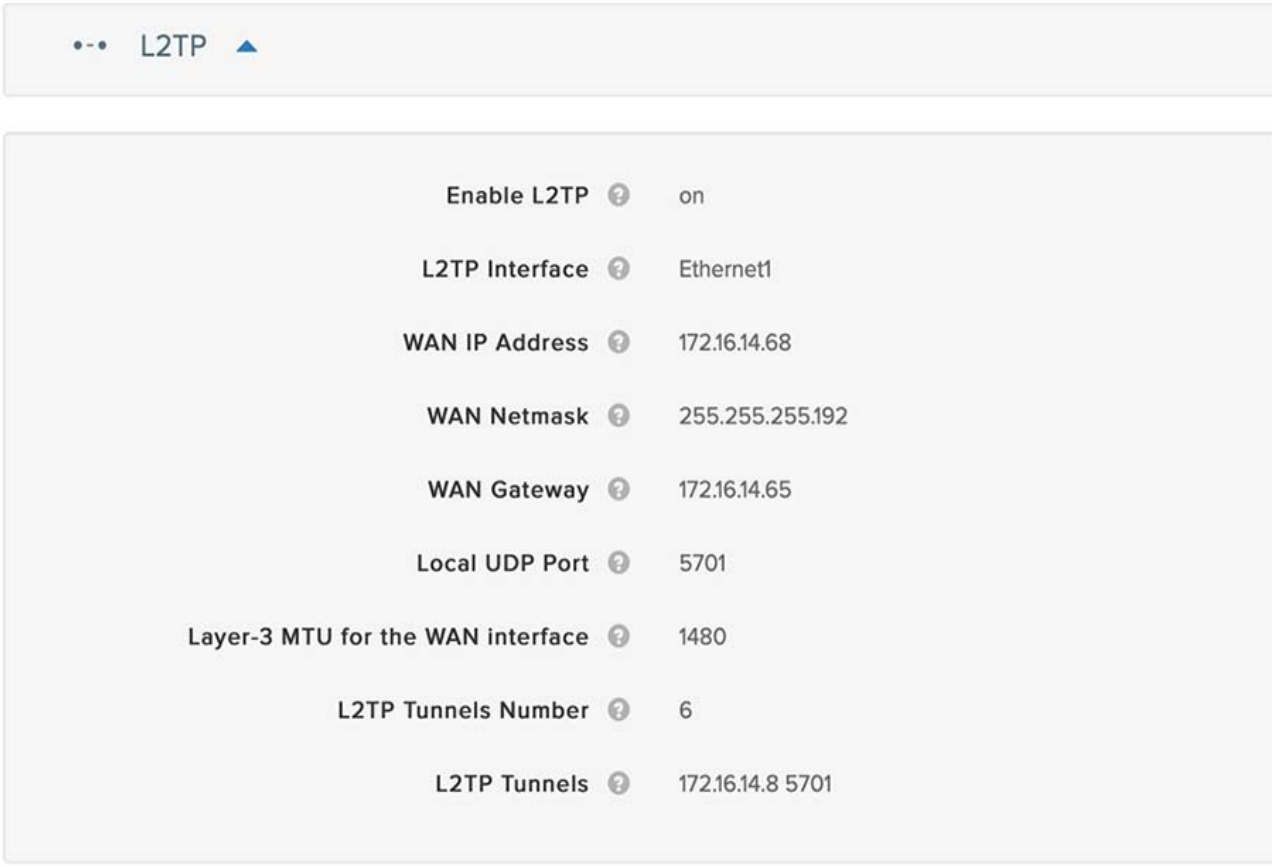
When configuring L2TP on the Mesh Ends, they only need tunnels pointing to the Global Gateway, not the other Mesh Ends. As mentioned in the Global Gateway section, the L2TP tunnels have their own virtual IP address and in this guide the host address is 1 digit higher than the interface address. If the Global Gateways are in redundant mode with TITAN, each Mesh End must configure an L2TP tunnel to each Global Gateway.

Figure 484 FM 1000 L2TP to Global Gateway



When a Mesh End is configured in redundant mode, the standby Mesh End L2TP tunnel will come up in IDLE Status.

Figure 485 FM 3500 Standby L2TP Configuration



Fluidity

When configuring Fluidity, the FM 1000 has the same configuration except for the Global Gateway setting. The FM 3500 cannot be a Global Gateway, but it includes the wireless specific components. Because this implementation uses Layer 3 Fluidity, the Network Type must be set to “Multiple subnets.” The differences are shown in Figure 486 and Figure 487.

Figure 486 FM 1000 Fluidity

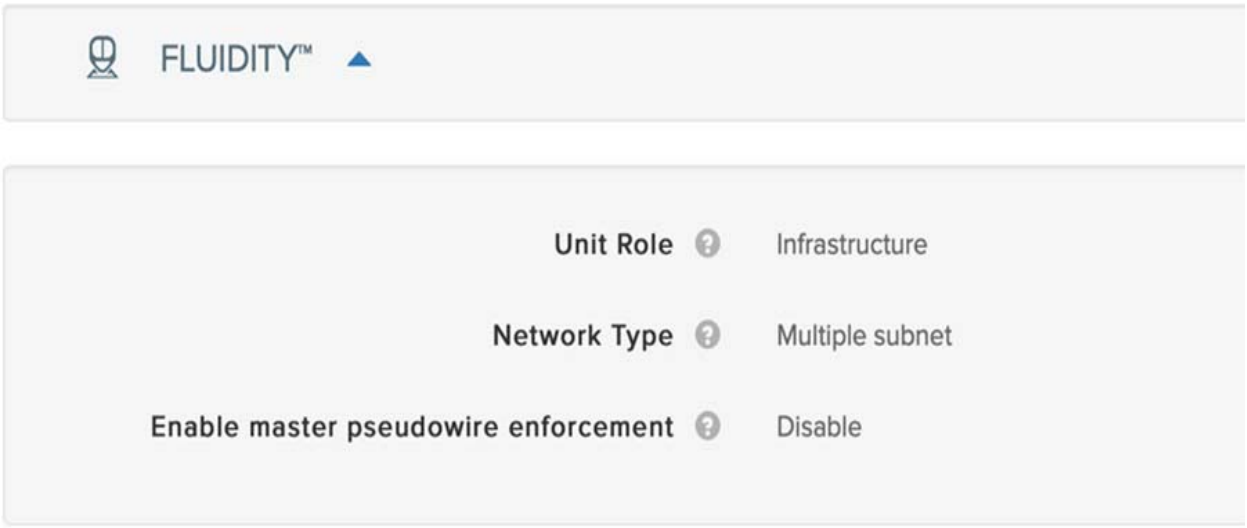
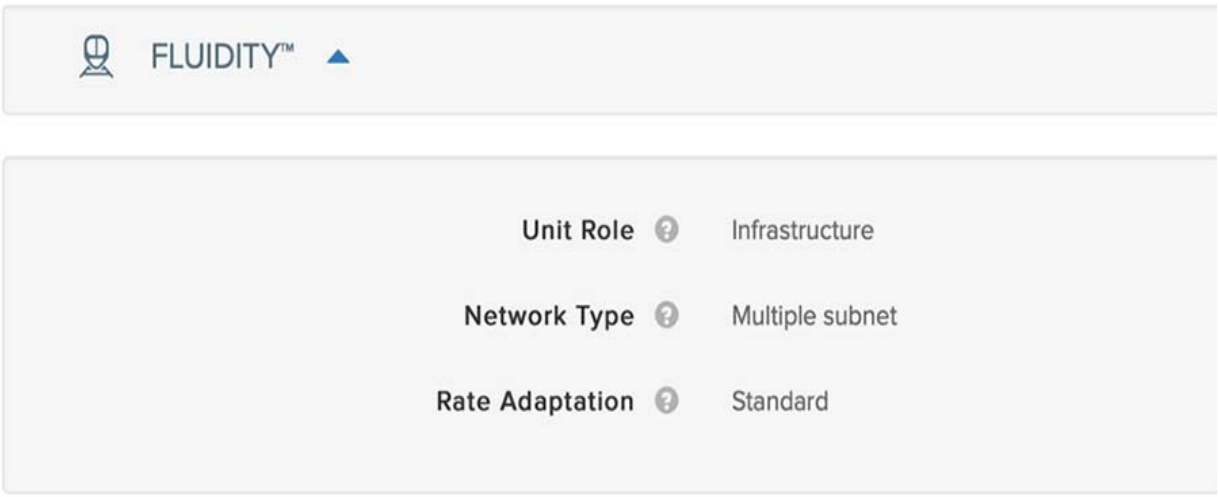


Figure 487 FM 3500 Fluidity



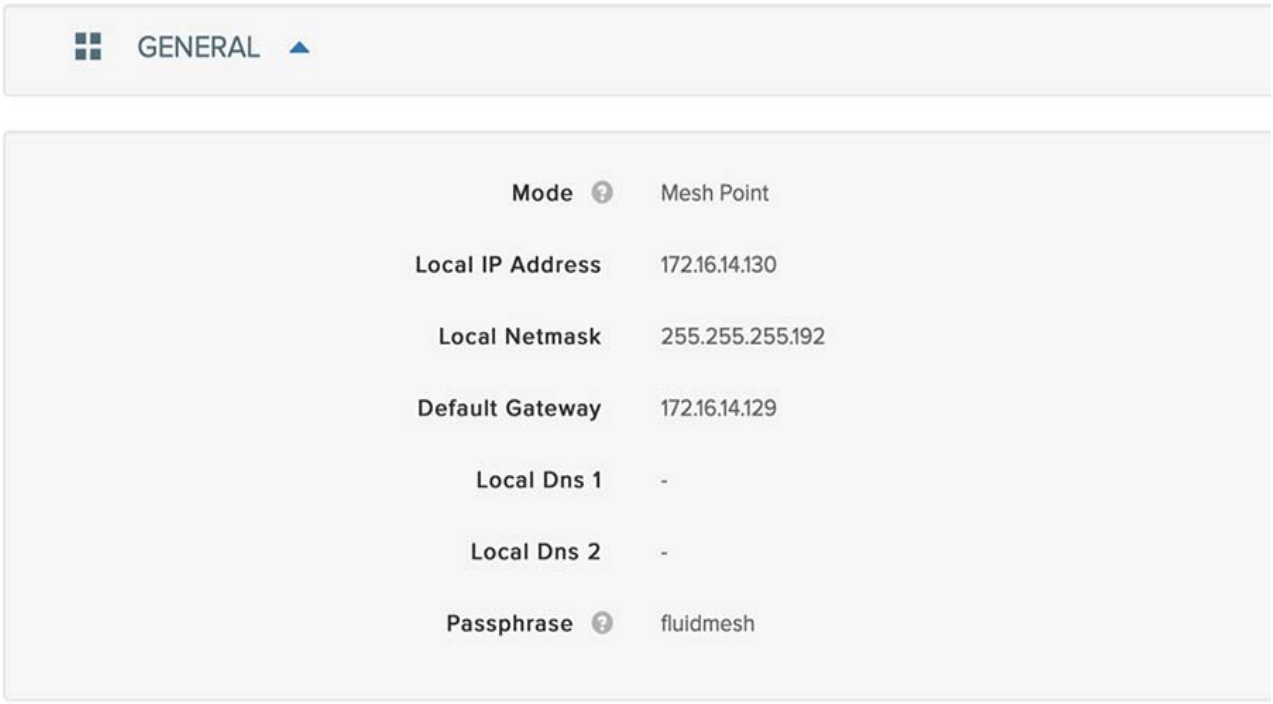
Mesh Point

A Mesh Point differs from a Mesh End in that it swaps the MPLS labels, whereas the Mesh End imposes or removes the L2TP header. The FM 3500 is the only trackside radio that can operate as a Mesh Point and is the only trackside radio that can communicate with the FM 4500 train radio. The configuration difference is that there is no L2TP configuration section.

General Mode

In General Mode, the Mesh Point radio button is selected and the device is put into the same subnet as the Mesh End for the radio group.

Figure 488 FM 3500 Mesh Point General Mode



Fluidity

The Fluidity configuration of the Mesh Point is the same as the Mesh End.

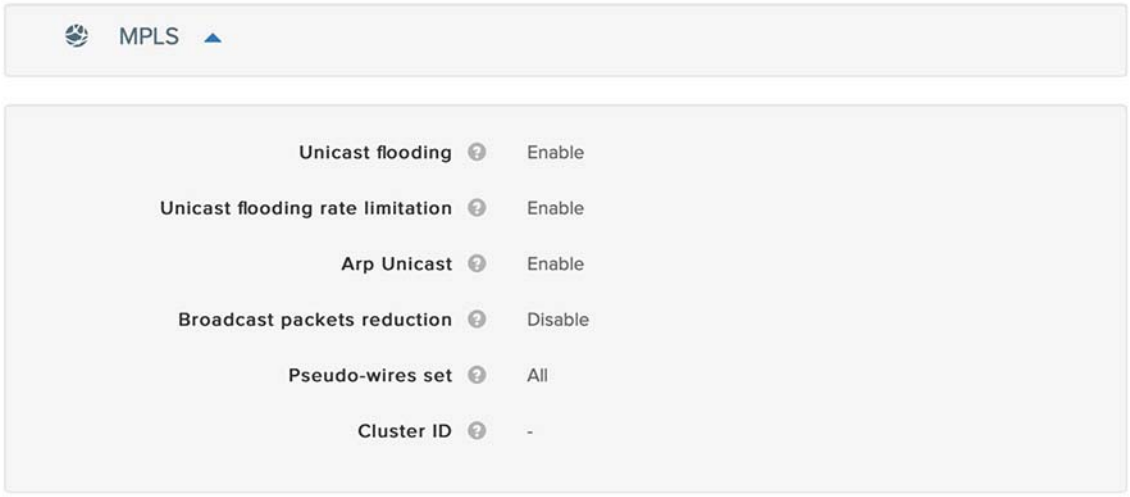
TITAN

TITAN is the redundancy feature, also known as Fast Failover. Since the Mesh End and Global Gateway are critical for transporting the train traffic from end to end, it is recommended to have a pair of devices when deployed: two Global Gateways in the data center and then a pair of Mesh Ends for every group of trackside Mesh Points. During testing, it was observed that without the TITAN feature enabled on those devices, the failure recovery time was on the order of a few minutes. With TITAN enabled, the failure recovery time was 500–600 ms.

When enabled, the TITAN feature works by sending periodic keepalives between the two units. When the primary fails, the secondary updates the other radios with a primary change command. It updates its own MAC and MPLS tables. It then sends gratuitous ARPs out to the connected switch.

This feature is one that cannot be configured through the built-in Configurator tool but only through the RACER portal or the CLI. Figure 489 shows an example of the recommended settings to configure TITAN.

Figure 489 MPLS Unicast Flooding



In Figure 490 and Figure 491, an additional IP address is allocated out of the same IP Pool for the virtual hot-standby address.

Figure 490 TITAN Fast Failover

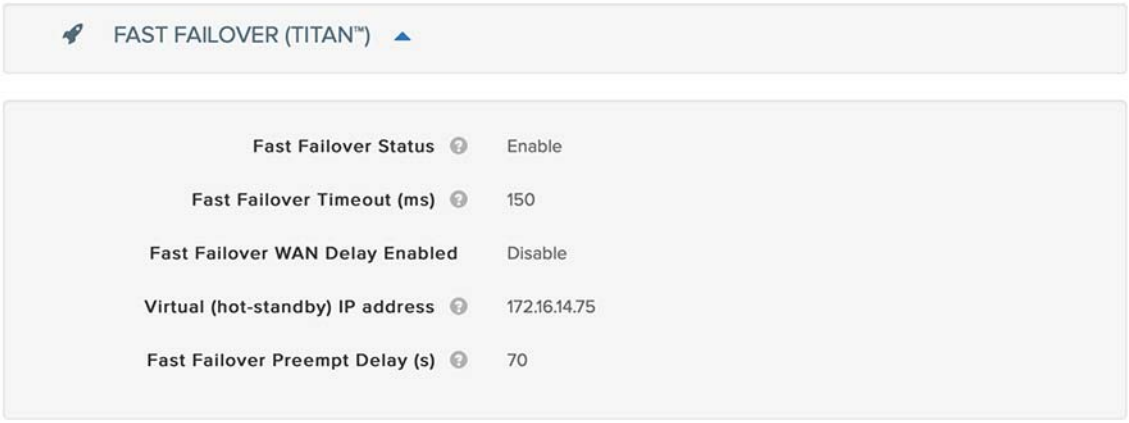
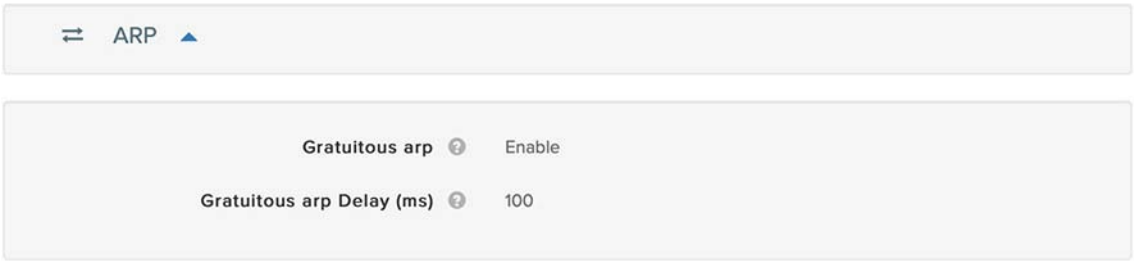


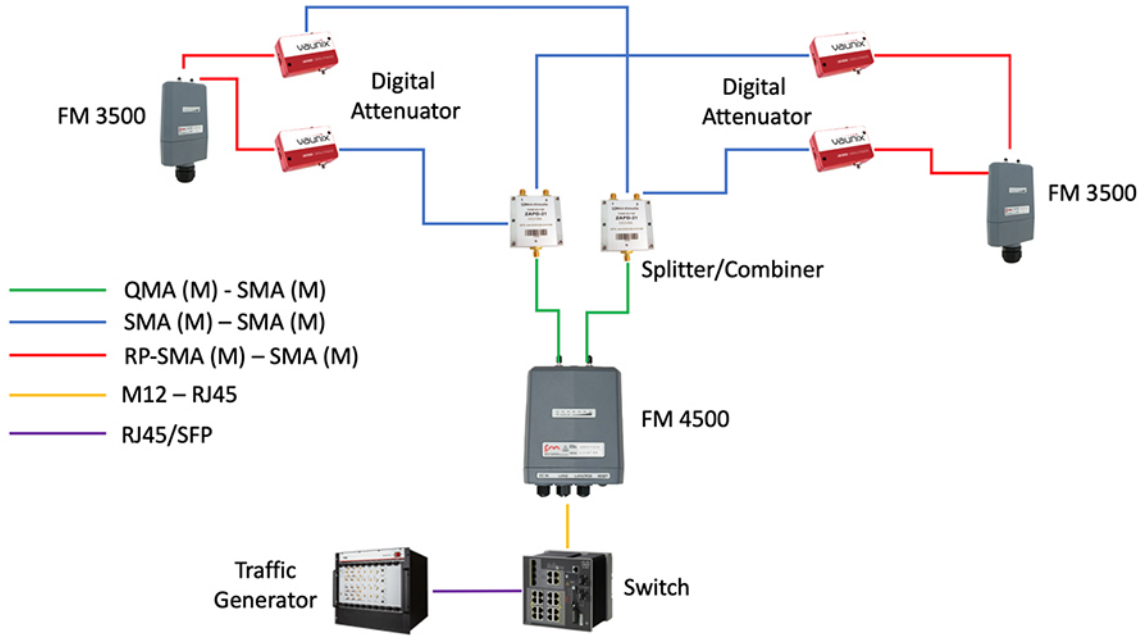
Figure 491 Gratuitous ARP



Wireless Roaming Test

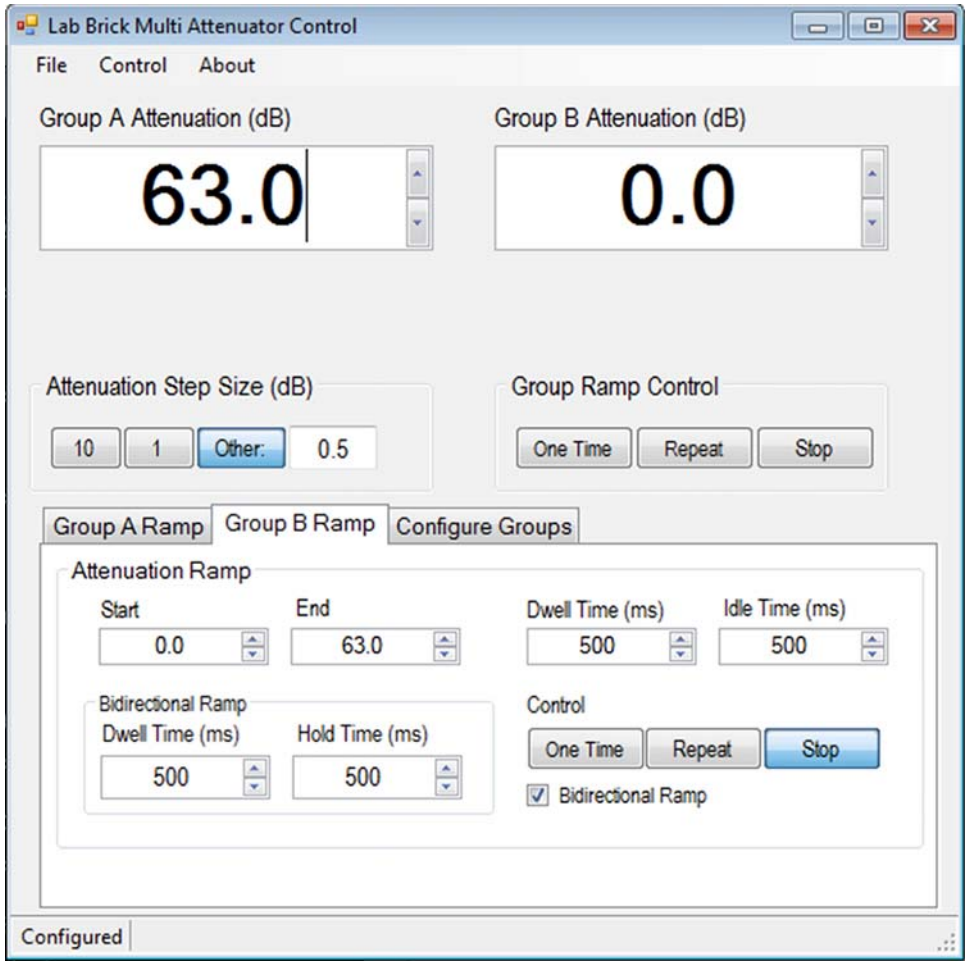
In this guide, the focus was on enabling wireless roaming between an Edge PoP in the CCI network rather than a detailed explanation of the specific wireless parameters for a trackside wireless deployment. To verify that traffic could pass end to end from a train to the data center while roaming between the Edge PoPs, a roaming testbed was built using digital attenuators to simulate the roaming. An example setup is shown in Figure 492.

Figure 492 Lab Roaming Setup



Each FM 3500 is placed in a different Edge PoP in the same VN but a different IP subnet. A traffic generator is placed in the data center and behind the train radio. The attenuators are grouped in the software so each set can be changed at the same time to provide a smooth attenuation profile. An example of the interface and profile is shown in Figure 493.

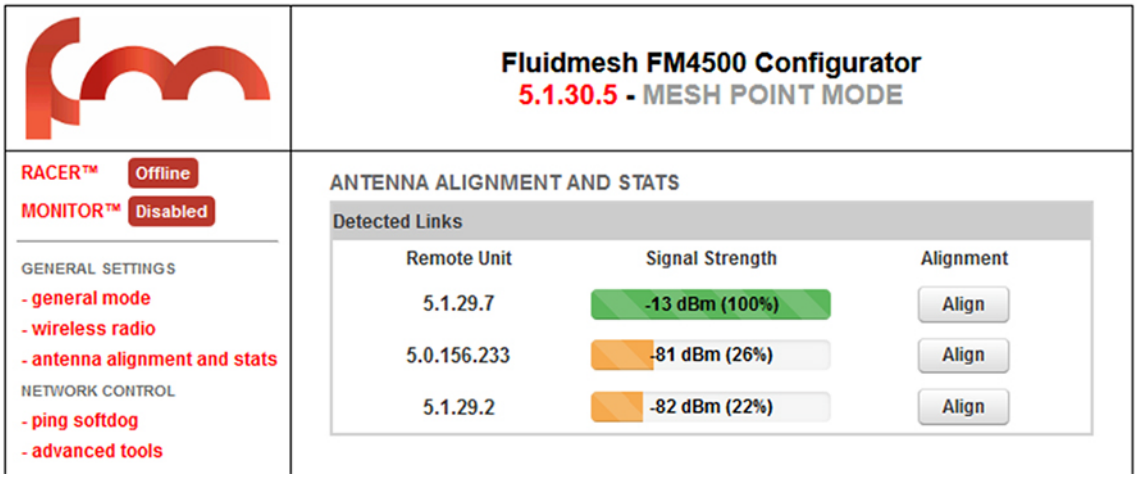
Figure 493 Digital Attenuator Profile



The attenuators are configured so the FM 4500 has a strong signal to a single FM 3500. The software is configured such that one group of attenuators starts at maximum attenuation and the other group is set at no attenuation. It will then step through the configured sequence so at the end of the process, each group of attenuators will have smoothly transitioned to the other end of the attenuation limits.

Bidirectional traffic is then started and checked for stability. Once stable, the digital attenuator profile is started. While running, the mobile train radio power levels can be monitored to ensure there is a smooth transition between the two FM 3500 radios. These power levels can be checked from the Configurator page on the mobile radio under the Antenna Alignment and stats section.

Figure 494 FM 4500 Antenna Alignment and Statistics



As a final check, the interface statistics on each IE switch with a connected FM 3500 radio are checked to see that the interface connected to the radio with the stronger signal is passing the traffic while the interface connected to the radio with the weaker signal has no traffic.

While the attenuator profile is running, the traffic generator's running statistics are monitored for any traffic loss. In this lab run test, there were no dropped packets during the handover between FM 3500 radios.

A real world scenario will depend heavily on the site survey, antenna selection, and wireless parameter optimization of the radios.

Caveats and Open Issues

This section details the caveats and open issues encountered while integrating CCI network.

Table 37 Caveats

Open Issues	Workaround
Cisco Catalyst 9300 stack in PoP for connecting fabric sites together via IP Transit (MPLS/Ethernet) contains single link from each switch in the stack towards transit network. Although Cisco Catalyst 9300 stack provides redundancy for PoP devices, it has been observed that the failover for traffic towards transit network approximates to 75s during implementation.	Recommendation is to use port channel towards transit network from each switch in the stack to avoid such a long failover.
After the TPE is installed and it is upgraded, a slow Internet connection may cause the upgrade to take several hours. The upgrade of the TPE may also halt at certain stage.	The upgrade must be re-initiated (if it had halted) and the upgrade will resume from the last failed point. This may have to be done several time for the successful upgrade. Having a fast Internet connection resolves the issue.
If the Internet connectivity of the TPE is lost, the Actility account may become inaccessible.	Once the Internet connection resumes, restart the TPE services and re-login from a new browser window
When entire SVL links between Fabric in a Box POP fails, Intermittent Loop and MAC flaps observed might be observed in CCI Access Rings.	Shut/no shut of 9500 REP interface would resolve the outage.
When REP interface failure seen on 9500 POP (aggregator) Node, Intermittent Traffic outage will be observed. Traffic flow will resume in few seconds after blocked port transition to forwarding state.	Not available.
With HA/SSO Events on 9500 POP (aggregator) Node, Intermittent Multicast Traffic outage will be observed for short duration. Traffic will resume in few seconds after HA event.	Not available.

Appendix: Configuration Examples

This appendix, which provides some example running configuration of few devices in the CCI network and IP addressing used in this CVD validation for the network topologies, as shown in Figure 3 and Figure 4 includes the following major topics:

IP Addressing of Solution Components

This section provides complete list of IP addressing used for various solution components in this CVD validation.

Table 38 provides the Underlay network IP addressing configuration used for the network topologies (IP transit-based and SD-Access Transit-based via Ethernet network backhaul), as shown in Figure 3 and Figure 4.

Table 38 Underlay Network IP Addressing

Prefix	Purpose	Components Connected by the subnet	IP Address
192.0.x.0/32	Loopback addresses for all the devices in the network topology. All fabric and non-fabric devices in the network.	PoP1: Cisco Catalyst 9500 SVL	192.0.160.11
		PoP2: Cisco Catalyst 9300 stack	192.0.150.11
		PoP3: Cisco Catalyst 9300 Stack	192.0.120.11
		RPoP1: Cisco IR1101	192.168.200.25
		HQ/DC Site: Cisco Catalyst 9300 stack	192.0.140.11
		Transit Site: Cisco Catalyst 9500 switch1	192.0.130.11
		Transit Site: Cisco Catalyst 9500 switch2	192.0.130.12
120.120.120.0/30	Example PoP3: Underlay Network Point-to-Point L3 interfaces	PoP3: Cisco Catalyst 9300 switch 1	120.120.120.2
120.120.121.0/30		PoP3: Cisco Catalyst 9300 switch 2	120.120.121.2
120.120.120.0/30		Transit Site: Cisco Catalyst 9500 switch1	120.120.120.1
120.120.121.0/30		Transit Site: Cisco Catalyst 9500 switch2	120.120.121.1
130.130.130.0/30	Transit Site: Underlay Network Point-to-Point L3 Interfaces between Catalyst 9500 switches	Transit Site: Cisco Catalyst 9500 switch1	130.130.130.1
		Transit Site: Cisco Catalyst 9500 switch2	130.130.130.2
120.120.122.0/30 120.120.123.0/30 120.120.122.0/30 120.120.123.0/30	HQ/DC site: Underlay Network Point-to-Point L3 interfaces	HQ/DC: Cisco Catalyst 9300 switch 1	120.120.122.2
		HQ/DC: Cisco Catalyst 9300 switch 2	120.120.123.2
		Transit Site: Cisco Catalyst 9500 switch1	120.120.122.1
		Transit Site: Cisco Catalyst 9500 switch2	120.120.123.1
50.50.50.0/30	Fusion Router: Underlay Network Point-to-point L3 interfaces	Fusion Router: CSR1KV-1	50.50.50.1
50.50.51.0/30		Fusion Router: CSR1KV-2	50.50.51.1
50.50.50.0/30		HQ/DC: Cisco Catalyst 9300 switch 1	50.50.50.2
50.50.51.0/30		HQ/DC: Cisco Catalyst 9300 switch 2	50.50.51.2
10.10.100.0/24	Shared Services Network	Cisco DNA Center Appliance	10.10.201.202
		Cisco Identity Service Engine (ISE)	10.10.100.55
		DHCP & DNS server	10.10.100.20
		Field Network Director (FND)	10.10.100.11
		CUWN WLC (C9800)	10.10.100.188
		Cisco Prime Infrastructure (PI)	10.10.100.65
		Cisco Stealthwatch Management Console	10.10.100.75
		Cisco Stealthwatch Flow Collector	10.10.100.85
10.10.204.0/24	Internet Edge/DMZ Network Connectivity (Inside)	Firepower2140: L3 Interfaces	10.10.204.1
		Fusion Router: CSR1KV-1	10.10.204.2
		Fusion Router: CSR1KV-2	10.10.204.3
10.40.100.0/24	DMZ Network Headend Router (HER) network	Firepower2140: L3 Interface to Headend Routers	10.40.100.1
		HER1	10.40.100.101
		HER2	10.40.100.102
		HER HSRP Virtual IP	10.40.100.100

Table 39 Fabric Overlay Network IP Addressing

Prefix	Purpose	Component(s) Connected by the Subnet	IP Address
172.10.80.0/24	PoP1: Data network IP Subnet for IP Cameras in SnS_VN	IPVC8030 Camera1	172.10.80.10
172.10.100.0/24	PoP2: Data network IP Subnet for IP Cameras in SnS_VN	IPVC8030 Camera2	172.10.100.10
172.10.90.0/24	PoP3: Data network IP Subnet for IP Cameras in SnS_VN	IPVC8030 Camera3	172.10.90.10
172.16.70.0/20	HQ/DC site: Data network IP Subnet for Servers in SnS_VN	Cisco VSM	172.16.70.11
172.20.80.0/24	PoP1: Data network IP Subnet in Lighting_VN	CGR1240-1	172.20.80.10
172.20.100.0/24	PoP2: Data network IP Subnet in Lighting_VN	CGR1240-2	172.20.100.10
172.20.90.0/24	PoP3: Data network IP Subnet in Lighting_VN	CGR1240-3	172.20.90.10
172.17.70.0/24	HQ/DC site: Data network IP Subnet for Servers in Lighting_VN	HQ/DC Site: ECC-CA & NPS Server	172.17.70.11
		HQ/DC Site: RSA-CA Server	172.17.70.12
172.21.80.0/24	PoP1: Data network IP Subnet for Lorawan Gateways	IXM Gateway1	172.21.80.11
172.21.100.0/24	PoP2: Data network IP Subnet for Lorawan Gateways	IXM Gateway2	172.21.100.11
172.21.90.0/24	PoP3: Data network IP Subnet for Lorawan Gateways	IXM Gateway3	172.21.90.11
172.21.70.0/24	HQ/DC site: Data network IP Subnet for Lorawan Server	TPE Server	172.21.70.11
192.168.X.0/24	SDA Transit Border Handoff Network Global Prefix	PoP1: Border Handoff network subnet	192.168.80.0/30
		PoP2: Border Handoff network subnet	192.168.100.0/30
		PoP3: Border Handoff network subnet	192.168.90.0/30
		HQ/DC Site: Border Handoff network subnet	192.168.40.0/30
192.100.X.0/24	Global IP Prefix used for Extended Nodes in the network	PoP1: Extended Nodes Subnet Pool	192.100.80.0/24
		PoP2: Extended Nodes Subnet Pool	192.100.100.0/24
		PoP3: Extended Nodes Subnet Pool	192.100.90.0/24

Table 39 provides the Fabric Overlay network IP addressing configuration used for the network topology (SD-Access Transit-based via Ethernet network backhaul), as shown in Figure 3.

Table 40 provides the IP addressing configuration used for the network topology (IP Transit-based via MPLS backhaul), as shown in Figure 4.

Table 40 IP Addressing Details for MPLS Backhaul Network Topology

Prefix	Purpose	Components Connected by the subnet	IP Address
192.168.11.x / 32	Loopback addresses for all the devices in the network topology. All fabric and non-fabric devices in the network.	HQ/DC Site - Cisco Catalyst 9500	192.168.11.2
		HQ/DC Site - Cisco Catalyst 9300	192.168.11.4
		Site 1 - Cisco Catalyst 9300 Switch Stack	192.168.11.1
		Site 2 - Cisco Catalyst 9300 Switch Stack	192.168.11.5
		Fusion Router	192.168.11.100
172.16.3.0/24	Prefix for LoRaWAN network in HQ	ThingPark Enterprise (TPE)	172.16.3.2
172.16.12.0/26	Prefix for DSRC upstream network in HQ	Cisco Edge & Fog Processing Module (EFM)	172.16.12.6
172.16.5.0/26	Prefix for Iteris in HQ		
172.16.6.0/26	Prefix for Schneider in HQ		
172.16.11.0/26	Prefix for DSRC Management network in Site 1	Cisco IC3000 management	172.16.11.6
172.16.12.64/26	Prefix for DSRC upstream network in Site 1	Cisco IC3000 upstream	172.16.12.66
192.168.0.0/26	Prefix for DSRC downstream network in Site 1	Cisco IC3000 downstream	192.168.0.11
		Cohda RSU	192.168.0.12
172.16.4.0/25	Prefix for LoRaWAN network in Site 1	Cisco Wireless Gateway for LoRaWAN	172.16.4.2
172.16.11.64/26	Prefix for DSRC Management network in Site 2	Cisco IC3000 management	172.16.11.68
172.16.12.128/26	Prefix for DSRC upstream network in Site 2	Cisco IC3000 upstream	172.16.12.131
192.168.0.64/26	Prefix for DSRC downstream network in Site 2	Cisco IC3000 downstream	192.168.0.68
		Cohda RSU	192.168.0.69
172.16.4.128/25	Prefix for LoRaWAN network in Site 2	Cisco Wireless Gateway for LoRaWAN	172.16.4.131
10.0.1.x/24	Shared Services Network Prefix	Cisco DNA Center	10.0.1.2
		Cisco ISE	10.0.1.5
		DHCP/DNS Server	10.0.1.6
		Field Network Director (FND)	10.0.1.7
		Fog Director (FD)	10.0.1.11

Configuration Examples for IP Transit, HER, and FiaB

This section provides the running configuration of fusion routers and Headend router FlexVPN configuration examples in both IP Transit and SD-Access Transit-based network topologies validated in this CVD.

IP Transit-based Fabric Interconnection on Ethernet Backhaul

The Fusion Router configuration example for the IP Transit-based Fabric Interconnection on Ethernet backhaul network is given below:

```
version 16.11
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname C9500-30-CP1
!
!
vrf definition Lighting_VN
 rd 1:4099
 !
 address-family ipv4
  import ipv4 unicast map SS-NETWORK-TO-VRF
  export ipv4 unicast map Lighting-VN-TO-GLOBAL
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition SnS_VN
 rd 1:4100
 !
 address-family ipv4
  import ipv4 unicast map SS-NETWORK-TO-VRF
  export ipv4 unicast map SnS-VN-TO-GLOBAL
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
!
enable secret 9 <Shared_Secret Value>
enable password 7 <Enable_Password>
!
aaa new-model
!
!
aaa group server radius Cisco DNA Center-client-radius-
 group server name Cisco DNA Center-radius_10.10.100.52
 ip radius source-interface Loopback0
!
aaa group server radius Cisco DNA Center-network-radius-
 group server name Cisco DNA Center-radius_10.10.100.52
 ip radius source-interface Loopback0
!
```

```
aaa authentication login default local
aaa authentication login VTY_authen group Cisco DNA Center-network-radius-group
local aaa authentication dot1x default group Cisco DNA Center-client-radius-group
aaa authorization exec default local
aaa authorization exec VTY_author group Cisco DNA Center-network-radius-group
local aaa authorization network default group Cisco DNA Center-client-radius-
group
aaa authorization network Cisco DNA Center-cts-list group Cisco DNA Center-client-radius-
group aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group Cisco DNA Center-client-radius-group
aaa accounting exec default start-stop group Cisco DNA Center-network-radius-group
!
aaa server radius dynamic-author
 client 10.10.100.52 server-key 7 <Server_Key>
!
aaa session-id common
boot system switch all
flash:cat9k_iosxe.16.11.01c.SPA.bin switch 1 provision
c9500-16x
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-
 licensing@cisco.com profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method
email ip routing
!
ip name-server 10.10.100.10
ip domain name ccibgl.cisco.com
!
login on-success log
!

vtp mode
transparent ipv6
unicast-routing
no device-tracking logging
theft access-session mac-
move deny
!

crypto pki trustpoint SLA-
 TrustPoint enrollment pkcs12
 revocation-check crl
!

crypto pki trustpoint TP-self-signed-
 1828488938 enrollment selfsigned

 subject-name cn=IOS-Self-Signed-Certificate-
 1828488938 revocation-check none
 rsakeypair TP-self-signed-1828488938
!

crypto pki trustpoint Cisco DNA
 Center-CA enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
```

```
!
crypto pki certificate chain SLA-
 TrustPoint certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101
  0B050030 <Snipped>
  quit
crypto pki certificate chain TP-self-signed-1828488938
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  <Snipped>
  quit
crypto pki certificate chain Cisco DNA Center-CA
 certificate ca 00E0F446909D34DA93
  30820397 3082027F A0030201 02020900 E0F44690 9D34DA93 300D0609
   2A864886 <Snipped>
  quit
!
cts authorization list Cisco DNA Center-cts-list
license boot level network-advantage addon dna-advantage
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 141152
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
 linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
dot1x system-auth-control
!
username dna privilege 15 password 7 106D000A0618325A5E57
!
redundancy
 mode sso
!
transceiver type all
 monitoring
!
vlan 50,200-201,300
!
vlan 401
 name UNDERLAY_40_SITE
!
vlan 600-603
!
vlan 1000
 name SHARED_SERVICES
!
vlan 3001-3009
!
vlan 3010
 name INFRA_VN_STACK_20
!
vlan 3011
 name SnS_VN_STACK_20
!
vlan 3012
 name Lighting_VN_STACK_20
!
```

```
class-map match-any system-cpp-police-ewlc-control
 description EWLC Control
class-map match-any system-cpp-police-topology-control
 description Topology control
class-map match-any system-cpp-police-sw-forward
 description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic


 class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic
 class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
 class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
 class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
 class-map match-any system-cpp-police-forus
   description Forus Address resolution and Forus traffic
 class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA
 match dscp cs1
 match dscp af12
 match dscp af13
 match dscp af11
 class-map match-any system-cpp-police-multicast-end-station
   description MCAST END STATION
 class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
 class-map match-any system-cpp-police-multicast
   description MCAST Data
 class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
 match dscp cs3
 match dscp cs2
 match dscp cs7
 match dscp cs6
 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
 match dscp af43
 match dscp af41
 match dscp af42
 class-map match-any system-cpp-police-l2-control
  description L2 control
 class-map match-any system-cpp-police-dot1x-auth
   description DOT1X Auth
 class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
 class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
 match dscp cs5
 match dscp cs4
 class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
 match dscp ef
 class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual OOB
 class-map match-any non-client-nrt-class
 class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
 class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
 class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
```

```
 class-map match-any system-cpp-police-ios-routing
  description L2 control, Topology control, Routing control, Low Latency
 class-map match-any DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
 match dscp af23
 match dscp af21
 match dscp af22
 class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
 class-map match-any system-cpp-police-ios-feature
  description
ICMPGEN,BROADCAST,ICMP,L2LVXCntrl,ProtoSnoop,PuntWebauth,MCASTData,Transit,DOT1XAuth,Swfwd,LOGGING,
L2LVXData,ForusTraffic,ForusARP,McastEndStn,Openflow,Exception,EGRExcption,NflSampled,RpfFailed
 class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
 match dscp af32
 match dscp af33
 match dscp af31
!
policy-map system-cpp-policy
policy-map DNA-dscp#APIC_QOS_Q_OUT
 class DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
  priority level 1
  police rate percent 2
  queue-buffers ratio 5
class DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
 priority level 2
 police rate percent 26
 queue-buffers ratio 5
class DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
 bandwidth remaining percent 21
 queue-buffers ratio 5
class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
 bandwidth remaining percent 1
 queue-buffers ratio 10
 queue-limit dscp af41 percent 100
 queue-limit dscp af42 percent 90
 queue-limit dscp af43 percent 80
class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
bandwidth remaining percent 1
 queue-buffers ratio 10
 queue-limit dscp af32 percent 90
 queue-limit dscp af33 percent 80
class DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
 bandwidth remaining percent 42
queue-buffers ratio 10
 random-detect dscp-based
 random-detect dscp 18 percent 80 100
 random-detect dscp 20 percent 70 100
 random-detect dscp 22 percent 60 100
class DNA-EZQOS_2P6Q3T_9K#BULK-DATA
 bandwidth remaining percent 8
 queue-buffers ratio 10
 random-detect dscp-based
 random-detect dscp 8 percent 60 100
 random-detect dscp 10 percent 80 100
 random-detect dscp 12 percent 70 100
 random-detect dscp 14 percent 60 100
class class-default
 bandwidth remaining percent 27
 queue-buffers ratio 25
 random-detect dscp-based
 random-detect dscp 0 percent 80 100
!
interface Loopback0
```

```
 ip address 192.0.30.11 255.255.255.255
!
interface Port-channel1
 switchport access vlan 300
 switchport mode access
!
interface Port-channel30
 description L3 PortChannel Interface to C9500-30-CP2
 no switchport
 ip address 30.30.30.1 255.255.255.252
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface TenGigabitEthernet1/0/1
 no switchport
 no ip address
 channel-group 30 mode active
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/2
 no switchport
 no ip address
 channel-group 30 mode active
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/3
 description Connected to C9300-20-STACK on Port Te1/1/1
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
interface TenGigabitEthernet1/0/4
 description connected to DC fabric site c9300-40-stack on port te 1/1/1
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/5
 description Connected to Site 2 C9300-60-STACK on port Te1/1/1
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/6
 description Connected to Nexus-5K-1 for Shared Services on Port Eth1/22
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/7
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/8
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/9
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/11
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
```

```
!
interface TenGigabitEthernet1/0/12
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/13
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/14
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/15
 switchport trunk allowed vlan 300
 service-policy output DNA-dscp#APIC_QOS_Q_OUTinterface TenGigabitEthernet1/0/16
 switchport access vlan 300
 switchport mode access
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/1
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/2
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/3
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/4
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/5
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/6
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/7
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/8
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet1/1/1
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet1/1/2
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 ip address 20.20.20.1 255.255.255.252
!
interface Vlan300
 ip address 10.30.200.2 255.255.255.252
 ipv6 address 2001:DB8:16:109::3/64
 ipv6 enable
!
interface Vlan401
 ip address 40.40.40.1 255.255.255.252
!
interface Vlan601
 ip address 60.60.60.1 255.255.255.252
!
```

```
interface Vlan1000
 ip address 10.10.100.6 255.255.255.0
 standby version 2
 standby 10 ip 10.10.100.1
 standby 10 priority 105
 standby 10 preempt delay minimum 120
 ipv6 address 2001:DB8:16:110::101/64
 ipv6 enable
!
interface Vlan3004
 description INFRA_VN for STACK40
 ip address 192.168.40.14 255.255.255.252
!
interface Vlan3005
 description SnS_VN for STACK40
 vrf forwarding SnS_VN
 ip address 192.168.40.18 255.255.255.252
!
interface Vlan3006
 description Lighting_VN for STACK40
 vrf forwarding Lighting_VN
 ip address 192.168.40.22 255.255.255.252
!
interface Vlan3010
 description INFRA_VN neighbour for 9300-stack-20
 ip address 192.168.20.14 255.255.255.252
!
interface Vlan3011
 description SnS_VN for STACK-20
 vrf forwarding SnS_VN
 ip address 192.168.20.18 255.255.255.252
!
interface Vlan3012
 description Lighting_VN for STACK-20
 vrf forwarding Lighting_VN
 ip address 192.168.20.22 255.255.255.252
!
router eigrp 1000
 network 10.10.100.0 0.0.0.255
 network 10.30.200.0 0.0.0.255
 network 20.20.20.0 0.0.0.3
 network 30.30.30.0 0.0.0.3
 network 40.40.40.0 0.0.0.3
 network 50.50.53.0 0.0.0.3
 network 192.0.30.11 0.0.0.0
 eigrp router-id 192.0.30.11
!
router ospf 1
 network 10.30.200.0 0.0.0.255 area 1
 network 10.30.201.0 0.0.0.255 area 1
!
router bgp 65500
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 30.30.30.2 remote-as 65500
 neighbor 192.168.20.13 remote-as 20
 neighbor 192.168.20.13 update-source Vlan3010
 neighbor 192.168.40.13 remote-as 40
 neighbor 192.168.40.13 update-source Vlan3004
 !
 address-family ipv4
  bgp aggregate-timer 0
```

```
  network 30.30.30.0 mask 255.255.255.252
  network 192.0.30.11 mask 255.255.255.255
  network 192.168.20.12 mask 255.255.255.252
  network 192.168.40.12 mask 255.255.255.252
  redistribute connected
  redistribute static
  neighbor 30.30.30.2 activate
  neighbor 192.168.20.13 activate
  neighbor 192.168.20.13 weight 65535
  neighbor 192.168.20.13 advertisement-interval 0
  neighbor 192.168.40.13 activate
  neighbor 192.168.40.13 weight 65535
  neighbor 192.168.40.13 advertisement-interval 0
  distribute-list 1 out
 exit-address-family
 !
 address-family ipv4 vrf Lighting_VN
  bgp aggregate-timer 0
  network 192.168.20.20 mask 255.255.255.252
  network 192.168.40.20 mask 255.255.255.252
  redistribute connected
  redistribute static
  neighbor 192.168.20.21 remote-as 20
  neighbor 192.168.20.21 update-source Vlan3012
  neighbor 192.168.20.21 activate
  neighbor 192.168.20.21 weight 65535
  neighbor 192.168.40.21 remote-as 40
  neighbor 192.168.40.21 update-source Vlan3006
  neighbor 192.168.40.21 activate
  neighbor 192.168.40.21 weight 65535
  default-information originate
 exit-address-family
 !
 address-family ipv4 vrf SnS_VN
  bgp aggregate-timer 0
  network 0.0.0.0
  network 10.40.100.0 mask 255.255.255.0
  network 192.168.20.16 mask 255.255.255.252
  network 192.168.40.16 mask 255.255.255.252
  redistribute connected
  redistribute static
  neighbor 192.168.20.17 remote-as 20
  neighbor 192.168.20.17 update-source Vlan3011
  neighbor 192.168.20.17 activate
  neighbor 192.168.20.17 weight 65535
  neighbor 192.168.40.17 remote-as 40
  neighbor 192.168.40.17 update-source Vlan3005
  neighbor 192.168.40.17 activate
  neighbor 192.168.40.17 weight 65535
  default-information originate
 exit-address-family
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
ip route 0.0.0.0 0.0.0.0 10.30.200.1
ip route 10.40.100.0 255.255.255.0 10.30.200.1
ip route 192.168.200.0 255.255.255.0 10.30.200.1
ip route vrf Lighting_VN 0.0.0.0 0.0.0.0 10.30.200.1
global ip route vrf SnS_VN 0.0.0.0 0.0.0.0 10.30.200.1
global !
ip ssh source-interface Loopback0
```

```
ip ssh version 2
!

ip prefix-list CESSNA_SnS_VN_ROUTES seq 5 permit 192.168.20.16/30 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 6 permit 192.168.20.4/30 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 7 permit 192.168.20.0/30 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 8 permit 172.10.20.0/24 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 9 permit 192.100.20.0/24 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 10 permit 192.168.40.4/30 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 11 permit 192.168.40.12/30 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 12 permit 172.16.100.0/24 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 13 permit 172.9.0.0/16 ip
prefix-list CESSNA_SnS_VN_ROUTES seq 14 permit 172.40.0.0/16
ip prefix-list
CESSNA_SnS_VN_ROUTES seq
15 permit 192.168.40.16/30
!
ip prefix-list
Lighting_VN_ROUTES seq 5
permit 192.168.20.8/30
ip prefix-list
Lighting_VN_ROUTES seq 6
permit 192.168.20.20/30
ip prefix-list
Lighting_VN_ROUTES seq 7
permit 172.20.20.0/24
ip prefix-list
Lighting_VN_ROUTES seq 9
permit 172.17.100.0/24
ip prefix-list
Lighting_VN_ROUTES seq 10 permit 192.168.40.0/30
ip prefix-list
Lighting_VN_ROUTES seq 11 permit 192.168.40.16/30
ip prefix-list
Lighting_VN_ROUTES seq 12 permit 192.168.40.20/30
!
ip prefix-list
SHARED_SERVICES_NETS seq
1 permit 10.10.100.0/24
ip prefix-list
SHARED_SERVICES_NETS seq
2 permit 10.30.200.0/30
ip prefix-list
SHARED_SERVICES_NETS seq
3 permit 10.30.201.0/30
ip prefix-list
SHARED_SERVICES_NETS seq
4 permit 10.40.100.0/24
ip prefix-list
SHARED_SERVICES_NETS seq
5 permit 0.0.0.0/0
ip prefix-list
SHARED_SERVICES_NETS seq
6 permit 192.168.200.0/24
ip radius source-interface Loopback0

!
ip access-list
extended ACL_WEBAUTH_REDIRECT
deny
ip any
host 10.10.100.52
permit tcp any any eq www
```

```
permit tcp any any eq 443
permit tcp any any eq 8443
deny
udp any any eq domain
deny
udp any eq bootpc any eq bootps
logging trap critical
logging host 10.10.100.50
ip access-list
standard 1
deny
10.10.100.0 0.0.0.255
deny
10.30.200.0 0.0.0.255
deny
10.30.201.0 0.0.0.255
 permit any
ipv6 route 2001:DB8:16:107::/64 2001:DB8:16:109::2 ipv6
route 2001:DB8:BABA:FACE::/64 2001:DB8:16:109::2 ipv6 route
2001:DB8:DABA:FACE::/64 2001:DB8:16:109::2 ipv6 route
2001:BEED::/64 2001:DB8:16:109::2 !
route-map Lighting-VN-TO-GLOBAL permit 10
 match ip address prefix-list Lighting_VN_ROUTES
!
route-map SS-NETWORK-TO-VRF permit 10
 match ip address prefix-list SHARED_SERVICES_NETS
!
route-map DMZ-TO-LIGHTING-VRF permit 10
 match ip address prefix-list LIGHTING_HER_NETS
!
route-map SnS-VN-TO-GLOBAL permit 10
 match ip address prefix-list CESSNA_SnS_VN_ROUTES
!
snmp-server group cisco v3 priv
snmp-server group default v3 priv snmp-server group default v3 auth context vlan- match prefix
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None snmp-server view SNMPv3All iso
included snmp-server view SNMPv3None iso excluded

snmp-server community CiscoDNA RW
snmp-server system-shutdown
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit snmp-server enable traps ospf
cisco-specific lsa snmp-server enable traps rep snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cpu threshold
snmp-server enable traps memory bufferpeak
snmp-server enable traps stackwise
snmp-server enable traps udld link-fail-rpt
```

```
snmp-server enable traps udld status-change
snmp-server enable traps fru-ctrl snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps energywise snmp-server enable traps power-ethernet police
snmp-server enable traps entity
snmp-server enable traps pw vc
snmp-server enable traps envmon
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps ipsla
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached
scheduled-test-fail
snmp-server enable traps bfd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps local-auth
snmp-server enable traps lisp
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps mvpn
snmp-server enable traps isis
snmp-server enable traps bgp
snmp-server enable traps bgp cbgp2
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server enable traps rf snmp-server enable traps transceiver all
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps mpls vpn snmp-server enable traps mpls rfc vpn
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 10.10.100.50 version 2c ciscosnmp
snmp-server host 10.10.100.51 version 2c ciscosnmp
snmp ifmib ifindex persist
!
```

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
radius server Cisco DNA Center-radius_10.10.100.52
 address ipv4 10.10.100.52 auth-port 1812 acct-port
 1813 timeout 4
 retransmit 3
 pac key 7 013047175804575D72
!
!
control-plane
 service-policy input system-cpp-policy
!
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 authorization exec VTY_author
 login authentication VTY_authen
 transport preferred ssh
 transport input all
line vty 5 15
 authorization exec VTY_author
 login authentication VTY_authen
 transport preferred ssh
 transport input all
!
ntp source Loopback0
ntp master 3
ntp server 10.10.100.1
!
end
```

HER Configuration

The HER configuration example for Cisco Smart Street Lighting Solution with CR-Mesh access network is given below:

```
version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname CITY-CSR1K-HER2
!
boot-start-marker
boot-end-marker
!
enable password xxxx
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local aaa
```

```
authorization network default local
!
aaa session-id common
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-
 licensing@cisco.com profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip host rsaca.iot.cisco.com 172.16.102.2
ip domain name iot.cisco.com
!
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-
 1919074303 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-
 1919074303 revocation-check none
 rsakeypair TP-self-signed-1919074303
!

crypto pki trustpoint SLA-
 TrustPoint enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint
 LDevID enrollment retry
 count 10 enrollment retry
 period 2 enrollment mode
 ra enrollment profile
 LDevID serial-number
 ip-address
 none password
 fingerprint D
 revocation-check none
 rsakeypair LDevID
!
crypto pki profile enrollment LDevID
 enrollment urlhttp://rsaca.iot.cisco.com/certsrv/mscep/mscep.dll
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = iot-rsa-root-ca
!
license udi pid CSR1000V sn 9WR6ZS2AXIX
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
username cg-nms-administrator privilege 15 secret 8
$8$o6itw59cNq6EuE$s41QkYLlmBR0DBp3y8zpaBc2mUYHul618Y4RIAGuiRM
!
redundancy
! ** Setting up prefix-list. **
crypto ikev2 authorization policy default
```

```
 route set interface
 route set access-list NET-list
 route set access-list ipv6 NETipv6-list
!  ** Setting up prefix-list. **
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route route set
 access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!**IKEv2 proposal **
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_Cert
 encryption aes-cbc-256
 integrity sha256
 group 14
!**IKEv2 Policy **
crypto ikev2 policy FlexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
crypto ikev2 policy FlexVPN_IKEv2_Policy_Cert
 proposal FlexVPN_IKEv2_Proposal_Cert
!
crypto ikev2 keyring mykeys
 peer CIMCONRouter
  address x.x.x.x
  pre-shared-key CiscoCSR123
 !
crypto ikev2 keyring FlexVPN_IKEv2_Keyring
 peer all
  address 0.0.0.0 0.0.0.0
  identity fqdn spoke-flexVPN
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
 !
! **Pre shared key based ikev2 profile **
crypto ikev2 profile FlexVPN_IKEv2_Profile1
 match identity remote address x.x.x.x 255.255.255.255 << Public IP Address
 match identity remote fqdn CSR.cimcon.com
 identity local fqdn CSR.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local mykeys
aaa authorization group psk list mylist default

! ** Certificate based ikev2 profile **
crypto ikev2 profile FlexVPN_IKEv2_Profile_Cert
 match identity remote fqdn spoke-4-flexVPN
 match identity remote fqdn spoke-5-flexVPN
 match identity remote fqdn spoke-6-flexVPN
 match identity remote fqdn spoke-7-flexVPN
 match certificate FlexVPN_Cert_Map
 identity local fqdn hub-flexVPN
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 dpd 30 3 periodic
 aaa authorization group cert list
 FlexVPN_Author FlexVPN_Author_Policy virtual-template 1
!
cdp run
!
crypto ipsec security-association replay disable
!**IPSec Transform Set **
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha-hmac mode transport
```

```
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_Cert esp-aes esp-sha-hmac mode transport
!
!**IPSEC Profile **
crypto ipsec profile FlexVPN_IPsec_Profile1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile1
!
crypto ipsec profile FlexVPN_IPsec_Profile_Cert
 set transform-set FlexVPN_IPsec_Transform_Set_Cert
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile_Cert
 responder-only
!
interface Loopback110
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback180
 ip address 192.168.180.2 255.255.255.0
 ipv6 address 2001:DB8:DABA:FACE::2/64
 ipv6 enable
!
interface Tunnel110
 ip unnumbered Loopback110
 ipv6 address 2001:DB:12::2/64
 ipv6 enable
 ipv6 eigrp 1
 tunnel source GigabitEthernet7
 tunnel destination <CIMCON LG cloudservice router's public
 IP> tunnel protection ipsec profile FlexVPN_IPsec_Profile1
!
interface GigabitEthernet1
 description connected to N5K for FAR Access
 ip address 10.20.100.102 255.255.255.0
 standby version 2
 standby 1 ip 10.20.100.31
 standby 1 preempt
 negotiation auto
 ipv6 enable
 no mop enabled
 no mop sysid

!
interface GigabitEthernet2
 description connected from HER2 to RSA CA
 ip address 172.16.102.102 255.255.255.0
 standby version 2
 standby 3 ip 172.16.102.1
 standby 3 preempt
 negotiation auto
 no mop enabled
 no mop sysid
!
!
interface GigabitEthernet4
 description connected to DMZ from CITY-CSR1K-HER2
 no ip address
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet5
 description connected to Headend network and ECC CA Server
```

```
 ip address 172.16.106.102 255.255.255.0 standby version 2
 standby 4 ip 172.16.106.1
 standby 4 preempt
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet6
 ip address 10.x.x.x 255.255.255.0
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet7
 ip address x.x.x.x 255.255.255.0 <<Public IP Address
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet8
description connected to Headend FND network
 ip address 172.16.107.102 255.255.255.0
 standby version 2
 standby 7 ip 172.16.107.1
 standby 7 preempt
 negotiation auto
 ipv6 address 2001:DB8:16:107::1/64
 ipv6 enable
 no mop enabled
 no mop sysid
!
interface GigabitEthernet9
 description connected from HER2 to CPNR
 ip address 172.16.108.102 255.255.255.0
 standby version 2
 standby 8 ip 172.16.108.1
 standby 8 preempt
 negotiation auto
 ipv6 address 2001:DB8:16:108::1/64
 ipv6 enable
 no mop enabled
 no mop sysid
!

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback180
 ipv6 enable
 ipv6 eigrp 1
 tunnel protection ipsec profile FlexVPN_IPsec_Profile_Cert
!
!
router eigrp 11
 network 192.168.150.0
 redistribute static
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip ssh time-out 30
ip ssh version 2
!
!
```

```
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit 172.16.103.0 0.0.0.255
 permit 172.16.102.0 0.0.0.255
 permit 172.16.107.0 0.0.0.255
 permit 172.16.106.0 0.0.0.255
ip access-list standard NET-list
 permit 10.x.1.0 0.0.0.255
 permit 172.16.0.0 0.0.255.255

ipv6 route 2001:BEED::10/128
2001:DB8:16:107:9966:9E00:CE20:2D4F ipv6 router eigrp 1
 eigrp router-id 7.7.7.7
 redistribute static metric 4290000000 0 255 255 65535
!
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 sequence 50 permit ipv6 2001:DB:12::/64 any
 permit ipv6 2001:DB8:16:107::/64 any
 permit ipv6 host 2001:FEED:BEEF::2 any
 permit ipv6 2600:1F16:C81:9B0B::/64 any
 permit ipv6 2001:DB8:16:108::/64 any
 permit ipv6 2001:FAF:FACE:CAF::/64 any
!
ipv6 access-list NETipv6-list
 sequence 20 permit ipv6 2001:BEED::/48 any
 permit ipv6 host 2001:DB:12::2 any
 permit ipv6 2001:DB8:16:103::/64 any
 permit ipv6 2001:DB8:16:107::/64 any
 permit ipv6 2001:DB8:16:108::/64 any
 permit ipv6 2001:FAF:FACE:CAF::/64 any
!
control-plane
!
line con 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 transport preferred ssh
line vty 5 15
 exec-timeout 0
 password cisco
 logging synchronous
!
ntp master
ntp server 10.64.58.51
netconf max-sessions 16
netconf ssh
end
```

FiaB Switch Stack Configuration

The configuration example of a Cisco Catalyst 9300 switch stack (FiaB) in a PoP site provisioned in the CCI network is given below:

```
  version 16.11
  no service pad
  service timestamps debug datetime msec
  service timestamps log datetime msec
  service password-encryption
  ! Call-home is enabled by Smart-
  Licensing. service call-home
```

```
 no platform punt-keepalive disable-kernel-core
!
 hostname C9300-20-STACK
!
!
 vrf definition
  Lighting_VN rd 1:4099
  !
 address-family ipv4 route-
  target export 1:4099
  route-target import
  1:4099
 exit-address-family
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition
 SnS_VN rd 1:4100
 !
 address-family ipv4 route-
  target export 1:4100
  route-target import
  1:4100
 exit-address-family
!
enable secret 9 <Shared_Secret>
enable password 7
<Enable_Sceret>
!
aaa new-model
!
!
aaa group server radius Cisco DNA Center-client-radius-
 group server name Cisco DNA Center-radius_10.10.100.52
 ip radius source-interface Loopback0
!
aaa group server radius Cisco DNA Center-network-radius-
 group server name Cisco DNA Center-radius_10.10.100.52
 ip radius source-interface Loopback0
!
aaa authentication login default local
aaa authentication login VTY_authen group Cisco DNA Center-network-radius-group
local aaa authentication dot1x default group Cisco DNA Center-client-radius-group
aaa authorization exec default local
aaa authorization exec VTY_author group Cisco DNA Center-network-radius-group
local aaa authorization network default group Cisco DNA Center-client-radius-group
aaa authorization network Cisco DNA Center-cts-list group Cisco DNA Center-client-radius-
group aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group Cisco DNA Center-client-radius-group aaa
accounting exec default start-stop group Cisco DNA Center-network-radius-group
!
aaa server radius dynamic-author
 client 10.10.100.52 server-key 7 <Server_Key>
!
aaa session-id common
switch 1 provision c9300-24ux
switch 2 provision c9300-24ux
!
call-home
```

```
  ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
  ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
  contact-email-addr sch-smart-
  licensing@cisco.com profile "CiscoTAC-1"
   active
   destination transport-method http
   no destination transport-method
 email ip routing
 !
 ip name-server 10.10.100.10
 ip domain name ccibgl.cisco.com
 ip dhcp relay information option
 !
 ip dhcp snooping vlan 1021-1024
 ip dhcp snooping
 login on-success log
 !
 device-sensor filter-list lldp list
  iseLLDP tlv name system-name
  tlv name system-description
  tlv name system-capabilities
 !
 device-sensor filter-list dhcp list
  iseDHCP option name host-name
  option name parameter-request-
  list option name class-identifier
 !
 device-sensor filter-list cdp list
  iseCDP tlv name device-name
 tlv name capabilities-type tlv name version-type
 tlv name platform-type
device-sensor filter-spec dhcp include list
iseDHCP device-sensor filter-spec lldp include
list iseLLDP device-sensor filter-spec cdp include
list iseCDP device-sensor notify all-changes
mpls label mode all-vrfs protocol all-afs per-
vrf no device-tracking logging theft device-
tracking tracking
!
device-tracking policy IPDT_MAX_10
 limit address-count 10
 no protocol udp
 tracking enable
!
access-session attributes filter-list list Def_Acct_List
 cdp
 lldp
 dhcp
 http
access-session accounting attributes filter-spec include list Def_Acct_List
access-session interface-template sticky
access-session acl default passthrough
!
table-map policed-dscp
 map from 0 to 8
 map from10 to 8
 map from18 to 8
 map from 24 to 8
 map from 34 to 8
 map from46 to 8
 default copy
table-map AutoConf-4.0-Trust-Cos-Table
```

```
 default copy
table-map AutoConf-4.0-Trust-Dscp-Table
 default copy
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint TP-self-signed-4270476506
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4270476506
 revocation-check none
 rsakeypair TP-self-signed-4270476506
!
crypto pki trustpoint Cisco DNA Center-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  <Snipped>
  quit

crypto pki certificate chain TP-self-signed-4270476506
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  <Snipped>
  quit

crypto pki certificate chain Cisco DNA Center-CA
 certificate ca 00E0F446909D34DA93
  30820397 3082027F A0030201 02020900 E0F44690 9D34DA93 300D0609 2A864886
  <Snipped>
  quit
!
cts authorization list Cisco DNA Center-cts-list
system mtu 9100
license boot level network-advantage addon dna-advantage
device classifier
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 141119
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
 linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 sgt 3999
 vlan 2047
service-template DefaultCriticalVoice_SRV_TEMPLATE
 voice vlan
service-template DefaultCriticalAccess_SRV_TEMPLATE
 access-group IPV4_CRITICAL_AUTH_ACL
 access-group IPV6_CRITICAL_AUTH_ACL
```

```
dot1x system-auth-control
dot1x critical eapol
!
!
username dna privilege 15 password 7 <DNA_Password>
!
redundancy
 mode sso
!
transceiver type all
 monitoring
!

vlan 1021
 name 172_20_20_0-Lighting_VN
!
vlan 1022
 name 192_100_20_0-INFRA_VN
!
vlan 1023
 name 172_10_20_0-SnS_VN
!
vlan 1024
 name 172_9_0_0-SnS_VN
!
vlan 2045
 name AP_VLAN
!
vlan 2046
 name VOICE_VLAN
!
vlan 2047
 name CRITICAL_VLAN
!
vlan 3007
 name 3007
!
vlan 3008
 name 3008
!
vlan 3009
 name 3009
!
vlan 3010
 name 3010
!
vlan 3011
 name 3011
!
vlan 3012
 name 3012
!
parameter-map type subscriber attribute-to-service BUILTIN_DEVICE_TO_TEMPLATE
 10 map device-type regex "Cisco-IP-Phone"
  20 interface-template IP_PHONE_INTERFACE_TEMPLATE 20
 map device-type regex "Cisco-IP-Camera"
  20 interface-template IP_CAMERA_INTERFACE_TEMPLATE
 30 map device-type regex "Cisco-DMP"
  20 interface-template DMP_INTERFACE_TEMPLATE 40
 map oui eq "00.0f.44"
  20 interface-template DMP_INTERFACE_TEMPLATE 50
 map oui eq "00.23.ac"
  20 interface-template DMP_INTERFACE_TEMPLATE 60
```

```
 map device-type regex "Cisco-AIR-AP"
  20 interface-template AP_INTERFACE_TEMPLATE 70
 map device-type regex "Cisco-AIR-LAP"
  20 interface-template LAP_INTERFACE_TEMPLATE 80
 map device-type regex "Cisco-TelePresence"
  20 interface-template TP_INTERFACE_TEMPLATE 90
 map device-type regex "Surveillance-Camera"
  10 interface-template MSP_CAMERA_INTERFACE_TEMPLATE
 100 map device-type regex "Video-Conference"
  10 interface-template MSP_VC_INTERFACE_TEMPLATE
 110 map device-type regex "Cisco-CAT-LAP"
  10 interface-template LAP_INTERFACE_TEMPLATE
 150 map device-type regex "CDB*"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
 160 map device-type regex "WS-C3560CX*"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
 170 map device-type regex "IE-400*"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
 180 map device-type regex "IE-401*"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
 190 map device-type regex "IE-500*"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
 200 map device-type regex "Cisco-Switch"
  10 interface-template SWITCH_INTERFACE_TEMPLATE
!
!
lldp run
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AUTHC_SUCCESS-AUTHZ_FAIL
 match authorization-status unauthorized
  match result-type success
!
class-map type control subscriber
 match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all
 DOT1X_MEDIUM_PRIO match authorizing-method-priority gt 20
!
class-map type control subscriber match-all
 DOT1X_NO_RESP match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all
 DOT1X_TIMEOUT match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber
 match-any IN_CRITICAL_AUTH
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
```

```
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all
 MAB_FAILED match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH match
 activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE match
 activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
!
class-map match-any system-cpp-police-ewlc-control
 description EWLC Control
class-map match-any system-cpp-police-topology-control
 description Topology control
class-map match-any system-cpp-police-sw-forward
 description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic


       class-map match-any AutoConf-4.0-Transaction-Class
        match access-group name AutoConf-4.0-Acl-Transactional-Data
       class-map match-any AutoConf-4.0-Output-Trans-Data-Queue
       match dscp af21  af22  af23
       match cos  2
       class-map match-any AutoConf-4.0-Default-Class
        match access-group name AutoConf-4.0-Acl-Default
       class-map match-any system-cpp-default
        description EWLC Data, Inter FED Traffic
       class-map match-any system-cpp-police-sys-data

 description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed


       class-map match-any AutoConf-4.0-Output-Scavenger-Queue
       match dscp cs1
       class-map match-any AutoConf-4.0-Output-Control-Mgmt-Queue
       match dscp cs2  cs3  cs6  cs7
       match cos  3
       class-map match-any AutoConf-4.0-Scavanger-Class
        match access-group name AutoConf-4.0-Acl-Scavanger
       class-map match-any AutoConf-4.0-Signaling-Class
        match access-group name AutoConf-4.0-Acl-Signaling
       class-map match-any system-cpp-police-punt-webauth
        description Punt Webauth
       class-map match-any system-cpp-police-l2lvx-control
        description L2 LVX control packets
       class-map match-any system-cpp-police-forus
         description Forus Address resolution and Forus traffic

class-map match-any DNA-EZQOS_2P6Q3T_9K#BULK-DATA
 match dscp cs1
 match dscp af12
 match dscp af13
 match dscp af11
class-map match-any system-cpp-police-multicast-end-station
 description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
```

```
 description High Rate Applications
class-map match-any AutoConf-4.0-Voip-Video-CiscoPhone-Class match
 cos 4
class-map match-any system-cpp-police-multicast
 description MCAST Data
class-map match-any DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE match
 dscp cs3
 match dscp cs2
 match dscp cs7
 match dscp cs6
class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING match
 dscp af43
 match dscp af41
 match dscp af42
class-map match-any system-cpp-police-l2-control
 description L2 control
class-map match-any system-cpp-police-dot1x-auth
 description DOT1X Auth
class-map match-any AutoConf-4.0-Output-Multimedia-ConfQueue match
 dscp af41 af42 af43
 match cos 4
class-map match-any system-cpp-police-data
 description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
 match dscp cs5
 match dscp cs4
class-map match-any DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
 match dscp ef
class-map match-any system-cpp-police-stackwise-virt-control
 description Stackwise Virtual OOB
class-map match-any AutoConf-4.0-Output-Multimedia-StrmQueue match
 dscp af31 af32 af33
class-map match-any AutoConf-4.0-Voip-Data-CiscoPhone-Class match
 cos 5
class-map match-any AutoConf-4.0-Voip-SignalClass
 match dscp cs3
 match cos3
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
 description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
 description Protocol snooping
class-map match-any AutoConf-4.0-Output-Bulk-Data-Queue match
 dscp af11 af12 af13
 match cos 1
class-map match-any AutoConf-4.0-Multimedia-Conf-Class match access-
 group name AutoConf-4.0-Acl-MultiEnhanced-Conf
class-map match-any system-cpp-police-dhcp-snooping
 description DHCP snooping
class-map match-any AutoConf-4.0-Bulk-Data-Class
 match access-group name AutoConf-4.0-Acl-Bulk-Data
class-map match-any system-cpp-police-ios-routing
 description L2 control, Topology control, Routing control, Low Latency class-map match-any
DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
 match dscp af23
 match dscp af21
 match dscp af22
class-map match-any system-cpp-police-system-critical
 description System Critical and Gold Pkt
class-map match-any AutoConf-4.0-VoipSignal-CiscoPhone-
 Class match cos 3
class-map match-any system-cpp-police-ios-feature
  description
ICMPGEN,BROADCAST,ICMP,L2LVXCntrl,ProtoSnoop,PuntWebauth,MCASTData,Transit,DOT1XAuth,Swfwd,LOGGING,
```

```
L2LVXData,ForusTraffic,ForusARP,McastEndStn,Openflow,Exception,EGRExcption,NflSampled,RpfFailed
class-map match-any DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
 match dscp af32
 match dscp af33
 match dscp af31
class-map match-any AutoConf-4.0-Output-Priority-Queue
 match dscp cs4cs5ef
 match cos5
class-map match-any AutoConf-4.0-Voip-Data-Class
match dscp ef
match cos5
!
!
policy-map type control subscriber
 PMAP_DefaultWiredDot1xClosedAuth_1X_MAB event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority
 10 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-
  failure 10 pause reauthentication
  20 authorize
 30 class DOT1X_NO_RESP do-until-
  failure 10 terminate dot1x
  20 authenticate using mab priority 20
 40 class MAB_FAILED do-until-
  failure 10 terminate mab
  20 authentication-restart
 60 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event aaa-available match-all
 10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-
  failure 10 clear-session
 20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
  10 resume reauthentication
event agent-found match-all
 10 class always do-until-failure 10 terminate mab
 20 authenticate using dot1x retries 2 retry-time 0 priority 10
event inactivity-timeout match-all
 10 class always do-until-failure 10 clear-session
event authentication-success match-all
event violation match-all
 10 class always do-until-failure
  10 restrict
event authorization-failure match-all

class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure 10 authentication-restart 60

!
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
event authentication-failure match-first
```

```
 5 class DOT1X_FAILED do-until-failure
 10 terminate dot1x
 20 authentication-restart 60
10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
 10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
 30 authorize
 40 pause reauthentication
20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
 10 pause reauthentication
 20 authorize
30 class MAB_FAILED do-until-failure
 10 terminate mab
 20 authenticate using dot1x retries 2 retry-time 0 priority 10
40 class DOT1X_NO_RESP do-until-failure
 10 terminate dot1x
 20 authentication-restart 60
60 class always do-until-failure
 10 terminate mab
 20 terminate dot1x
 30 authentication-restart 60
event aaa-available match-all
10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
 10 clear-session
20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
 10 resume reauthentication
event agent-found match-all
10 class always do-until-failure
 10 terminate mab
 20 authenticate using dot1x retries 2 retry-time 0 priority 10
event inactivity-timeout match-all
 10 class always do-until-failure 10 clear-session
event authentication-success match-all
event violation match-all
 10 class always do-until-failure 10 restrict
event authorization-failure match-all
 10class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
  10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
event authentication-failure match-first
 5class DOT1X_FAILED do-until-failure 10
  terminate dot1x
  20 authenticate using mab priority 20
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
  20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
  25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
  30 authorize
  40 pause reauthentication
 20 class AAA_SVR_DOWN_AUTHD_HOST do-until-
  failure 10 pause reauthentication
  20 authorize
30 class DOT1X_NO_RESP do-until-
 failure 10 terminate dot1x
 20 authenticate using mab priority 20
40 class MAB_FAILED do-until-failure
 10 terminate mab
 20 authentication-restart 60
60 class always do-until-failure
 10 terminate dot1x
 20 terminate mab
```

```
 30 authentication-restart 60
event aaa-available match-all
 10 class IN_CRITICAL_AUTH do-until-failure
  10 clear-session
 20 class NOT_IN_CRITICAL_AUTH do-until-failure 10 resume reauthentication
event agent-found match-all
 10 class always do-until-failure
  10 terminate mab
 20 authenticate using dot1x retries 2 retry-time 0 priority 10
event inactivity-timeout match-all
 10 class always do-until-failure 10 clear-session
  10 event authentication-success match-all
event violation match-all
 10 class always do-until-failure
 10 restrict
event authorization-failure match-all
 10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
 10 authentication-restart 60
!
policy-map type control subscriber
 PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X event session-started match-all
 10 class always do-until-failure
  10 authenticate using mab priority 20
event authentication-failure match-first
 5 class DOT1X_FAILED do-until-failure
 10 terminate dot1x
 20 authentication-restart 60
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
  20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
  25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
  30 authorize
  40 pause reauthentication
 20 class AAA_SVR_DOWN_AUTHD_HOST do-until-
  failure 10 pause reauthentication
  20 authorize
 30 class MAB_FAILED do-until-
  failure 10 terminate mab
  20 authenticate using dot1x retries 2 retry-time 0 priority 10
 40 class DOT1X_NO_RESP do-until-
 failure 10 terminate dot1x
 20 authentication-restart 60
60 class always do-until-failure
 10 terminate mab
 20 terminate dot1x
 30 authentication-restart 60
event aaa-available match-all
 10 class IN_CRITICAL_AUTH do-until-failure
  10 clear-session
 20 class NOT_IN_CRITICAL_AUTH do-until-
  failure resume reauthentication
event agent-found match-all
 10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x retries 2 retry-time 0 priority 10
event inactivity-timeout match-all
 10 class always do-until-failure
  10 clear-session
event authentication-success match-all
event violation match-all
 10 class always do-until-failure
  10 restrict
event authorization-failure match-all
```

```
 10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
  10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_MAB_1X
 event session-started match-all
 10 class always do-until-failure
  10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-
   failure 10 pause reauthentication
   20 authorize
```

```
  30 class MAB_FAILED do-until-
   failure 10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-
   failure 10 terminate dot1x
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-
   failure 10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-
   failure 10 authentication-restart 60
!
policy-map AutoConf-4.0-Trust-Cos-Input-Policy
 class class-default
  set cos cos table AutoConf-4.0-Trust-Cos-Table
policy-map AutoConf-4.0-Output-Policy
 class AutoConf-4.0-Output-Priority-Queue
  priority level 1 percent 30
 class AutoConf-4.0-Output-Control-Mgmt-Queue
  bandwidth remaining percent 10
  queue-limit dscp cs2 percent 80
  queue-limit dscp cs3 percent 90
  queue-limit dscp cs6 percent 100
  queue-limit dscp cs7 percent 100
  queue-buffers ratio 10
 class AutoConf-4.0-Output-Multimedia-ConfQueue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class AutoConf-4.0-Output-Trans-Data-Queue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class AutoConf-4.0-Output-Bulk-Data-Queue
  bandwidth remaining percent 4
  queue-buffers ratio 10
 class AutoConf-4.0-Output-Scavenger-Queue
  bandwidth remaining percent 1
  queue-buffers ratio 10
 class AutoConf-4.0-Output-Multimedia-StrmQueue
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
policy-map AutoConf-4.0-CiscoSoftPhone-Input-Policy
 class AutoConf-4.0-Voip-Data-Class
```

```
  set dscp ef
   police cir 128000 bc 8000
    conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoConf-4.0-Voip-SignalClass
 set dscp cs3
 police cir 32000 bc 8000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoConf-4.0-Multimedia-Conf-Class
 set dscp af41
 police cir 5000000
  conform-action transmit
  exceed-action drop
class AutoConf-4.0-Bulk-Data-Class
 set dscp af11
 police cir 10000000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoConf-4.0-Transaction-Class
 set dscp af21
 police cir 10000000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
class AutoConf-4.0-Scavanger-Class
 set dscp cs1
 police cir 10000000
  conform-action transmit
  exceed-action drop
class AutoConf-4.0-Signaling-Class
 set dscp cs3
 police cir 32000 bc 8000
  conform-action transmit
  exceed-action drop
class AutoConf-4.0-Default-Class
 set dscp default
 police cir 10000000
  conform-action transmit
  exceed-action set-dscp-transmit dscp table policed-dscp
policy-map system-cpp-policy
policy-map DNA-dscp#APIC_QOS_Q_OUT
 class DNA-EZQOS_2P6Q3T_9K#VOICE-PQ1
  priority level 1
  police rate percent 2
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#VIDEO-PQ2
  priority level 2
  police rate percent 26
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#CONTROL-PLANE
  bandwidth remaining percent 21
  queue-buffers ratio 5
 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-CONFERENCING
  bandwidth remaining percent 1
  queue-buffers ratio 10
  queue-limit dscp af41 percent 100
  queue-limit dscp af42 percent 90
  queue-limit dscp af43 percent 80
 class DNA-EZQOS_2P6Q3T_9K#MULTIMEDIA-STREAMING
  bandwidth remaining percent 1
  queue-buffers ratio 10
  queue-limit dscp af32 percent 90
  queue-limit dscp af33 percent 80
 class DNA-EZQOS_2P6Q3T_9K#TRANSACTIONAL-DATA
  bandwidth remaining percent 42
```

```
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 18 percent 80 100
  random-detect dscp 20 percent 70 100
  random-detect dscp 22 percent 60 100
 class DNA-EZQOS_2P6Q3T_9K#BULK-DATA
  bandwidth remaining percent 8
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 60 100
  random-detect dscp 10 percent 80 100
  random-detect dscp 12 percent 70 100
  random-detect dscp 14 percent 60 100
 class class-default
  bandwidth remaining percent 27
  queue-buffers ratio 25
  random-detect dscp-based
  random-detect dscp 0 percent 80 100
policy-map AutoConf-4.0-Trust-Dscp-Input-Policy
 class class-default
  set dscp dscp table AutoConf-4.0-Trust-Dscp-Table
policy-map AutoConf-4.0-CiscoPhone-Input-Policy
 class AutoConf-4.0-Voip-Data-CiscoPhone-Class
  set dscp ef
  police cir 128000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-
 dscp class AutoConf-4.0-Voip-Video-CiscoPhone-Class
  set dscp af41
  police cir 10000000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-
  dscp class AutoConf-4.0-VoipSignal-CiscoPhone-Class
   set dscp cs3
   police cir 32000 bc 8000
    conform-action transmit
    exceed-action set-dscp-transmit dscp table policed-
  dscp class AutoConf-4.0-Default-Class
   set dscp default
policy-map port_child_policy
 class non-client-nrt-class
  bandwidth remaining ratio 10
!
autoconf enable
!
template ApAutzTemplate
 switchport access vlan 2045
 switchport mode access
 access-session interface-template sticky timer 10
!
template DefaultWiredDot1xClosedAuth
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server service-policy type control
 subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
!
template DefaultWiredDot1xLowImpactAuth
```

```
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server service-policy type control subscriber
 PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
!
template DefaultWiredDot1xOpenAuth
 dot1x pae authenticator
 switchport access vlan 2047
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server service-policy type control
 subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
!
template SWITCH_INTERFACE_TEMPLATE
 switchport mode trunk
!
interface Loopback0
 ip address 192.0.20.11 255.255.255.255
!
 interface Port-channel1
  switchport mode trunk
!
 interface Port-channel2
  switchport mode trunk
!
 interface Port-channel3
  switchport mode trunk
!
 interface Port-channel4
  switchport mode trunk
!
 interface Port-channel5
  switchport mode trunk
!
interface LISP0
!
interface LISP0.4097
!
interface LISP0.4099
!
interface LISP0.4100
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed 1000
 negotiation auto
!
interface TenGigabitEthernet1/0/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/2
 switchport mode access
 device-tracking attach-policy IPDT_MAX_10 access-
 session inherit disable interface-template-sticky
```

```
 access-session inherit disable autoconf no macro auto
 processing
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/3
 switchport mode access
 device-tracking attach-policy IPDT_MAX_10 access-
 session inherit disable interface-template-sticky
 access-session inherit disable autoconf no macro auto
 processing
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DefaultWiredDot1xClosedAuth
 spanning-tree portfast
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/4
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/5
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/6
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/7
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/8
 switchport mode trunk
 channel-group 5 mode on
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/9
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/10
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/11
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/12
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/13
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/14
 device-tracking attach-policy IPDT_MAX_10
```

```
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/15
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/16
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/17
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/18
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/19
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/20
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/21
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/22
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/23
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/0/24
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet1/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet1/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet1/1/3
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet1/1/4
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/1
 description Connected to Transit Site C9500-30-CP1 port Te1/0/3
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/2
 device-tracking attach-policy IPDT_MAX_10
```

```
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/3
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/4
 switchport mode trunk
 channel-group 2 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/5
 switchport mode trunk
 channel-group 3 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/6
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/7
 switchport mode trunk
 channel-group 4 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet1/1/8
 switchport mode trunk
 channel-group 1 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet1/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet1/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TwentyFiveGigE1/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TwentyFiveGigE1/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface AppGigabitEthernet1/0/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/3
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/4
```

```
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/5
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/6
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/7
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/8
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/9
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/10
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/11
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/12
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/13
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/14
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/15
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/16
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/17
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/18
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/19
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/20
 device-tracking attach-policy IPDT_MAX_10
```

```
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/21
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/22
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/23
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/0/24
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet2/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet2/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet2/1/3
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface GigabitEthernet2/1/4
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/1
 description Connected to Transit Site C9500-30-CP2 port TeGig2/0/3
 switchport mode trunk
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/3
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/4
 switchport mode trunk
 channel-group 2 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/5
 switchport mode trunk
 channel-group 3 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/6
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/7
 switchport mode trunk
```

```
 channel-group 4 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TenGigabitEthernet2/1/8
 switchport mode trunk
 channel-group 1 mode desirable
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet2/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface FortyGigabitEthernet2/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TwentyFiveGigE2/1/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface TwentyFiveGigE2/1/2
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface AppGigabitEthernet2/0/1
 device-tracking attach-policy IPDT_MAX_10
 service-policy output DNA-dscp#APIC_QOS_Q_OUT
!
interface Vlan1
 no ip address
!
interface Vlan200
 ip address 20.20.20.2 255.255.255.252
!
interface Vlan201
 ip address 20.20.21.2 255.255.255.252
!
interface Vlan1021
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45c
 vrf forwarding Lighting_VN
 ip address 172.20.20.1 255.255.255.0
 ip helper-address 10.10.100.10
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 172_20_20_0-Lighting_VN-IPV4
!
interface Vlan1022
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45d
 ip address 192.100.20.1 255.255.255.0
 ip helper-address 10.10.100.10
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_100_20_0-INFRA_VN-IPV4
!
interface Vlan1023
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45e
 vrf forwarding SnS_VN
 ip address 172.10.20.1 255.255.255.0
 ip helper-address 10.10.100.10
 no ip redirects
```

```
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 172_10_20_0-SnS_VN-IPV4
!
interface Vlan1024
 description Configured from Cisco DNA-Center
 mac-address 0000.0c9f.f45f
 vrf forwarding SnS_VN
 ip address 172.9.0.1 255.255.0.0
 ip helper-address 10.10.100.10
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 172_9_0_0-SnS_VN-IPV4
!
interface Vlan3007
 description vrf interface to External router
 vrf forwarding SnS_VN
 ip address 192.168.20.1 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3008
 description vrf interface to External router
 ip address 192.168.20.5 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3009
 description vrf interface to External router
 vrf forwarding Lighting_VN
 ip address 192.168.20.9 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3010
 description vrf interface to External router
 ip address 192.168.20.13 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3011
 description vrf interface to External router
 vrf forwarding SnS_VN
 ip address 192.168.20.17 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
interface Vlan3012
 description vrf interface to External router
 vrf forwarding Lighting_VN
 ip address 192.168.20.21 255.255.255.252
 no ip redirects
 ip route-cache same-interface
!
!
router eigrp 1000
 network 20.20.20.0 0.0.0.3
 network 20.20.20.4 0.0.0.3
 network 20.20.21.0 0.0.0.3
 network 192.0.20.11 0.0.0.0
 eigrp router-id 192.0.20.11
!
```

```
router lisp
 locator-table default
 locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
  IPv4-interface Loopback0 priority 10 weight 10 auto-
  discover-rlocs
  exit-locator-set
!
service ipv4
 encapsulation vxlan
 itr map-resolver 192.0.20.11
 etr map-server 192.0.20.11 key 7 094E1F0C1C5C15
 etr map-server 192.0.20.11 proxy-reply
 etr
 sgt
 no map-cache away-eids send-map-request
 proxy-etr
 proxy-itr 192.0.20.11
 map-server
 map-resolver
 exit-service-ipv4
!
service ethernet
 database-mapping limit dynamic 5000
 itr map-resolver 192.0.20.11
 itr
 etr map-server 192.0.20.11 key 7 04595A030A784E
 etr map-server 192.0.20.11 proxy-reply
 etr
 map-server
 map-resolver
 exit-service-ethernet
!
instance-id 4097
 remote-rloc-probe on-route-change
 dynamic-eid 192_100_20_0-INFRA_VN-IPV4
  database-mapping 192.100.20.0/24 locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
  exit-dynamic-eid
 !
 service ipv4
  eid-table default
  map-cache 192.100.20.0/24 map-request
  route-export site-registrations
  distance site-registrations 250
  map-cache site-registration
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 4099
 remote-rloc-probe on-route-change
 dynamic-eid 172_20_20_0-Lighting_VN-IPV4
  database-mapping 172.20.20.0/24 locator-set rloc_b9ea8edc-51cc-4af2-bd81-
  28bd2efb8538 exit-dynamic-eid
 !
 service ipv4
  eid-table vrf Lighting_VN
  route-import database bgp 20 route-map DENY-Lighting_VN locator-
set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
  route-export site-registrations
  distance site-registrations 250
  map-cache site-registration
  exit-service-ipv4
 !
 exit-instance-id
!
```

```
instance-id 4100
 remote-rloc-probe on-route-change
 dynamic-eid 172_10_20_0-SnS_VN-IPV4
  database-mapping 172.10.20.0/24 locator-set rloc_b9ea8edc-51cc-4af2-bd81-
  28bd2efb8538 exit-dynamic-eid
  !
  dynamic-eid 172_9_0_0-SnS_VN-IPV4
   database-mapping 172.9.0.0/16 locator-set rloc_b9ea8edc-51cc-4af2-bd81-
   28bd2efb8538 exit-dynamic-eid
  !
  service ipv4
   eid-table vrf SnS_VN
   route-import database bgp 20 route-map DENY-SnS_VN locator-
set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
   route-export site-registrations
   distance site-registrations 250
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 8188
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1021
   database-mapping mac locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
   exit-service-ethernet
  !
  exit-instance-id
 !
 instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1022
   database-mapping mac locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
   exit-service-ethernet
  !
  exit-instance-id
 !
 instance-id 8190
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1023
   database-mapping mac locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
   exit-service-ethernet
  !
  exit-instance-id
 !
 instance-id 8191
  remote-rloc-probe on-route-change
  service ethernet
  eid-table vlan 1024
  database-mapping mac locator-set rloc_b9ea8edc-51cc-4af2-bd81-28bd2efb8538
  exit-service-ethernet

 !
 ipv4 locator reachability exclude-default
 ipv4 source-locator Loopback0
 exit-router-lisp
!
router bgp 20
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
```

```
 bgp graceful-restart
 neighbor 192.168.20.6 remote-as 65500
 neighbor 192.168.20.6 update-source Vlan3008
 neighbor 192.168.20.14 remote-as 65500
 neighbor 192.168.20.14 update-source Vlan3010
 !
 address-family ipv4
  bgp aggregate-timer 0
  network 192.0.20.11 mask 255.255.255.255
  network 192.100.20.0
  aggregate-address 192.100.20.0 255.255.255.0 summary-only
  redistribute lisp metric 10
  neighbor 192.168.20.6 activate
  neighbor 192.168.20.6 weight 65535
  neighbor 192.168.20.6 advertisement-interval 0
  neighbor 192.168.20.14 activate
  neighbor 192.168.20.14 weight 65535
  neighbor 192.168.20.14 advertisement-interval 0
 exit-address-family
 !
 address-family ipv4 vrf Lighting_VN
  bgp aggregate-timer 0
  network 172.20.20.0 mask 255.255.255.0 aggregate-address
  172.20.20.0 255.255.255.0 summary-only redistribute lisp
  metric 10
  neighbor 192.168.20.10 remote-as 65500
  neighbor 192.168.20.10 update-source Vlan3009
  neighbor 192.168.20.10 activate
  neighbor 192.168.20.10 weight 65535
  neighbor 192.168.20.22 remote-as 65500
  neighbor 192.168.20.22 update-source Vlan3012
  neighbor 192.168.20.22 activate
  neighbor 192.168.20.22 weight 65535
 exit-address-family
 !
 address-family ipv4 vrf SnS_VN
  bgp aggregate-timer 0
  network 172.9.0.0
  network 172.10.20.0 mask 255.255.255.0 aggregate-address
  172.10.20.0 255.255.255.0 summary-only aggregate-address
  172.9.0.0 255.255.0.0 summary-only redistribute lisp
  metric 10
  neighbor 192.168.20.2 remote-as 65500
  neighbor 192.168.20.2 update-source Vlan3007
  neighbor 192.168.20.2 activate
  neighbor 192.168.20.2 weight 65535
  neighbor 192.168.20.18 remote-as 65500
  neighbor 192.168.20.18 update-source Vlan3011
  neighbor 192.168.20.18 activate
  neighbor 192.168.20.18 weight 65535
 exit-address-family
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
ip route 0.0.0.0 0.0.0.0 20.20.20.1
!
ip community-list 1 permit 655370
ip ssh source-interface Loopback0
ip ssh version 2
!
!
```

```
ip prefix-list Lighting_VN seq 95472733 permit 172.20.20.0/24
ip prefix-list Lighting_VN seq 629796565 permit 0.0.0.0/0
!
ip prefix-list SnS_VN seq 74127274 permit 172.9.0.0/16
ip prefix-list SnS_VN seq 247440264 permit 172.10.20.0/24
ip prefix-list SnS_VN seq 629796565 permit 0.0.0.0/0
!
ip prefix-list deny_0.0.0.0 seq 10 permit 0.0.0.0/0
!
ip prefix-list l3handoff-prefixes seq 106750737 permit 192.168.20.0/30
ip prefix-list l3handoff-prefixes seq 106898705 permit 192.168.20.4/30
ip prefix-list l3handoff-prefixes seq 107046673 permit 192.168.20.8/30
ip prefix-list l3handoff-prefixes seq 126319505 permit 192.168.20.12/30
ip prefix-list l3handoff-prefixes seq 126467473 permit 192.168.20.16/30
ip prefix-list l3handoff-prefixes seq 127392273 permit 192.168.20.20/30
ip radius source-interface Loopback0
!
ip access-list extended ACL_WEBAUTH_REDIRECT
 denyip any host 10.10.100.52
 permit tcp any any eq www
icmp-echo 10.10.100.10 source-ip 192.168.20.9
 vrf Lighting_VN
 threshold 3
ip sla schedule 2 life forever start-time now
ip sla 3
 icmp-echo 10.10.100.10 source-ip 192.168.20.1
 vrf SnS_VN
 threshold 3
ip sla schedule 3 life forever start-time now
ip sla 4
 icmp-echo 10.10.100.10 source-ip 192.168.20.21
 vrf Lighting_VN
 threshold 3
ip sla schedule 4 life forever start-time now
ip sla 5
 icmp-echo 10.10.100.10 source-ip 192.168.20.17
 vrf SnS_VN
 threshold 3
ip sla schedule 5 life forever start-time now
ip sla 6
icmp-echo 10.10.100.52 source-ip 192.0.20.11
threshold 3
ip sla schedule 6 life forever start-time now
logging trap critical
logging host 10.10.100.50
!
route-map DENY-SnS_VN deny 5
 match ip address prefix-list SnS_VN
!
route-map DENY-SnS_VN deny 10
 match ip address prefix-list l3handoff-prefixes
!
route-map DENY-SnS_VN deny 15
 match community 1
!
route-map DENY-SnS_VN deny 25
 match ip address prefix-list deny_0.0.0.0
!
route-map DENY-SnS_VN permit 30
!
route-map DENY-Lighting_VN deny 5
 match ip address prefix-list Lighting_VN
!
```

```
route-map DENY-Lighting_VN deny 10
 match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Lighting_VN deny 15
 match community 1
!
route-map DENY-Lighting_VN deny 25
 match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Lighting_VN permit 30
!
snmp-server group default v3 priv snmp-server group default v3 auth
context vlan- match prefix snmp-server group ciscogrp v3 priv read
SNMPv3All write SNMPv3None snmp-server view SNMPv3All iso included snmp-
server view SNMPv3None iso excluded

snmp-server community CiscoDNA RW
snmp-server system-shutdown
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit snmp-server enable traps ospf
cisco-specific lsa snmp-server enable traps rep snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cpu threshold
snmp-server enable traps memory bufferpeak
snmp-server enable traps stackwise
snmp-server enable traps udld link-fail-rpt
snmp-server enable traps udld status-change
snmp-server enable traps fru-ctrl snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps energywise snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet group 2
snmp-server enable traps power-ethernet police
snmp-server enable traps entity
snmp-server enable traps pw vc
snmp-server enable traps envmon
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps ipsla
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached
scheduled-test-fail
snmp-server enable traps bfd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps nhrp nhs
```

```
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps local-auth
snmp-server enable traps lisp
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps mvpn
snmp-server enable traps isis
snmp-server enable traps bgp
snmp-server enable traps bgp cbgp2
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server enable traps rf
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfc vpn
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 10.10.100.51 version 2c ciscosnmp
snmp ifmib ifindex persist
!

 pac key 7 15314A1F07257A767B
!
!
ipv6 access-list IPV6_CRITICAL_AUTH_ACL
 sequence 10 permit ipv6 any any
!
ipv6 access-list IPV6_PRE_AUTH_ACL
 sequence 10 permit udp any any eq bootpc
 sequence 20 permit udp any any eq domain
 sequence 30 deny ipv6 any any
!
control-plane
 service-policy input system-cpp-policy
!
cts role-based enforcement
cts role-based enforcement vlan-list 1021-1024
!
line con 0
```

```
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 authorization exec VTY_author
 login authentication VTY_authen
 transport preferred ssh
 transport input all
line vty 5 15
 authorization exec VTY_author
 login authentication VTY_authen
 transport preferred ssh
 transport input all
!
ntp source Loopback0
ntp server 10.10.100.1
!
pnp startup-vlan 1022
end
```

Acronyms and Initialisms

The following table summarizes all acronyms and initialisms used in the *Cisco Connected Communities Infrastructure Solution Design Guide*:

Term	Definition
AB	Anywhere Border
ADR	Adaptive Data Rate
AMP	Advanced Malware Protection
AVC	Application Visibility & Control
BGP	Border Gateway Protocol
BN	Border Node
BSM	Basic Safety Message
BSW	Blind Spot Warning
BW	Bandwidth
CA	Certificate Authority
CCI	Cisco Connected Communities Infrastructure
CCTV	Closed Circuit Television
CCV	Cisco CyberVision
CDN	Cisco Developer Network
CGE	Connected Grid Endpoint
CGR	Connected Grid Router
Cisco DNA Center	Cisco Digital Network Architecture Center
CKC	Cisco Kinetic for Cities
CP	Control Plane
CPNR	Cisco Prime Network Registrar
CR-Mesh	Cisco Resilient Mesh
CSMP	CoAP Simple Management Protocol
CSR	Common Safety Request
CSW	Curve Speed Warning
CTS	Cisco TrustSec
CVD	Cisco Validated Design
DAG	Directed Acrylic Graph
DAO	Destination Advertisement Object
DC	Data Center
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	De-militarized Zone
DNPW	Do Not Pass Warning
DNS	Domain Name System
DODAG	Destination Oriented Directed Acrylic Graph
DoS	Denial of Service

Term	Definition
DSRC	Dedicated Short-Range Communications
EB	Enhanced Beacon
EB	External Border
ECC	Elliptic Curve Cryptography
ECMP	Equal-Cost Multi Path
EEBL	Emergency Electronic Brake Lights
EID	End Point Identifier
EIGRP	Enhanced Interior Gateway Routing Protocol
EN	extended nodes
EPs	Endpoints
ETS	European Teletoll Services
ETSI	European Telecommunications Standards Institute
EVA	Emergency Vehicle Alert
FAR	Field Area Routers
FC	Fiber Channel
FCAPS	enhanced fault, configuration, accounting, performance, and security
FCC	Federal Communications Commission
FCoE	Fiber Channel over Ethernet
FCW	Forward Collision Warning
FE	Fabric Edges
FI	Fabric Interconnects
FiaB	Fabric in a Box
FND	Cisco Field Network Director
GIS	Geological Information System
GRE	Generic Routing Encapsulation
GRT	Global Routing Table
GTK	Group Temporal Key
HER	headend router
HSRP	Hot Standby Router Protocol
HQ	Headquarter
HTDB	Host Tracking Database
IB	Internal Border
ICA	Intersection Collision Avoidance
IE	Industrial Ethernet
IKE	Internet Key Exchange
IMA	Intersection Movement Assist
IPAM	IP Address Management
iSCSI	Internet Small Computer Systems Interface
ISE	Identity Services Engine
ITS	Intelligent Transportation System

LCW	Lane Change Warning
LG	Cimcon LightingGale
LISP	Location/IP Separation Protocol
LoRa	Long Range
LoRaWAN	Long Range WAN
LTA	Left Turn Assist
MAB	MAC Address Bypass
MAC	Media Access Control
MAN	Metropolitan Area Network
MEC	Multi-chassis EtherChannel
MIC	Message Integrity Code
MNT	Monitoring Node
MPLS	Multiprotocol Label Switching
MUD	Manufacture Usage Description
NAN	Neighborhood Area Network
NAT	network address translation
NBAR2	Cisco Next Generation Network-Based Application Recognition
NGFW	Next General Firewall
NGIPS	Next-Generation Intrusion Prevention System
NOC	Network Operation Center
NSF/SSO	Non-Stop Forwarding with Stateful Switchover
NTP	Network Time Protocol
OAM	Operations, Administration, and Management
OBU	On-board Unit
OSPF	Open Shortest Path First
OTAA	Over the Air Activation
PAN	Policy Administration Node; Personal Area Networks
PAgP	Port Aggregated Protocol
PCA	Pedestrian Crossing Assist
PEN	Policy Extended Node
PEP	Policy Enforcement Point
PIM-ASM	Protocol Independent Multicast - Any Source Multicast
PIM-SSM	Protocol Independent Multicast - Source Specific Multicast
PKI	Public Key Infrastructure
PLC	Power Line Communication
PnP	Plug and Play
PoP	Point of Presence
PQ	Priority Queuing
PSM	Personal Safety Message
PSN	Policy Services Node

Term	Definition
PVD	Probe Vehicle Data
PVM	Probe Vehicle Management
PXG	Platform Exchange Grid Node
pxGrid	Platform eXchange Grid
RADIUS	Remote Authentication Dial-In User Service
REP	Resilient Ethernet Protocol
RLOC	Routing Locator
RLVW	Red Light Violation Warning
RPL	Routing Protocol for Low-Power and Lossy Networks
RPoPs	Remote Points-of-Presence
RSA	Roadside Alert
RSU	Roadside Unit
RSZW	Reduce Speed/Work Zone Warning
RTA	Right Turn Assist
SCMS	Security Credential Management System
SD-Access	Software-defined Access
SFP	Small Form-Factor Pluggable
SGTs	Security Group Tags
SGACL	Security Group-based Access Control List
SLC	Street Light Controller
SMC	StealthWatch Management Console
SPAT	Signal Phase and Timing Message
SRM	Signal Request Message
SSID	Service Set Identifier
SSM	Software Security Module
SVL	StackWise Virtual Link
SXP	SGT eXchange Protocol
TC	Transit Control
TFTP	Trivial File Transfer Protocol
TIM	Traveler Information Message
TMC	Traffic Monitoring Center
TPE	ThingPark Enterprise
UCS	Cisco Unified Computing System
UDP	User Datagram Protocol
UPS	Uninterrupted Power Supply
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle-to-Infrastructure

Term	Definition
VN	virtualized network
VNI	VXLAN Network Identifier
VoD	Video-on-Demand
VRF	virtual routing and forwarding
VSM	Video Surveillance Manager
VXLAN	Virtual Extensible LAN
WAVE	Wireless Access in Vehicular Networking
Wi-Fi	Wireless Fidelity
WLC	Wireless LAN Controller
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WRED	Weighted Random Early Detect
WSMP	WAVE Short Message Protocol
ZTD	Zero Touch Deployment