Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1

Implementation Guide

April 2024

Cisco Validated Design

Cisco Systems, Inc. www.cisco.com

Contents

Preface

This Cisco Renewable Energy Offshore Wind Farm Solution Release 1.0 Cisco Validated Design (CVD) Implementation Guide provides a comprehensive explanation of the offshore wind farm operator (asset operator) network infrastructure implementation. It includes information about onshore network, offshore network, turbine area network (TAN), and farm area networks (FAN). It also discusses offshore wind farm solution use cases, such as wind farm operator enterprise network services, physical security, miscellaneous systems, supervisory control and data acquisition (SCADA) for wind turbine generators, and more. Implementation guidance also is provided for the Cisco Ultra-Reliable Wireless (URWB) network for service operations vessel (SOV) to offshore substation (OSS) connectivity.

This document includes information about the solution architecture and possible deployment models and provides guidelines for deployment. It also discusses best practices and potential issues to be aware of when deploying the reference architecture.

Document Objective and Scope

This implementation guide provides comprehensive details about the Cisco renewable energy offshore wind farm asset operator's network infrastructure implementation. This implementation leverages Cisco Industrial Ethernet switches, Cisco Catalyst 9300 and 9500 Series switches, Cisco Next Generation Firewall (NGFW), Cisco Digital Network Architecture Center (Cisco Catalyst Center), Cisco C9800 WLC and APs, and URWB.

This document also provides detailed information about wind farm implementation use cases, including physical safety and security and offshore wind farm network enterprise services such as IP telephony, network security, and so on. The implementation steps that are described in this document can be used as a reference for wind farm deployments as described in *Cisco Solution for Renewable Energy: Offshore Wind Farm 1.0 Design Guide*:

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/wind-farm-design-guide.pdf

Detailed implementation for other wind farm use cases such as the turbine vendor's control network, power automation and control, and marine related systems that are not validated in this solution and are outside the scope of this document.

This document provides detailed information about the implementation of the Cisco Renewal Energy Offshore Wind Farm operator's network, which includes the implementation of a wind farm offshore, onshore access and core network services, Cisco SD-WAN backhaul, network security service, wind farm data enter, and management applications.

This document provides example of offshore wind farm operator's network configurations and WAN backhaul with private multiprotocol label switching (MPLS) network configuration for the deployment models and network topologies that are validated in the solution. Detailed implementation of network routing protocols and configuring MPLS network backhaul is beyond the scope of this document.

Audience

The audience for this guide includes, but is not limited to, system architects; network, computer, and systems engineers who manage offshore wind farm assets; field consultants; Cisco Solution Support specialists; and customers.

You should be familiar with networking protocols and IP routing, basic network security, and QoS. You also should have some understanding of server virtualization using hypervisor and the Cisco Renewable Energy Offshore Wind Farm Solution Architecture, which is described in *Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide*.

Chapter 1: Introduction

Most countries are investing in renewable energy generation to accelerate the move toward carbon neutrality. The following technologies are growing steadily and being deployed at scale:

- Onshore and offshore wind
- Onshore solar farms
- Onshore battery storage

Other renewable technologies also are being researched and developed, such as wave, tidal, and energy storage technologies. We will start to see more innovative renewable energy deployments in the future.

Some countries are leading the push to integrate renewable energy into the grid. China and the UK are examples of countries leading the way with large deployments of wind farms, both onshore and offshore. European countries in general are setting big targets for offshore wind farms. And the United States is predicted to become a major offshore wind energy producer in the coming decade. Cisco can help with renewable energy technologies, and this document focuses on the challenges offshore wind farms are facing and the solutions that Cisco offers to address them.

Deploying and operating renewable technologies can be challenging. They need to operate in harsh and remote locations, a secure and reliable network is required, and that network needs to work flawlessly with the various OT and IT technologies that form the solution.

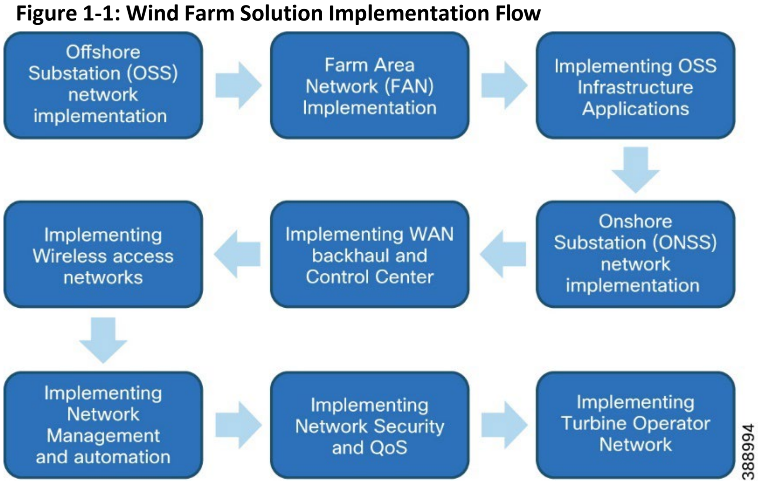
The offshore wind farm solution architecture includes ruggedized access network devices, such as Cisco Industrial Ethernet (IE) switches and Cisco Industrial Routers (IR). It also includes Cisco Catalyst 9300 and 9500 Series switches, Cisco Next Generation Firewalls (NGFW) and the Cisco Unified Computing Systems (UCS) servers, C9800 Wireless LAN Controllers (WLCs), URWB, and other network infrastructure components. These devices and components provide a scalable and secure network for wind farm solution use cases.

The wind farm solution implementation is based on the design that is recommended in [Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide.]

Implementation Flow

Figure 1-1 shows the implementation flow that this document describes for an offshore wind farm network. We recommend that a wind farm network be implemented according to this flow.

Figure 1-1: Wind Farm Solution Implementation Flow



The document addresses the implementation of the following network building blocks in sequence to implement an end-to-end offshore wind farm solution:

- Implementation of an offshore substation (OSS) network, which includes OSS core Catalyst 9500 Series switches StackWise Virtual (SVL), an infrastructure access switch stack using Catalyst 9300 Series switches, a farm area network (FAN) ring aggregation switch stack, and an OSS DMZ network with a firewall.
- Implementation of a FAN ring topology on Cisco Catalyst Industrial Ethernet switches, including REP configuration for FAN resiliency, and a turbine area network (TAN) with REP subtended rings for high availability.
- Deployment of an OSS infrastructure access network switch stack and related applications such as Cisco Cyber Vision Center (local),

Cisco Secure Network Analytics (SNA) NetFlow collector, OPC-UA Server applications, and more.

- Implementation of an onshore substation (ONSS) network, which includes ONSS core Catalyst 9500 Series switches StackWise Virtual (SVL), an ONSS network access switch stack using Catalyst 9300 Series switches, and an ONSS DMZ network with a firewall.
- Implementation of WAN backhaul using Cisco Industrial 8340 Series rugged routers (IR8340) leveraging a Cisco SD-WAN deployment.
- Deployment of wind farm control center network components, including a WAN headend, a firewall, and applications such as Cisco Catalyst Center, Cisco ISE, Cyber Vision Global Center, SNA Manager, and so on.
- Deployment of wireless network components, such as WLC, access points, URWB radios, and so on for wind farm wireless network access.
- Implementation of network management services using Cisco Catalyst Center, and automated provisioning of wind farm network components using Cisco Catalyst Center workflows and day N template features.
- Configuration of network security components, such as Firepower, Cyber Vision network sensors, SNA NetFlow, and so on, and quality of service (QoS) provisioning in the OSS network.

Chapter 2: Solution Network Topology and Addressing

This chapter discusses the various topologies that are used for the wind farm solution validation and implementation. It includes the following topics:

- Solution Validation Topologies
- Network VRFs and VLANs
- IP Addressing
- Solution Components

Solution Validation Topologies

Two deployment topologies have been validated as part of the Offshore Wind Farm CVD Solution validation effort:

- Offshore wind farm wired network topology with turbine area networks (TAN), a farm area network (FAN), an offshore substation (OSS), an onshore substation (ONSS), WAN backhaul, and a control center. See Figure 2-1, which shows the offshore wind farm wired network topology, including endpoints for various validated wind farm use cases.
- Offshore wind farm wireless network topology, consisting of Cisco WLCs and access points that provide Wi-Fi access for the OSS, FAN, and TAN, and a URWB network that provides wireless connectivity for SOVs back to the OSS. See Figure 2-2.

Figure 2-1: Wind Farm 1.1 Wired Network Topology

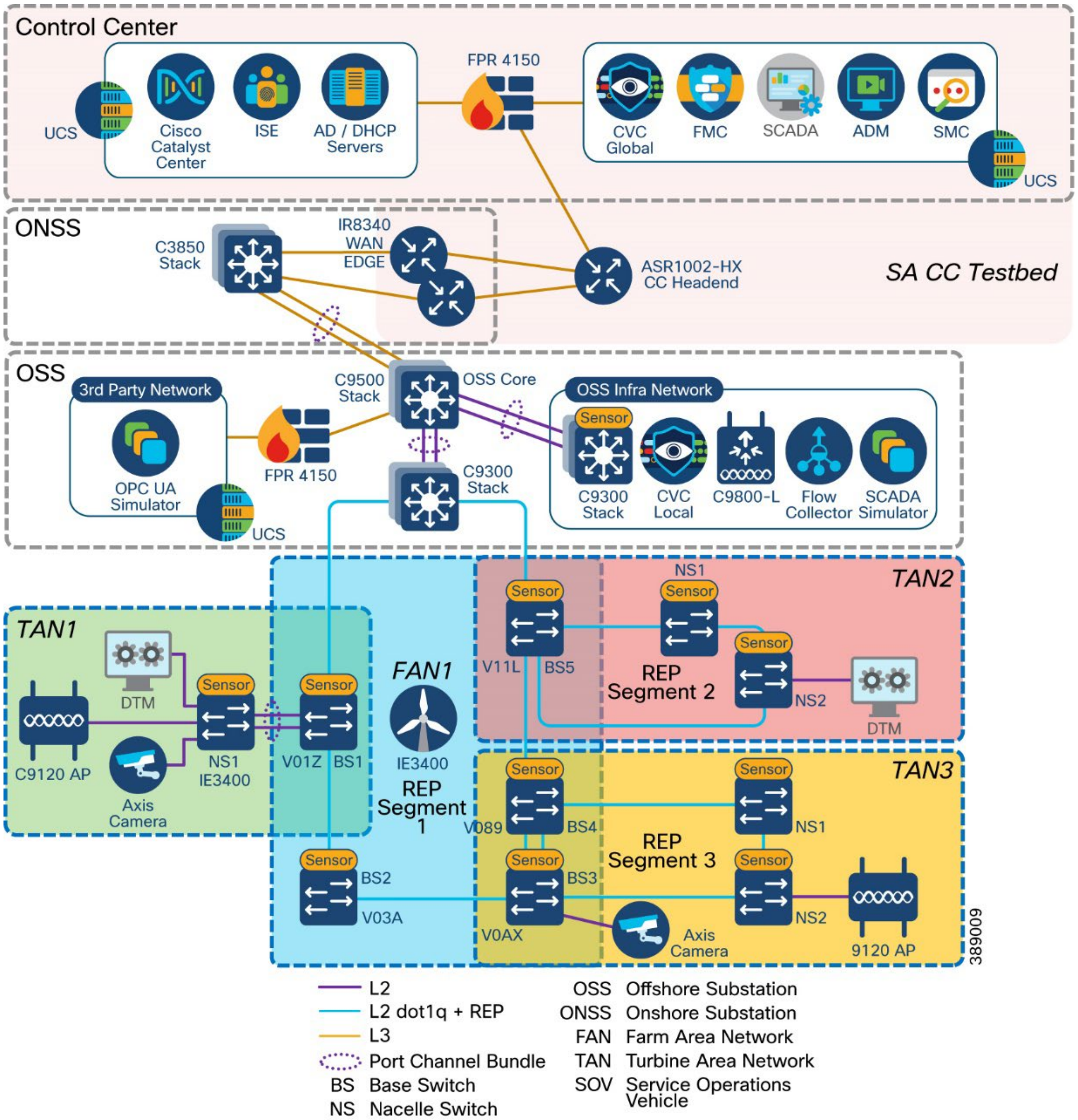
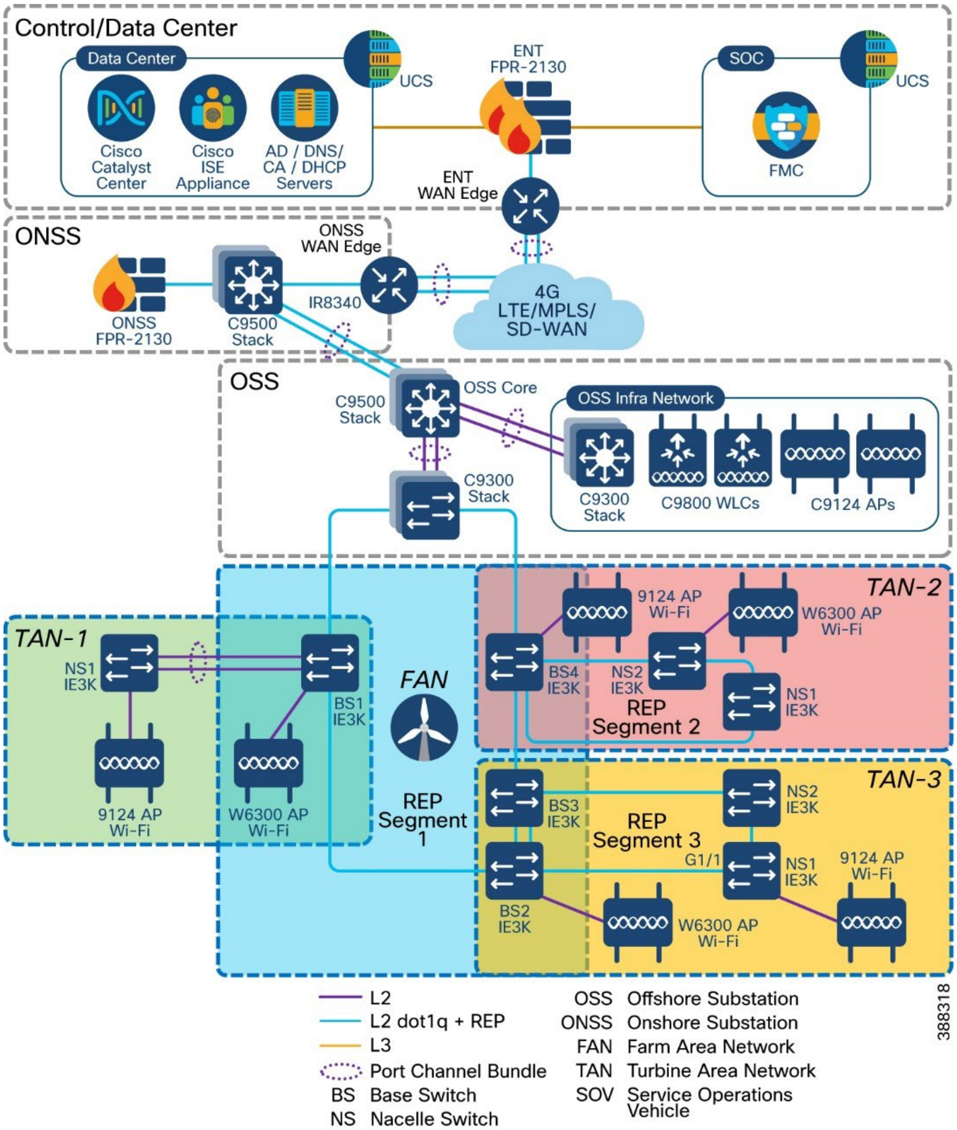


Figure 2-2: Wind Farm 1.1 Wireless Network Topology



Network VRFs and VLANs

This section describes example virtual routing and forwarding (VRF) and VLANs that are configured in the wind farm solution network and layer 3 routing configuration between OSS and ONSS core networks. The wind farm network is segmented by using VLANs for various end points and applications traffic. There is a dedicated VRF and VLAN for each service and endpoint and for application traffic in the network. Table 2-1 provides examples of VRFs and VLANs in the network.

Table 2-1: Examples of VLANs and VRFs Validated in this Implementation

VRF Name	VLAN ID	VLAN Name and Description
Management_VRF (VRF for network management traffic)	▪ 100 ▪ 101 ▪ 102 ▪ 103 ▪ 104 ▪ 105 ▪ 106	▪ OSS infrastructure applications and services VLAN ▪ Network device management VLAN ▪ Cyber Vision sensors IP subnet for collection network ▪ Wi-Fi APs management VLAN ▪ Network management traffic simulation VLAN ▪ REP admin VLAN ▪ URWB management VLAN
VnV_VRF (voice and video VRF)	▪ 500 ▪ 600	▪ VLANs for CCTV cameras in FAN and TAN ▪ IP telephony devices voice VLAN
Wi-Fi access	▪ 900 ▪ 901	▪ Employee and contractor Wi-Fi access ▪ Guest Wi-Fi access
URWB	▪ 1000	▪ URWB traffic
OT_VRF (SCADA and other OT traffic)	▪ 700	▪ SCADA OT traffic VLAN in TAN and turbine base network (TBN) Example: turbine controller VLAN, SCADA clients
Global routing table (GRT)	▪ 800 ▪ 801	▪ OSS local VLAN in OSS network only (not to be routed) ▪ ONSS local VLAN in ONSS network only (not to be routed)

Table 2.2 VLANs used in Turbine operator network

VLAN Name	VLAN ID	Description
Multicast_VLAN	5	Used for multicast
PVLAN_vlan	10	Primary VLAN (Used for OPC-UA)
Traffic-test	20	Traffic test VLAN
Isolated_vlan	101	Isolated secondary VLAN
Management_VLAN	111	Management VLAN

IP Addressing

This section describes example IP addressing prefixes that are used in the topologies that Figure 2-1 and Figure 2-2 show.

Note: The IP addresses that are shown in this section are examples used only for the solution validation as internal subnetworks in the CVD lab. This information provides a reference for selecting subnets for the solution implementation. We recommend choosing private network prefixes and an IP addressing scheme based on the solution deployment and devices that are connected to the offshore wind farm network.

Table 2-2: Example list of IP Addressing Validated in this Implementation

VRF Name	VLAN ID	Subnet ID	Default Gateway	Description
Management_VRF	100	10.10.100.0/24	10.10.100.1	OSS infrastructure applications and services VLAN
	101	10.10.101.0/24	10.10.101.1	Network switches, routers, FP management VLAN
	102	10.10.102.0/24	10.10.102.1	Cyber Vision sensors IP subnet for collection network
	103	10.10.103.0/24	10.10.103.1	Wi-Fi AP management
	104	10.10.104.0/24	10.10.104.1	VLAN for network management traffic
	105	10.10.105.0/24	10.10.105.1	REP admin VLAN
	106	10.10.106.0/24	10.10.106.1	URWB management
VnV_VRF	500	172.16.50.0/24	172.16.50.1	VLAN for CCTV cameras in TAN and FAN
	501	172.16.51.0/24	172.16.51.1	VLAN for video traffic simulation
	600	172.16.60.0/24	172.16.60.1	VLAN for voice communications (IP telephony) in TAN and FAN
	601	172.16.61.0/24	172.16.61.1	VLAN for voice traffic simulation
Wi-Fi access	900	172.16.90.0/24	172.16.90.1	VLAN for employee and contractor Wi-Fi
	901	172.16.91.0/24	172.16.91.1	VLAN for guest Wi-Fi
URWB access	1000	172.18.100.0/24	172.18.100.1	VLAN for URWB traffic
OT_VRF	700	172.16.70.0/24	172.16.70.1	SCADA OT traffic VLAN in TAN and TBN Example: turbine controller VLAN, SCADA Clients
	701	172.16.71.0/24	172.16.71.1	SCADA OT traffic simulation VLAN
Global routing table (GRT)	800	172.16.80.0/24	172.16.80.1	OSS Local VLAN in OSS network only (Nonroutable across OSS and ONSS)
	801	172.16.81.0/24	172.16.81.1	ONSS Local VLAN in ONSS network only (Nonroutable across OSS and ONSS)

Solution Components

This section lists the Cisco hardware and software component versions that are validated in the wind farm solution implementation topologies that Figure 2-1 and Figure 2-2 show.

It also describes the wind farm third-party hardware and software components that are validated in this implementation.

Table 2-3: Cisco Components and Versions Validated in the Wind Farm Solution

Hardware Model	Role in Offshore Wind Farm	Software or Firmware Version
IE3400-8P2S, IE3400-8T2S	Turbine nacelle switch, non-HA	17.11.1
IE3400-8P2S, IE3400-8T2S	Turbine nacelle switch, HA	17.11.1
IE3400-8P2S, IE3400-8T2S	Turbine base switch	17.11.1
C9300-24UX	Farm area aggregation	17.11.1
C9500-16X	OSS core switch, HA	17.11.1
C9300-24UX	OSS IT network access switch	17.11.1
C3850-24UX	ONSS core switch	16.12.1
Firepower 2140	OSS and ONSS DMZ firewall	7.0.1
Firepower Management Center (FMC)	Firewall management application	7.0.1
IR8340	ONSS WAN edge router	17.11.1
DN2-HW-APL	Cisco Catalyst Center Network Management Appliance	2.3.6.0
UCS-C240-M5S	Unified Computing System (UCS)	3.1.3c
Cisco ISE Virtual Appliance	AAA server	3.2
IoX Sensor App	Cyber Vision network sensors	4.1.2
Cisco Cyber Vision Center Global and local	OT security dashboard	4.1.2
C9800-L-C-K9	Wireless LAN controller	17.11.1
IW6300-AP	Cisco IW6300 ruggedized AP for Wi-Fi access	17.11.1
AIR-AP9120	Cisco AP for Wi-Fi access	17.11.1
URWB FM3500 and FM4500	URWB mesh point	9.4
URWB FM1000 Gateway	URWB mesh gateway	1.6.0
URWB FM-Monitor VM	URWB FM-Monitor	1.0.1
Cisco Secure Network Analytics (Stealthwatch)	IT and OT security management	7.4.1
ASR-1002-HX	Control center headend router	17.3.4a
Cisco SD-WAN vManage, vSmart, vBond	WAN management	20.8.1

Table 2-4: Third-party Hardware and Software Validated in this Wind Farm Solution

Hardware Model	Role in Offshore Wind Farm	Software/Firmware Version
AXIS P3717-PLE	Turbine physical security (CCTV) camera	10.3.0
Axis Device Manager (ADM)	Video server for CCTV camera	5.9.42
Microsoft Windows 2016 Server	AD, DHCP, and DNS servers in control center	Windows 2016 Server Edition

Note: Ensure that you enable appropriate licenses for the features and functions for the network components that are listed in Table 2-3 and Table 2-4. See the product data sheets for more information.

Chapter 3: Offshore Substation Network Implementation

This chapter includes the following topics:

- Offshore Substation Core Network Implementation
- Configuring FAN Ring Aggregation Switch Stack
- Configuring OSS Infrastructure Network Access
- OSS Network DMZ with Firewall

Offshore Substation Core Network Implementation

Cisco Catalyst 9500 Series switches can be used as core switches in the wind farm solution. For redundancy, Cisco StackWise Virtual (SVL) is configured between two 9500 switches, with each switch sharing an interface with the distribution layer and access switches.

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

The connection to the distribution layer is accomplished with interfaces that are configured as switchport trunks. Switched Virtual Interface (SVI) is used for the layer 3 configuration, and the SVIs serve as the default gateways for management VLANs.

Bringing Up Catalyst 9500 StackWise Virtual

Configuration of 9500 starts with configuring SVL. Figure 3-1 shows how the cabling of the two Cisco 9500 switches must be done before starting SVL configuration:

Figure 3.1: DAD and SVL links for 9500 SVL

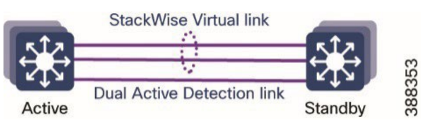
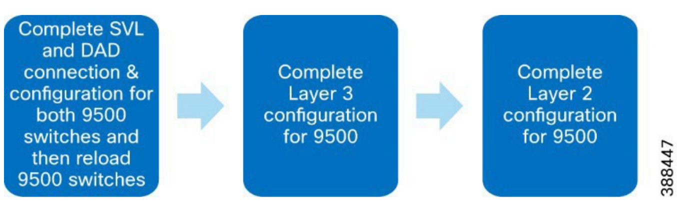


Figure 3-2 shows the workflow for the initial bring-up of the Catalyst 9500 Series switches.

Figure 3-2: Workflow for Initial Bring-Up of Catalyst 9500 Series Switches in the Wind Farm OSS Core



This solution uses one connection for the SVL and one connection for the dual active detection link. For detailed SVL configuration steps and prerequisites, see “Configuring Cisco StackWise Virtual” in *High Availability Configuration Guide, Cisco IOS XE Bengaluru 17.5.x (Catalyst 9500 Switches)*:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-5/configuration_guide/ha/b_175_ha_9500_cg/configuring_cisco_stackwise_virtual.html

After the physical connection of the 9500 switches is complete, follow these steps to complete the SVL configuration:

1. Perform these actions to configure SVL:
   a. Reassign the switch numbers of the two switches to switch numbers 1 and 2, and assign priorities as follows:

      9500-1:
      ```
      Switch 1 priority 15
      ```
      9500-2:
      ```
      switch 1 renumber  2
       switch 1 priority
      ```
   b. Complete the following SVL configuration on each of the switches:

      9500-1:
      ```
      stackwise-virtual
       domain 2
      !
      interface TenGigabitEthernet1/1/1
       stackwise-virtual link 1
      !
      interface TenGigabitEthernet1/1/5
       stackwise-virtual dual-active-detection
      !
      ```
      9500-2:
      ```
      interface TenGigabitEthernet2/1/1
       stackwise-virtual link 1
      !

      interface TenGigabitEthernet2/1/5
       stackwise-virtual dual-active-detection
      ```
   c. Reload the two switches to cause the SVL configuration to take effect.
   d. Enter the following command on each 9500 switch to verify that switches are now in SVL mode:

      show stackwise-virtual

      The command output should show that the two switches are in Active Standby mode and show their configured switch numbers.
2. Configure layer 3 for 9500 SVL:
   a. Configure a switched virtual interface (SVI) for management VLAN 101, assign an IP address to it, and forwarding VRF in Management_VRF:
      ```
      hostname WF-OSS-C9500
      vlan 100
       name OSS_INFRA_VLAN
      !
      vlan 101
       name OSS_NET_MGMT
      !
      interface Vlan101
       vrf forwarding Management_VRF
       ip address 10.10.101.1 255.255.255.0
      !
      vrf definition Management_VRF
       rd 100:1
       !
       address-family ipv4
        route-target export 100:1
        route-target import 100:1
        route-target export 100:1
       stitching
        route-target import 100:1
       stitching
       exit-address-family
       !
       address-family ipv6
        route-target export 100:1
      ```

```
  route-target import 100:1
  route-target export 100:1
 stitching
  route-target import 100:1
 stitching
 exit-address-family
```

b. Configure OSPF routing for underlay network reachability between OSS and ONSS core switches:

```
router ospf 1
 router-id 192.168.5.2
 network 172.16.1.0 0.0.0.3 area 0
 network 192.168.2.2 0.0.0.0 area 0
 network 192.168.5.2 0.0.0.0 area 0
 network 192.168.7.2 0.0.0.0 area 0
```

c. Configure the core face VLAN on the C9500 SVL VTEP:

```
!
vlan configuration 11
 member vni 5000
!
```

d. Configure Switch Virtual Interface (SVI) for the core facing VLAN:

```
interface Vlan11
 vrf forwarding Management_VRF
 ip unnumbered Loopback0
 no autostate
```

e. Configure Switch Virtual Interface (SVI) for the access facing VLAN:

```
interface Vlan100
 vrf forwarding Management_VRF
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 192.168.6.2
!
```

f. Configure loopback interface on the VTEP:

```
interface Loopback0
 ip address 192.168.5.2 255.255.255.255
!
```

g. Configure NVE interface on the VTEP:

```
interface nve1
 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 5000 vrf Management_VRF
!
```

h. Configure BGP with IPv4 or IPv6 or both address families on the VTEP:

```
router bgp 1
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 192.168.5.1 remote-as 1
 neighbor 192.168.5.1 update-source Loopback0
 !
```

```
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  neighbor 192.168.5.1 activate
  neighbor 192.168.5.1 send-community both
exit-address-family
 !
 address-family ipv4 vrf Management_VRF
  advertise l2vpn evpn
  redistribute static
  redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf Management_VRF
  redistribute connected
  redistribute static
  advertise l2vpn evpn
 exit-address-family
 !
```

i. After EVPN VXLAN BGP core routing is configured on the peer ONSS core C9500 SVL switch, you can verify the VXLAN NVE peer status, BGP routing tables using the following CLIs:

```
WF-OSS-C9500#show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Interface  VNI      Type Peer-IP          RMAC/Num_RTs   eVNI     state flags UP time
nve1       5000     L3CP 192.168.5.1      ccb6.c864.f7d4 5000       UP  A/M/4 2d09h
!

WF-OSS-C9500#show bgp l2vpn evpn all
BGP table version is 132, local router ID is 192.168.7.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf Management_VRF)
 *>    [5][100:1][0][16][172.114.0.0]/17
                      0.0.0.0                  0         32768 ?
 *>    [5][100:1][0][24][10.10.1.0]/17
                      10.10.100.2              0         32768 ?
 *>    [5][100:1][0][24][10.10.100.0]/17
                      0.0.0.0                  0         32768 ?
 * i   [5][100:1][0][24][10.10.201.0]/17
                      192.168.5.1              0    100      0 ?
```

```
 * i                    192.168.5.1              0    100       0 ?
 *>i                    192.168.5.1              0    100       0 ?
```

Refer to the following URL for more details on EVPN VXLAN BGP Core routing implementation steps network VTEPs:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-3/configuration_guide/vxlan/b_173_bgp_evpn_vxlan_9500_cg/configuring_evpn_vxlan_layer_3_overlay_network.html

3. Configure layer 2 for 9500 SVL:

   a. Configure port-channels and trunk port on the links going to the Catalyst 9300 FAN aggregation:

```
interface TenGigabitEthernet1/0/3
 description ##Connection to 9300 Agg##
 channel-group 1 mode desirable
!
interface TenGigabitEthernet2/0/3
 description ##Connection to 9300 Agg##
 channel-group 1 mode desirable
!
!
interface Port-channel1
 switchport mode trunk
!
```

   b. Configure port-channels and trunk port on links going to the C9300 access switch of the OSS infrastructure network and on the links going to the ONSS core:

```
interface TenGigabitEthernet1/1/3
 channel-group 2 mode desirable
 description ##Connection to 9300 Access##
!
interface TenGigabitEthernet2/1/3
 channel-group 2 mode desirable
 description ##Connection to 9300 Access##
!
!
interface Port-channel2
 switchport mode trunk
!
interface TenGigabitEthernet1/1/7
 channel-group 3 mode desirable
 description ##ConnectionTo3850##
!
interface TenGigabitEthernet2/1/7
 channel-group 3 mode desirable
 description ##ConnectionTo3850##
!
interface Port-channel3
 switchport mode trunk
!
```

Configuring FAN Ring Aggregation Switch Stack

A pair of Cisco Catalyst 9300 Series switches in a stack is configured as a FAN ring aggregation switch in the wind farm network. This section describes the implementation of a FAN ring aggregation switch stack.

Catalyst 9300 Switch Stack for FAN Aggregation

Figure 3-3 shows the workflow configuring a Cisco Catalyst 9300 access switch stack.

Figure 3-3: Workflow for Configuring Catalyst 9300 Access Switch Stack

1. Configure a 9300 access switch stack by connecting the stack cables for each switch and booting each switch.

   When the switches come up, they are in a stack. The active and standby switches are selected automatically.

   Alternatively, you can assign a priority and switch number to a switch manually. The switch that is to be the active switch should be assigned a higher priority.

   For information about Cisco Catalyst 9300 Series switch stack configuration, see “Managing Switch Stacks” in *Stacking and High Availability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x Catalyst 9300 Switches*:

   https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/stck_mgr_ha/b_173_stck_mgr_ha_9300_cg/managing_switch_stacks.html

2. Configure layer 3 for the 9300 switch stack:

   a. Configure the management SVI interface as Vlan101 and assign an IP address to Vlan101:

   ```
   hostname WF-OSS-C9300Agg
   vlan 101
   interface Vlan101
    ip address 10.10.101.13 255.255.255.0
   !
   ```

   b. Configure the **ip routing** command and then configure the default route to point to the 9500 SVL:

   ```
   ip routing
   !
   ip route 0.0.0.0 0.0.0.0 10.10.101.1
   ```

3. Configure Layer 2 for the Cisco Catalyst 9300 switch stack:

   a. Configure port-channels and trunk port on links going to the Catalyst 9500 SVL:

   ```
   !
   interface TenGigabitEthernet1/1/3
    description ##ConnectionTo9500##
    channel-group 1 mode desirable
   !
   interface TenGigabitEthernet2/1/3
    description ##ConnectionTo9500##
    channel-group 1 mode desirable
   !
   interface Port-channel1
    switchport mode trunk
   ```

   b. Enter the following command to verify that the port-channel is up and that the trunk port is created:

   show etherchannel summary

Configuring OSS Infrastructure Network Access

Before configuring layer 2 and layer 3 for the C9300 stack of the OSS infrastructure network, ensure that the switch stack configuration for the C9300 is complete as described in the previous section. The follow these steps on the C9300 stack.

1. Perform these actions to complete the layer 3 configuration for the C9300 stack from the CLI:

   a. Configure the management VLAN and the SVI in Vlan101:

   ```
   hostname OSS-C9300-Access
   vlan 101
   !
   interface Vlan101
    ip address 10.10.101.5 255.255.255.0
   ```

b. Configure the Catalyst 9500 SVL as the default gateway:

```
ip default-gateway 10.10.101.1
!
```

2. Perform these actions to configure layer 2 for the C9300 stack from the CLI:

a. Configure port-channels and the trunk port on links that are connected to the Catalyst 9500 SVL:

```
interface TenGigabitEthernet1/1/1
description ##ConnectionTo9500##
 channel-group 1 mode desirable
!
interface TenGigabitEthernet2/1/1
 description ##ConnectionTo9500##
 channel-group 1 mode desirable
!
interface Port-channel1
 switchport mode trunk
```

b. Enter the following command to verify that the port-channel is up and that the trunk port is created:

show etherchannel summary

```
--------Output Omitted------------
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
---------+------------------+---------------+------------------------------------------------------------------
1     Po1(SU)         PAgP        Te1/1/1(P)       Te2/1/1(P)

show interfaces trunk
Port           Mode             Encapsulation  Status        Native vlan
Po11           on               802.1q         trunking      1
```

OSS Network DMZ with Firewall

This section describes the implementation of a firewall in an OSS DMZ network.

Cisco Firepower Next Generation Firewall (NGFW) Implementation

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 wind farm solution, the 2140 series Firepower model is used. In this implementation, a Firepower device is managed by the Firepower Management Center (FMC). The FMC is installed in the Control Center UCS as shown in Figure 2-1.

FMC is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for a Firepower system deployment. FMC controls the network management features on devices, including switching, routing, NAT, VPN, and so on.

In the wind farm solution, FMC is deployed as a virtual machine. It must be configured in the same network as the management ports of Firepower NGFWs.

Figure 3-4 shows the workflow for the Firepower configuration.

Figure 3-4: Workflow for Configuring Firepower

For more information about FMC and the configuration steps for management of Firepower, see "Getting Started With Firepower" in *Firepower Management Center Configuration Guide*:

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

After the FMC is installed as a virtual appliance as described in “Getting Started With Firepower,” open the FMC console and configure the management IP address (which should have reachability to the FPR management IP address), configure the default gateway, and log in credentials.

Next, log in to a Microsoft Windows PC that is in a network that the FMC can reach and open the FMC in a web browser. Enter the configured FMC IP address and login credentials. The FMC is now ready to start configuring Firepower.

Firepower Installation and High Availability Configuration

In the wind farm solution, Firepower is used to provide network security between zones and secure access to third-party OPC-UA clients that are connected behind a firewall. Firepower is configured with high availability (HA) to provide redundancy in the setup. An HA pair of Firepower Threat Defense (FTD) devices results in a single logical system for policy application, system updates, and registration. With HA, the system can fail over either manually or automatically.

A third-party turbine vendor SCADA network connects to the OSS DMZ network through a firewall, as described in

Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf?dtid=odicdc000509

OPC-UA clients from the OSS infrastructure network access OPC-UA servers in the third-party network via secure Firepower policies.

Before configuring Firepower as described in the following sections, follow these steps to configure Firepower for routed mode and to be managed via the FMC.

1. Configure routed mode.

   Routed mode for Firepower must be chosen as a part of the initial configuration when the FTD device boots up for the first time. If Firepower was not configured for routed mode when the FTD device booted for the first time, enter the following command in the Firepower CLI to configure Firepower for routed mode:

   > **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.
   ```

   For more detailed information, see “Transparent or Routed Firewall Mode for Firepower Threat Defense” in *Firepower Management Center Configuration Guide, Version 7.0*:

   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

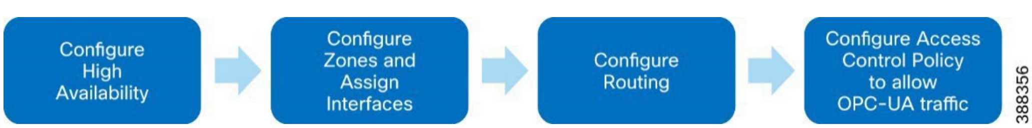
2. Configure management via the FMC.

   See *Cisco Firepower 2100 Getting Started Guide* for the steps to perform the initial configuration of Firepower Threat Defense (FTD) and configure the management of the FTD via the FMC:

   https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/ftd-fdm-2100-qsg.html

Configuring Firepower for Wind Farm Solution Use Cases

Figure 3-5: Workflow for Configuring Cisco Firepower Using FMC



To configure Firepower, follow these steps.

1. After adding both devices to the Firepower Management Center, perform the following steps to configure high availability:
   a. Under **Devices**, choose **Device Management**.
   b. From the **Add** drop-down menu, choose **High Availability**.
   c. In the **Add High Availability Pair** dialog box, enter a logical name for the high availability pair in the **Name** field.
   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. From the **LAN Failover Link** drop-down list, 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 are listed in the **Interface** drop-down list in the **Add High Availability Pair** dialog box.

i. Enter any identifying logical name for the link in the dialog box that appears.

j. Enter 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** . It then takes a few minutes for system data to be synchronized.

For more detailed information about configuring high availability and cabling FPRs for high availability, see "High Availability for FTD" in *Firepower Management Center Configuration Guide, Version 7.0*:

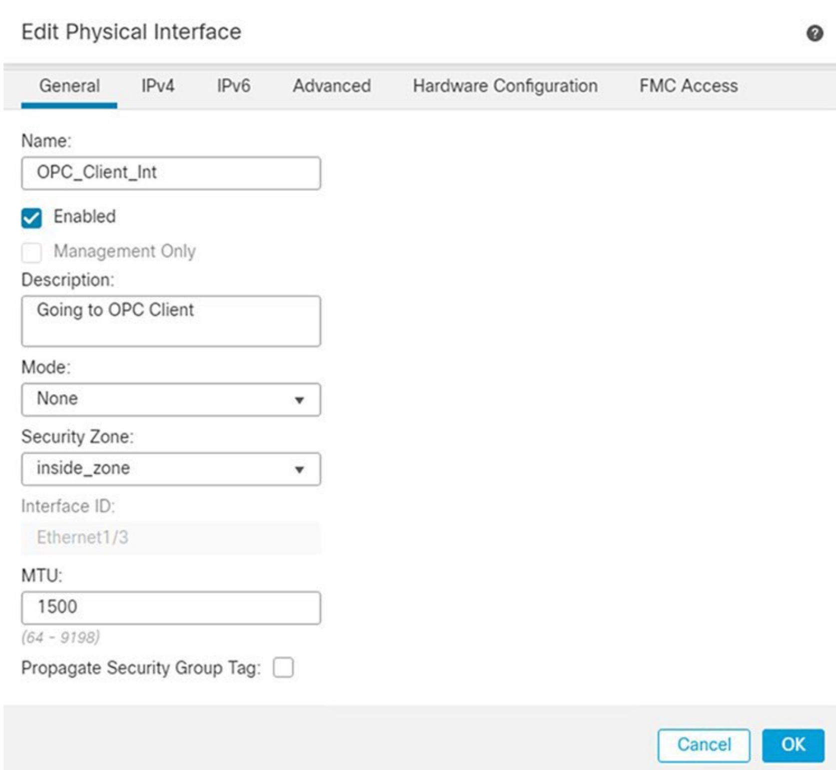
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/high_availability_for_firepower_threat_defense.html

2. Perform the following steps to configure Firepower interfaces:

a. Choose **Devices > Device Management** and click the edit icon that corresponds to the HA pair.

b. Click the **Edit** icon next to the interface to be configured and configure the details for that interface, as shown in Figure 3-6.

Figure 3-6: Configuring Interfaces



Repeat Steps 2a and 2b as needed to bring up the other Firepower interfaces and assign IP addresses and names to them.

3. Perform the following steps to configure routing for network reachability via Firepower.

Because Firepower acts as the firewall between the DMZ and the outside network, a static default route must be configured on Firepower so that permitted devices can reach the DMZ.

a. Choose **Devices > Device Management** and click the edit icon that corresponds to the HA pair.

b. Click the **Routing** tab.

c. Click **Static Route**.

d. Click **Add Route**.

e. Click the **IPv4** radio button.

f. From the **Interface** drop-down list, choose the interface to which this static route applies.

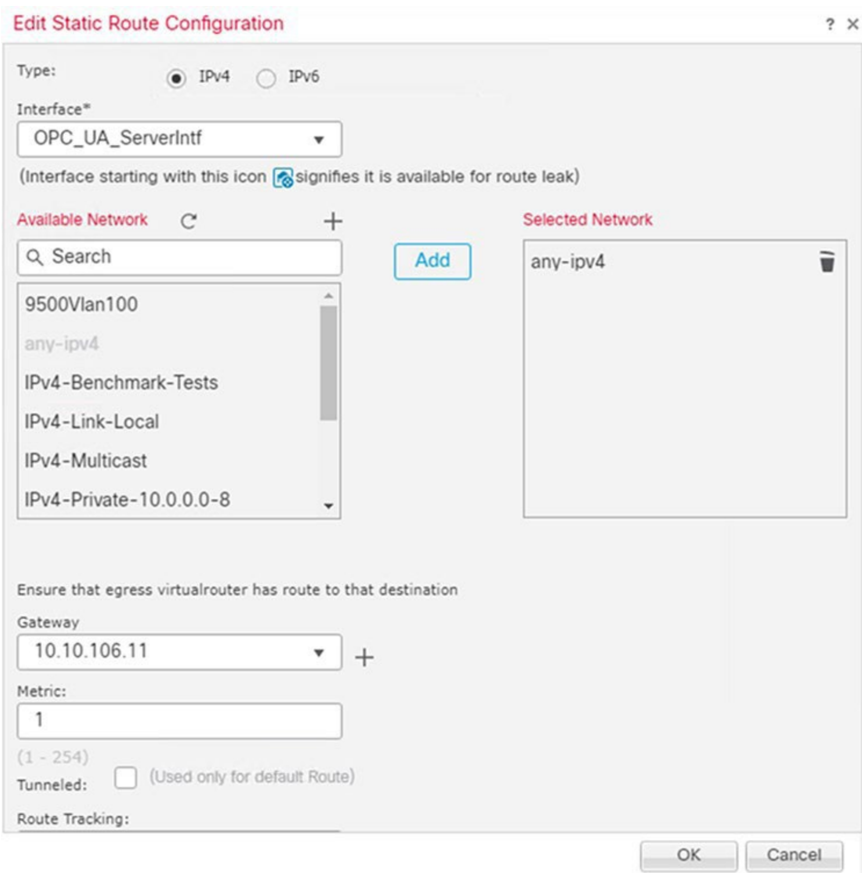
g. In the **Available Network** window, a network object for the destination network can be added clicking **+** . To add a static default route, choose the network **any-ipv4** (0.0.0.0/0) from the **Available Network** window.

h. In the **Gateway** field, enter the IP address or network/hosts object of the gateway router, which is the next hop for this route.

i. 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. See Figure 3-7.

Figure 3-7: Example of Adding a Static Default Route



The configured routes appear as shown in Figure 3-8.

Figure 3-8: Example View of a Static Route Configured in Firepower

+ Add Route

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	OPC_UA_ServerIntf	Global	10.10.106.11	false	1	

Note: The output shown above is a sample output and a large section of output may have been omitted. For more detailed information, see "Static and Default Routes for Firepower Threat Defense" in *Firepower Management Center Configuration Guide, Version 7.0*:

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

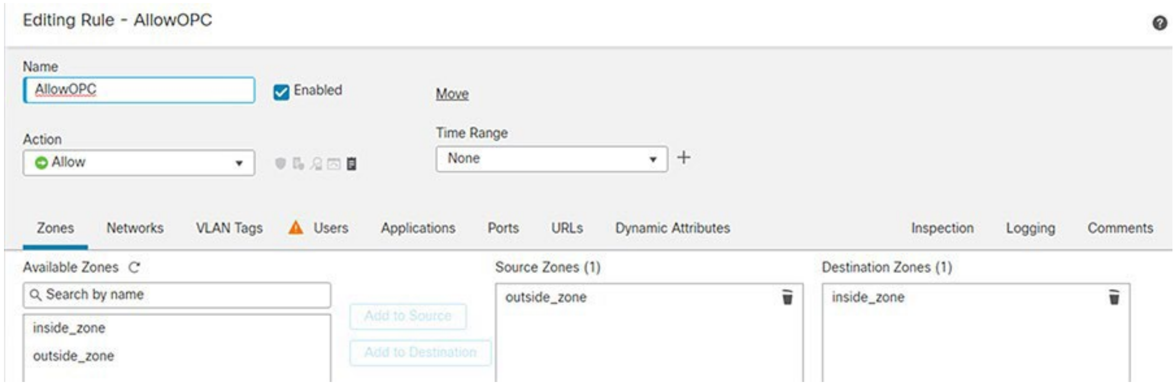
4. Perform the following actions to configure an access control policy:

An access control policy allows or disallows communication between different zones.

a. Choose **Policies > Access Control > New Policy** from the Main menu.

b. Click **Add Rule** and configure the policy. See Figure 3-9 for an example.

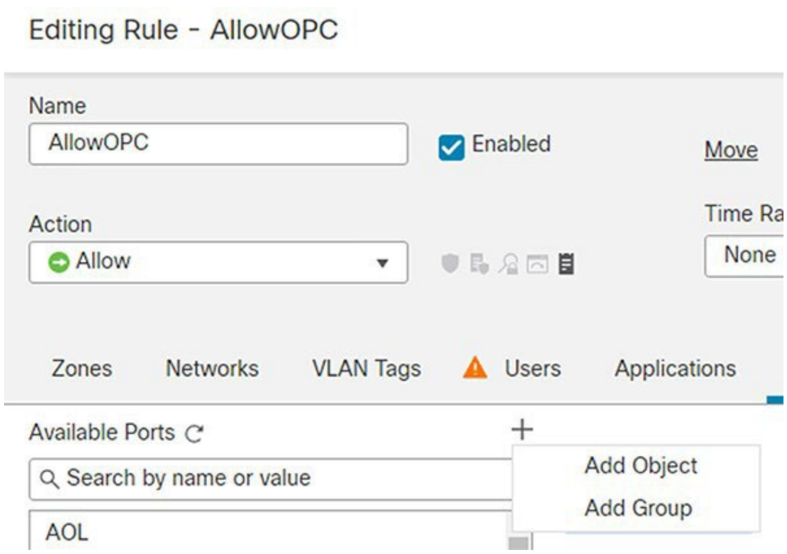
Figure 3-9: Adding an Access Control Policy



c. Choose **Edit policy > Add Rule** and add the source and destination zone for allowing communication between the OPC-UA server in a third-party network and OPC-UA client in an OSS network.

d. Under **Ports**, create a port object by clicking **+ > Add object** and then entering details for the port objects, as shown in Figure 3-10.

Figure 3-10: Creating a Port Object

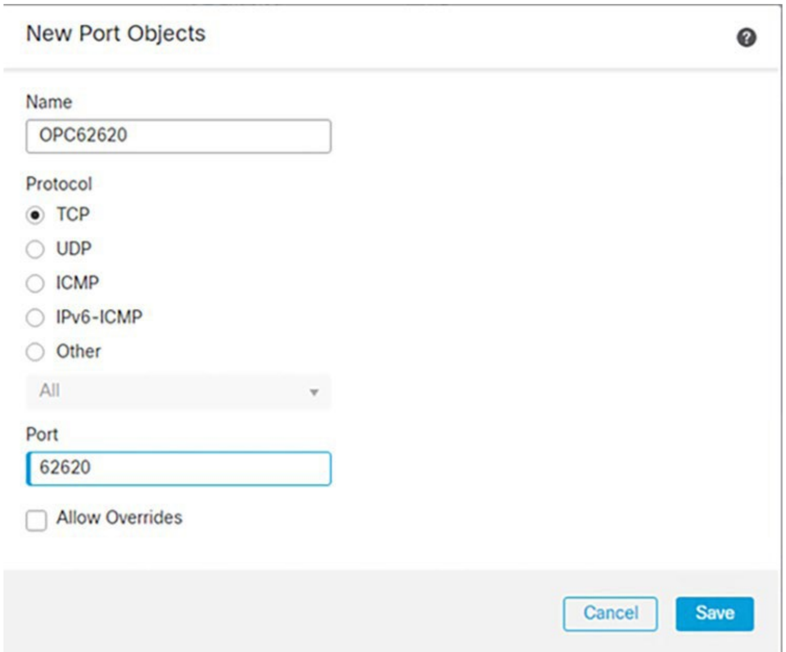


e. For OPC UA communication, create a port object with the following UDP ports:

48010
49320
53530
62620
62626

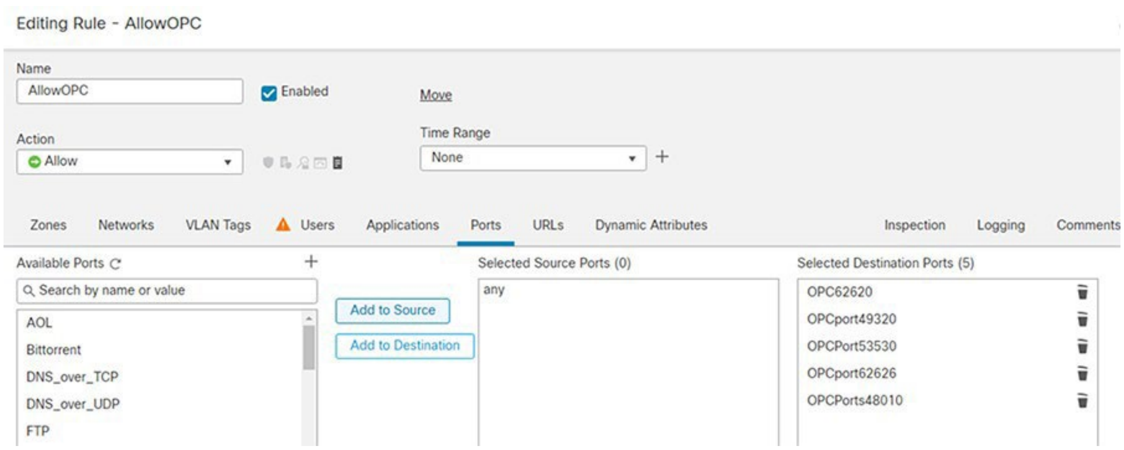
See Figure 3-11 for an example.

Figure 3-11: Adding Ports Objects



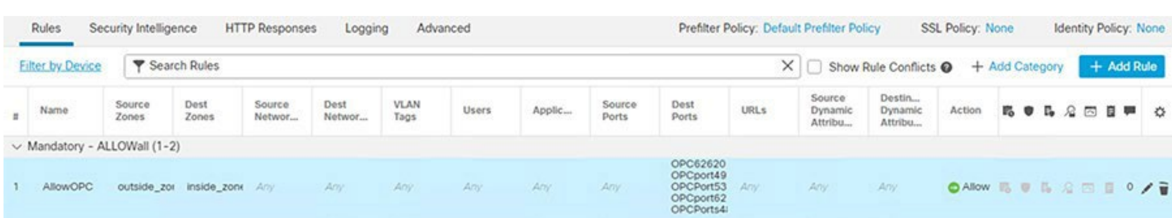
f. Choose any item from the **Available Ports** window as the source port, choose the ports that you created in Step 4e as the destination ports, and click **Save**. See Figure 3-12.

Figure 3-12: Adding Access Control Policy



g. Click **Deploy**.

Figure 3-13: Rules Configured Under Access Control Policy



Chapter 4: Farm Area Network Implementation

This chapter describes how to manually bring up a farm area network (FAN) ring in a wind farm by using switch CLI commands. You also can perform this procedure by using the Cisco Catalyst Center REP provisioning workflow, which simplifies the configuration and management of devices (see Onboard TAN Switches).

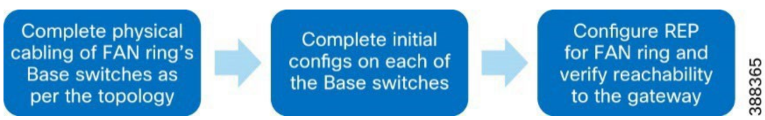
This chapter includes the following topics:

- Configuring a Farm Area Network Ring
- Configuring a Turbine Area Network

Configuring a Farm Area Network Ring

Figure 4-1 shows the workflow for bringing up a farm area network (FAN) ring.

Figure 4-1: FAN Ring Bring-up Workflow



FAN Ring Topology and REP Ring Configuration

After completing physical connections for bringing up FAN ring, configure each of the 3400 switches as follows to create VLANs and bring up the management interface:

hostname *name*
vlan 101
name Management_vlan
vlan 105
name REP_ADMIN_VLAN
rep admin vlan 105
interface Vlan101
ip address dhcp
interface range gi 1/1-2
switchport mode trunk

A sample configuration for a 3400 switch is as follows:

```
hostname FAN-BS1
vlan 101
name Management_vlan
vlan 105
name REP_ADMIN_VLAN
interface Vlan101
ip address dhcp
rep admin vlan 105
```

Configuring REP for the FAN Ring

REP configuration for the FAN ring is done with the 9300 aggregation switch interface as the edge port. The configuration in the FAN ring must be performed in either the clockwise or counterclockwise direction.

1. Enter the following commands on the 9300 aggregation switch:

   Conf t
   Vlan 105
   Rep admin vlan 105
   Int range Te 1/1/2,2/1/2

Rep segment 1 edge

2. Configure the neighboring 3400 switches in either a clockwise or counterclockwise direction by entering the following commands on each switch:

   Conf t
   Rep admin vlan 105
   Int range gi 1/1-2
   Rep segment 1

2. Replicate this 3400 configuration on all 3400 switches of the FAN ring sequentially in the direction chosen in Step 2.
3. After all switches in the FAN ring are configured, verify REP by entering the s**how rep topology** CLI command in any of the member switches.

For more detailed information about REP configuration, see *REP Command Reference*:

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_chapter_0111.pdf

Configuring a Turbine Area Network

Configuring Turbine Area Network without High Availability

A turbine area network (TAN) without high availability is configured by linearly by connecting a 3400 switch to a node of the FAN ring using two links that are formed into a port-channel. The port-channel provides redundancy.

Here is a sample configuration on a base switch that forms part of the TAN:

```
!
int range gi 2/1-2
channel-group 3 mode desirable
switchport mode trunk
switchport trunk allowed vlan 1-2507,2509-4094
```

The same base switch configuration must be repeated on the TAN switches on the interfaces that connect to the base switch.

Configuring TAN with High Availability and REP Subtended Ring

TAN high availability with a REP subtended ring is created with two kinds of REP segments:

- REP closed segment (TAN2): In this type of REP ring, the primary and secondary edges of the REP reside on the same switch
- REP open segment (TAN3): In this type of REP ring, the primary and secondary edge of the REP reside on different switches

TAN2 Ring Configuration

A TAN2 ring is formed similarly to the FAN ring with edge ports configured on the base switch, as shown in the wind farm topology in figure 2-1. Switches should be configured as follows:

- Base switch configuration:

```
Int range Te 1/1/1,2/1/1
Rep segment 2 edge
rep stcn segment 1 /* to send a segment TCN for this new segment in the main REP ring
segment*/
```

- TAN switch configuration:

```
Rep admin vlan 105
Int range gi 1/1-2
Rep segment 2
```

- TAN3 ring configuration (REP open segment).

  TAN3 ring is formed similarly to the FAN ring, except that the edge port is configured on two different 3400s.

```
FAN-BS4#conf  t
Int range Gi 2/1
Rep segment 3 edge
rep stcn segment 1
FAN-BS3#conf t
```

```
Int range Gi 2/1
Rep segment 3 edge
rep stcn segment 1
TAN3-BS1#conf t
Rep admin vlan 105
Int range gi 1/1-1/2
Rep segment 3
```

Chapter 5: Implementing OSS Infrastructure Applications and Services

This chapter includes the following topics:

- Cisco Cyber Vision Center Local Installation and Configuration
- Cisco Stealthwatch Flow Collector Installation and Configuration
- SCADA OPC-UA Server Installation and Configuration
- Cisco Cyber Vision Sensor installation on a 9300 Switch to Detect OPC-UA Traffic

Cisco Cyber Vision Center Local Installation and Configuration

This section describes the deployment of Cisco Cyber Vision Center (CVC) local in an offshore substation infrastructure network, and the deployment of network sensors on IE3400 Series switches in the TAN and FAN.

Cisco Cyber Vision Center Installation

CVC can be deployed as a virtual machine (VM) or as a hardware appliance. In Figure 2-1, Cyber Vision Center (local) is deployed as a VM on a Cisco Unified Computing System (UCS) in the OSS infrastructure network. After CVC (local) is installed, it is registered with Cyber Vision Global Center in the control center for centralized management and monitoring.

For CVD installation instructions and resource recommendations, see *Cisco Cyber Vision Center VM Installation Guide, Release 4.1.2*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Center-VM/Release-4-1-2/b_Cisco_Cyber_Vision_Center_VM_Installation_Guide.html

We recommended that the CVC application be installed in the OSS network with dual interfaces, one interface for management and the other for sensor communication. The following is an example of the IP addressing schema used in the CVC installation:

- Administration interface (eth0): 10.104.206.225 (routable IP address for CVC UI access)
- Collection interface (eth1): 10.10.100.30 (OSS infrastructure VLAN)
- Collection network gateway: 10.10.100.1 (OSS infrastructure gateway)
- NTP: 10.10.100.1

See "Operational Technology Flow and Device Visibility using Cisco Cyber Vision" in

Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf?dtid=odicdc000509

for detailed design and deployment considerations for CVC and network sensors on TAN and FAN IE switches.

Configuring Cyber Vision Center Data Synchronization

To synchronize local CVC data with CVC Global in the control center, follow the instructions in "Configure Center data synchronization" in *Cisco Cyber Vision Center VM Installation Guide, Release 4.1.2*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Center-VM/Release-4-1-2/b_Cisco_Cyber_Vision_Center_VM_Installation_Guide/m_Configure_the_Center_CENTER_VM_v3_4_0_0.html#topic_5397

Cisco Stealthwatch Flow Collector Installation and Configuration

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

The Stealthwatch Management Console (also known as Stealthwatch Manager) and Stealthwatch Flow Collector (SFC) are deployed as virtual appliances on ESXI hosts in the wind farm control center and OSS infrastructure, respectively. Install the SMC in the control center before installing the SFC in the OSS infrastructure network.

For more detailed information about Stealthwatch design, see "Cisco Secure Network Analytics (Stealthwatch)"in

Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf?dtid=odicdc000509

For information about installing the SMC and SFC Virtual Edition without datastore see *Cisco Secure Network Analytics Virtual Edition Appliance Installation Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_4_2_VE_Appliance_Installation_Guide_DV_1_3.pdf

For information about configuring the SMC and SFC Virtual Edition without datastore, see *Cisco Secure Network Analytics System Configuration Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_4_2_System_Configuration_Guide_DV_1_2.pdf

Note: Make sure to register the SFC with the SMC after the flow collector is installed and configured with basic network settings.

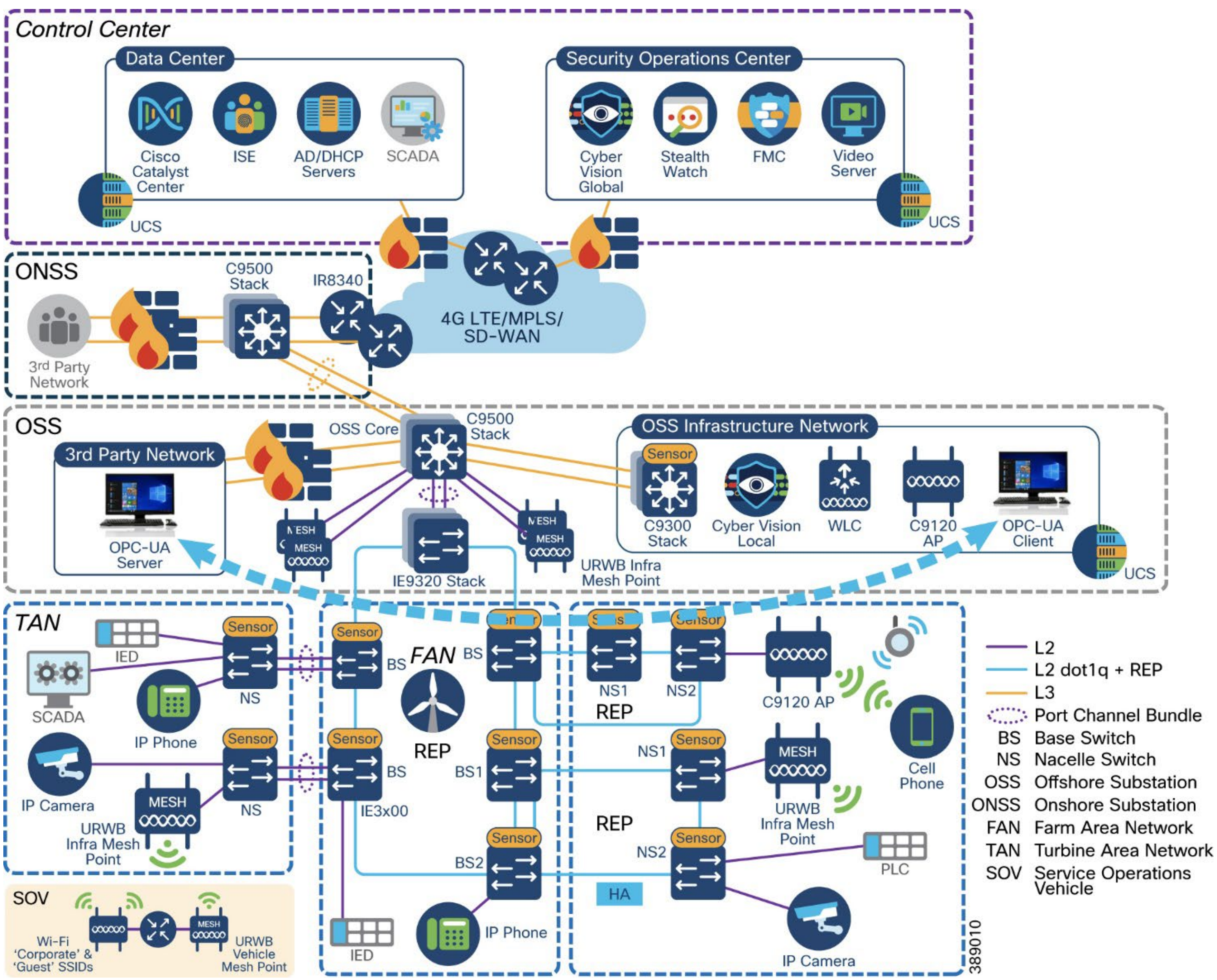
Note: Make sure to activate Cisco Smart Software Licensing for the SNA appliances (SMC and SFC) after the installation and configuration. For information about SNA licensing, see *Cisco Secure Network Analytics Smart Software Licensing Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/license/7_4_2_Smart_Software_Licensing_Guide_DV_1_0.pdf

SCADA OPC-UA Server Installation and Configuration

As shown in Figure 5-1, ports 48010, 49320, 53530, 62620, and 62626 must be allowed for Firepower for successful OPC-UA communication between the OPC-UA server and OPC-UA client.

Figure 5-1: OPC-UA Server in Third-Party Network and OPC-UA Client in OSS Infrastructure Network



The OPC-UA client application provides the following options for OPC-UA client/server communication:

- Anonymous and unsecure OPC-UA packet simulation
- Username and password-based secure OPC-UA
- x.509 certificate based secure OPC-UA communication between a client and server

Figure 5-2 shows a Wireshark trace of the OPC-UA packet flow. It begins with an OPC-UA hello message from the client, when the simulated OPC-UA packets are sent from server to the client. The OPC-UA client application can connect to the OPC-UA server application via HTTP and TCP over secure and unsecure communication media.

Figure 5-2: OPC-UA Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
936	135.915848	10.10.100.5	10.10.100.11	OpcUa	140	Hello message
937	135.946843	10.10.100.11	10.10.100.5	OpcUa	82	Acknowledge message
938	135.947761	10.10.100.5	10.10.100.11	OpcUa	186	OpenSecureChannel message: OpenSecureChannelRequest
939	135.957329	10.10.100.11	10.10.100.5	OpcUa	189	OpenSecureChannel message: OpenSecureChannelResponse
940	135.959055	10.10.100.5	10.10.100.11	OpcUa	1382	UA Secure Conversation Message: CreateSessionRequest
944	136.091659	10.10.100.11	10.10.100.5	OpcUa	1254	UA Secure Conversation Message (Message fragment 125)
946	136.092228	10.10.100.11	10.10.100.5	OpcUa	938	UA Secure Conversation Message: CreateSessionResponse (Message Reassembled)
948	136.093731	10.10.100.5	10.10.100.11	OpcUa	203	UA Secure Conversation Message: ActivateSessionRequest
949	136.096490	10.10.100.11	10.10.100.5	OpcUa	150	UA Secure Conversation Message: ActivateSessionResponse
950	136.096790	10.10.100.5	10.10.100.11	OpcUa	170	UA Secure Conversation Message: CreateSubscriptionRequest
951	136.125188	10.10.100.11	10.10.100.5	OpcUa	126	UA Secure Conversation Message: CreateSubscriptionResponse
952	136.125839	10.10.100.5	10.10.100.11	OpcUa	412	UA Secure Conversation Message: CreateMonitoredItemsRequest
953	136.138914	10.10.100.11	10.10.100.5	OpcUa	252	UA Secure Conversation Message: CreateMonitoredItemsResponse
954	136.139470	10.10.100.5	10.10.100.11	OpcUa	182	UA Secure Conversation Message: ReadRequest
955	136.146002	10.10.100.11	10.10.100.5	OpcUa	491	UA Secure Conversation Message: ReadResponse
956	136.146468	10.10.100.5	10.10.100.11	OpcUa	182	UA Secure Conversation Message: ReadRequest
957	136.150277	10.10.100.11	10.10.100.5	OpcUa	296	UA Secure Conversation Message: ReadResponse

OPC-UA message types and Flow

Figure 5-3 shows the OPC-UA message types from the Hello message to the close of the OPC-UA session.

Figure 5-3: OPC-UA Message Types

Any OPC-UA client application from vendors such as Unified Automation, Matricon, Kepware, and others provides options for fetching data using HTTP or TCP, as shown in Figure 5-4.

Figure 5-4: OPC-UA Client application Supporting Different Encryption Types

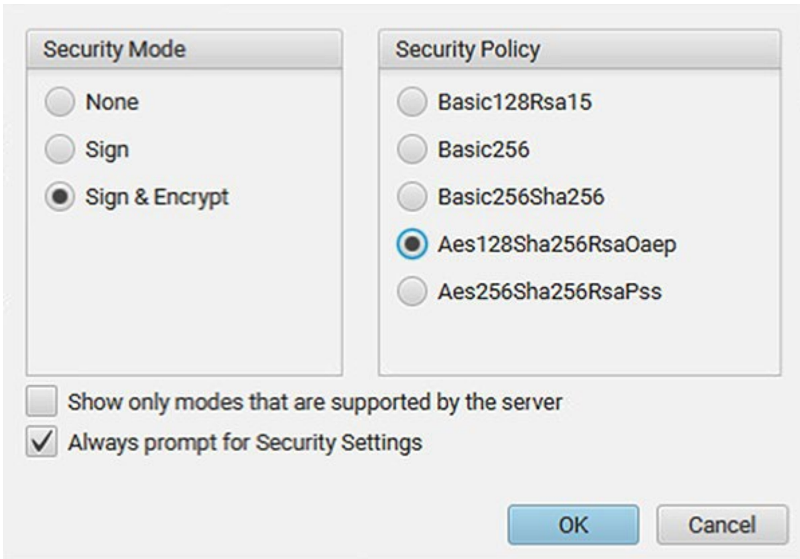


Figure 5-5 shows the OPC-UA client application fetching parameters from an OPC-UA server application over TCP.

Figure 5-5: OPC-UA Client Fetching Data from and OPC-UA Server

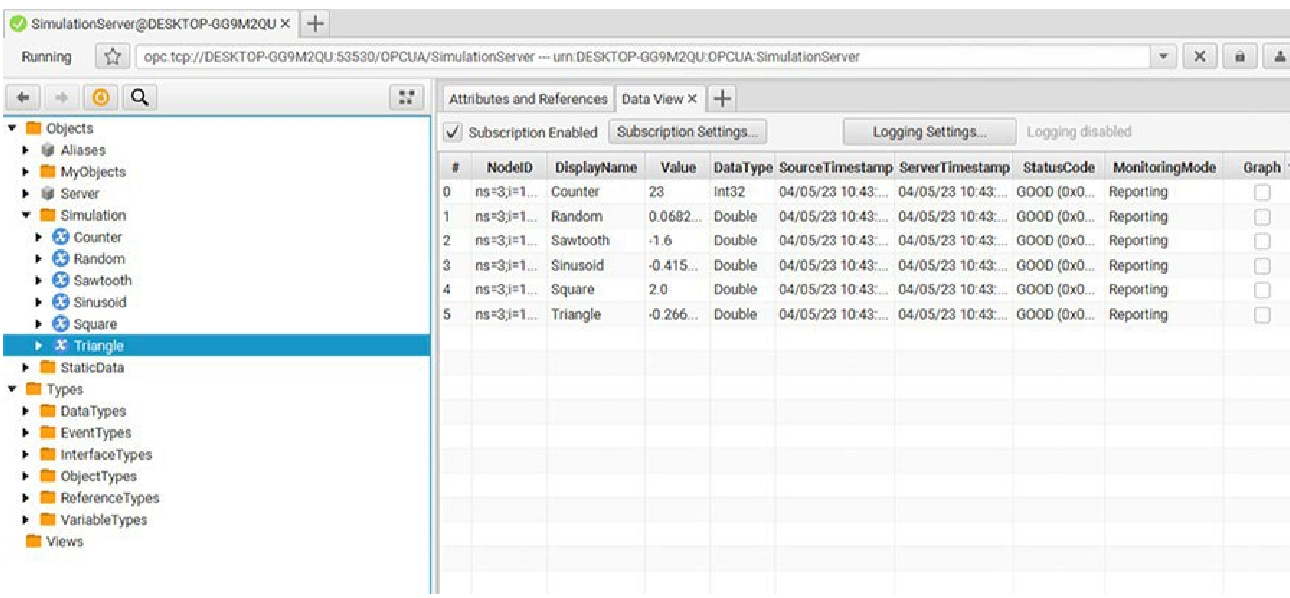


Figure 5-6 shows the Prosys OPC-UA server application provisioned to establish a connection to a server over TCP or HTTP.

Note: If an OPC-UA client application is in a different network than the distributed controlled system-process control network (DCS-PCN), there is a DNS entry in the C:\windows\System32\etc\hosts file, as shown in Figure 5-6.

Figure 5-6: OPC-UA Server

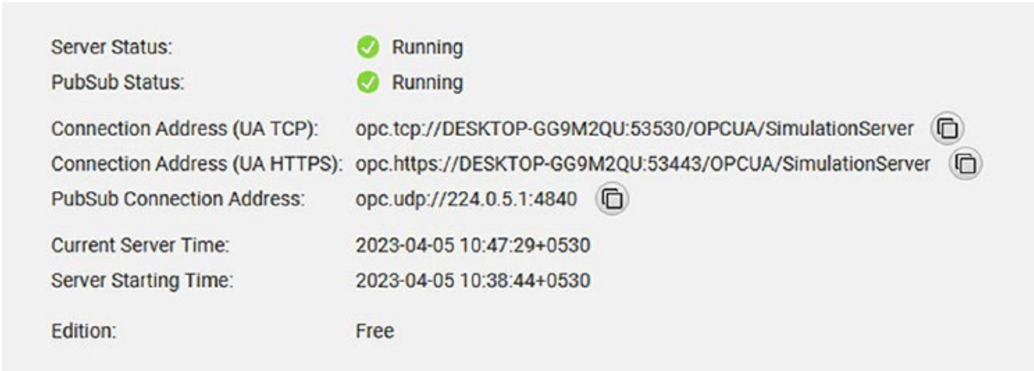
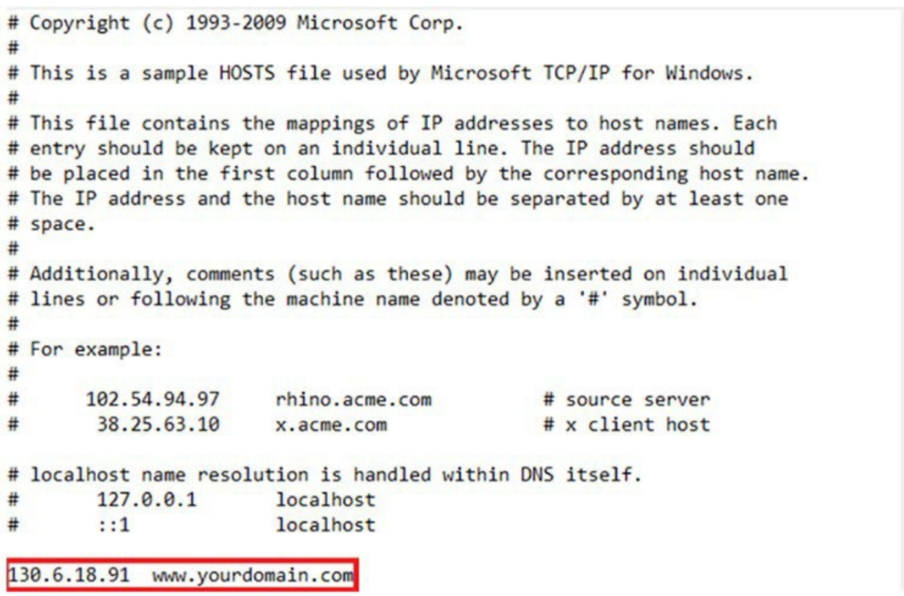


Figure 5-7 shows a hosts file that is configured with a DNS entry for an OPC-UA client connection to an OPC-UA server over TCP or HTTP.

Figure 5-7: DNS Entry for OPC-UA Server and Client in Hosts File



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

130.6.18.91   www.yourdomain.com
```

Cisco Cyber Vision Sensor installation on a 9300 Switch to Detect OPC-UA Traffic

The general workflow for installing Cyber Vision sensors on 9300 switches is as follows:

Step 1: Mount the USB SSD on a 9300 switch and install the Cyber Vision sensor application on the mounted drive.

Step 2: Configure the Cyber Vision sensor application on the 9300 switch so that OPC-UA traffic can be detected.

Step 3: Install the Cyber Vision sensor on the 9300 switch from the Cyber Vision Center.

Step 4: Edit the yaml file on the 9300 switch and add OPC-UA ports.

Step 5: Verify the OPC-UA flow in Cisco Cyber Vision Center.

These steps are described in detail in the following sections.

Step 1: Mount the USB SSD on a 9300 Switch and Install the Cyber Vision Sensor Application on the Mounted Drive

To install the CVC sensor application on a 9300 switch, mount the USB SSD on the switch and install the CVC sensor application on the USB-SSD drive. For more detailed instructions, see “Installing a USB 3.0 SSD” in *Cisco Catalyst 9300 Series Switches Hardware Installation*

Guide:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/m_9300_installing_a_usb30ssd.html

After you install the CVC sensor application, verify that the switch can reach the Cyber Vision Center by pinging the CVC collection of IP address from the 9300 switch. Ensure that there is IP reachability to the CVC local manager instance from OSS-access on the 9300, as shown in Figure 5-8.

Figure 5-8: Ping CVC Collection IP address from C-9300

```
Password:
OSS-C9300-Access#ping 10.10.100.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
OSS-C9300-Access#
```

Step 2: Configure the Cyber Vision Sensor Application on the 9300 Switch

1. Configure the following IP addresses on the 9300 switch to bring up the Cyber Vision sensor application and integrate the switch with CVC:
   - CVC Admin Interface (eth0)
   - Collection interface (eth1)
   - Collection network gateway
   - NTP
2. Configure the IP addresses in Cisco Cyber Vision as shown in Figure 5-9 (sample IP addresses shown).

   Figure 5-9: Cyber Vision Configuration Parameters

3. Enable iox on the C-9300 switch:

```
configure terminal
    iox
    end !
```

For more detailed information, see “Initial Configuration” steps in *Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300, Release 4.1.0*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/IE3400/b_Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300/m_Installation_procedures_IE3400_Catalyst_9300_v3_4_0_0.html#topic_5146

Step 3: Install the Cyber Vision Sensor on the 9300 Switch from the Cyber Vision Center

1. Install the Cyber Vision extension file:
   a. Download the extension (.ext file) from cisco.com.
   b. In Cyber Vision Center, choose **Admin > Extensions**.
   c. Click **Import Extension File** button and then browse to the extension file.
2. Install a sensor:
   a. In Cyber Vision Center, choose **Admin > Sensors > Sensors**.
   b. Click **Deploy Cisco Device**.
   c. In the **IP address** field, enter the IP address of the switch.
   d. In the **Port** field, enter 443 for a network sensor.
   e. In the **User** field, enter the username for logging in to the switch.
   f. In the **Password** field, enter the password that is associated with the user account on the switch.
   g. In the **Center IP field**, enter the IP address of the Center that the sensors should use for communication.

      For dual interface Center deployments, we recommend that you enter the eth1 IP address.
   h. Under **Capture mode**, choose options as needed to designate what data the sensor processes.

      In this validation, the **Optimal (default)** option was selected.
   i. Click **Deploy**.
3. Configure the additional options that appear:
   a. In the **Capture IP address** field, enter the ERSPAN destination IP address for the sensor.
   b. In the **Capture prefix length** field, enter the prefix that is associated with the ERSPAN IP address.
   c. In the **Capture VLAN number** field, enter the monitoring session destination VLAN.
   d. In the **Collection IP address** field, enter the IP address of the eth0 interface of the sensor.

      This IP address is used for communication with the CVC.
   e. In the **Collection prefix length** field, enter the prefix that is associated with the sensor IP address.
   f. In the **Collection gateway** field, enter the IP address of the gateway that the sensor should use for communicating through the network.
   g. In the **Collection VLAN number** field, enter the VLAN of the sensor IP address.
   h. 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:
      i. 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 that you wish to discover. If active discovery is necessary on the same subnet as the sensor itself, you can click the **USE COLLECTION** button.
      ii. In the **Prefix length** field, enter the prefix associated with the IP address.
      iii. In the **VLAN** field, enter the VLAN for the subnet.
   i. (Optional) Click the **ADD ONE** button to configure another Active Discovery interface. This secondary interface should be configured for performing active discovery on a different subnet than what was specified for the first interface.
   j. Click **deploy**.

For more information about Cyber Vision sensor installation on a 9300 switch, see “Procedure with the Cyber Vision sensor management extension” in *Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300, Release 4.1.0*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/IE3400/b_Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300/m_Installation_procedures_IE3400_Catalyst_9300_v3_4_0_0.html#topic_5701

Figure 5-10 shows the sensor installation from CVC on a 9300 using the extension method.

Figure 5-10: Cyber Vision Installation via Extension

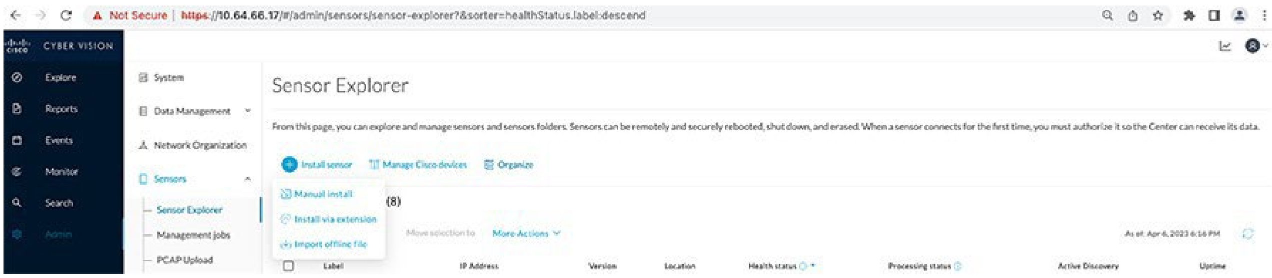
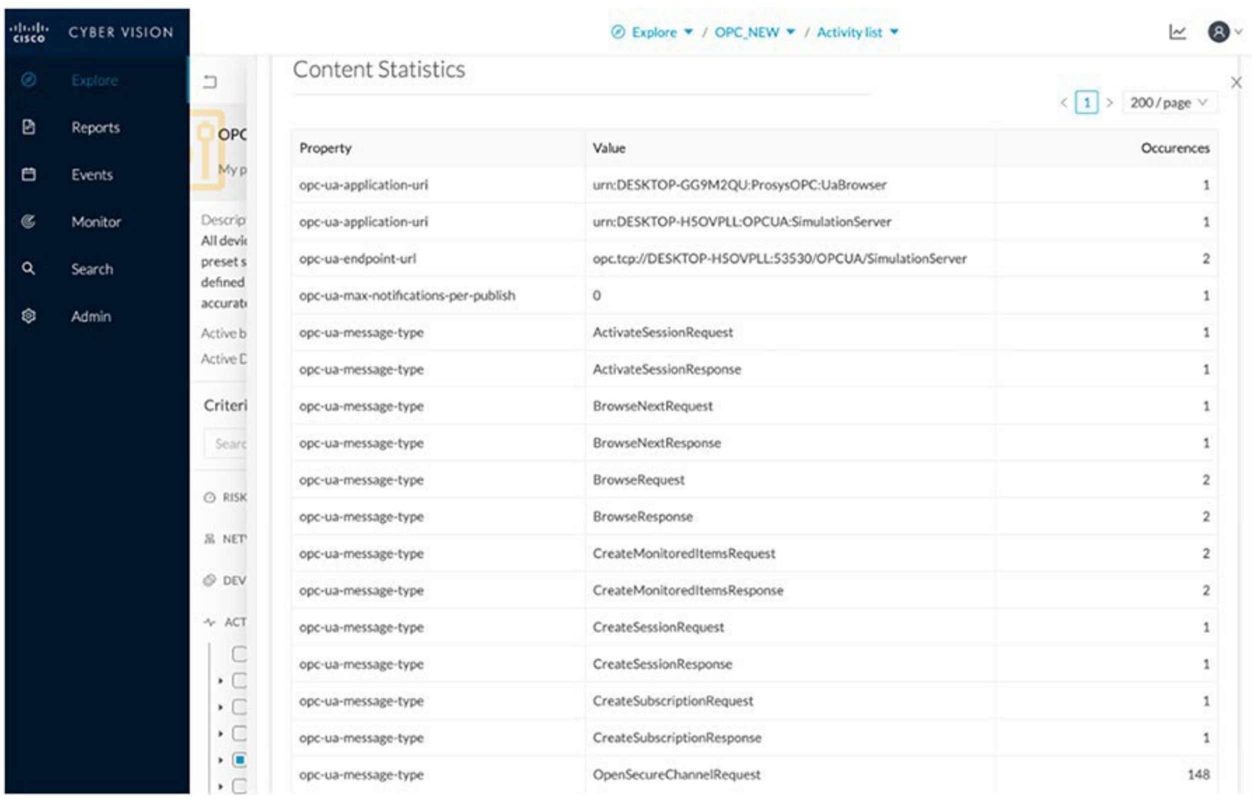


Figure 11 shows the status of the sensor deployment on the CVC Dashboard after completing the installation.

Figure 5-11: Cyber Vision Installation Completion Display on CVC Dashboard



Step 4: Edit the yaml File on the 9300 Switch and Add OPC-UA Ports

OCP-UA ports must be added to the CVC sensor for the detection of the OPC-UA flows and traffic.

1. Update the /iox_data/etc/flow/config.yaml file on the 9300 switch to add the required ports.

   The following example shows ports 48010, 49320, 53530, 62620, and 62626 added in the config.yaml file.

```
OSS-C9300-Access#app-hosting connect appid ccv_sensor_iox_x86_64  session
sh-5.0# cd /iox_data/etc/flow/
sh-5.0# vi  config.yml
gopacket:
```

```
  opcua:
    mapping: tcp:4840, tcp:51210,
tcp:12403,tcp:49320,tcp:53530,tcp:62626,tcp:48010,tcp:62620
```

2. Enter the following command to reload the 9300 switch:

   flowctl reload

Step 5: Verify the OPC-UA Flow in Cyber Vison Center

From the Cyber Vision Center Dashboard, verify that the OPC-UA flow is as shown in the following figures.

Figure 5-12 shows OPC-UA frame types in the Cyber Vision Center Dashboard.

Figure 5-12: OPC-UA Frame Types in CVC Dashboard

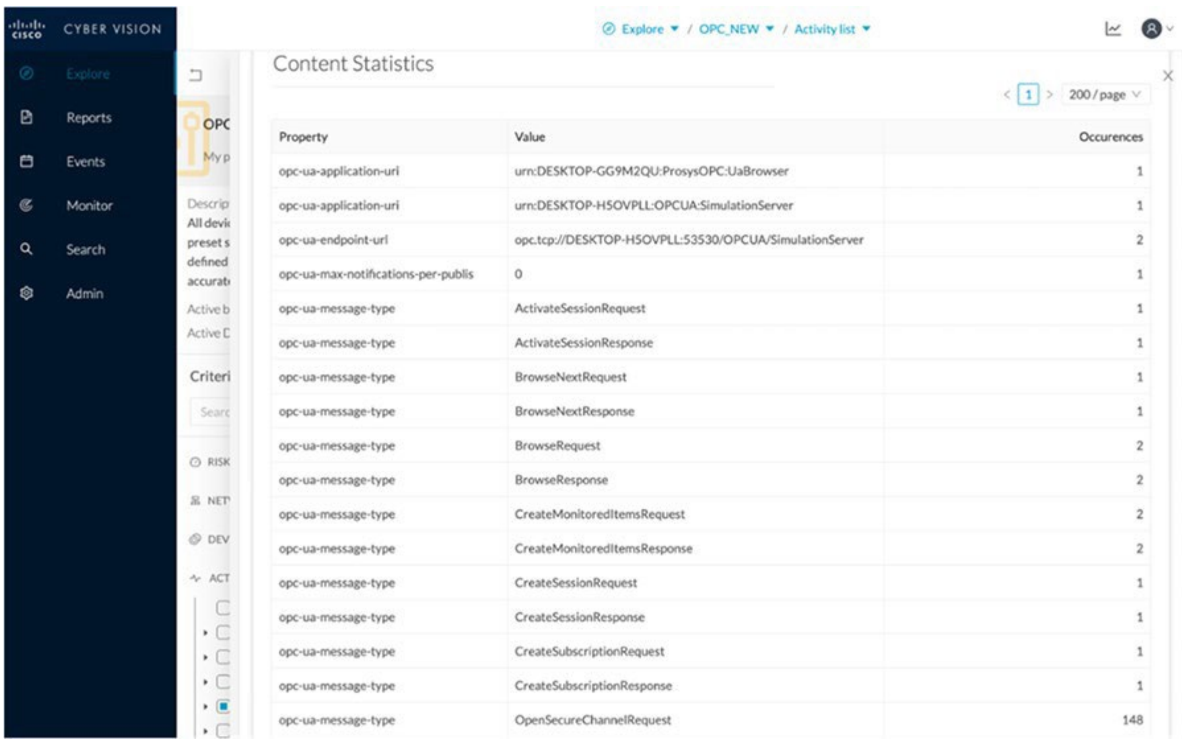
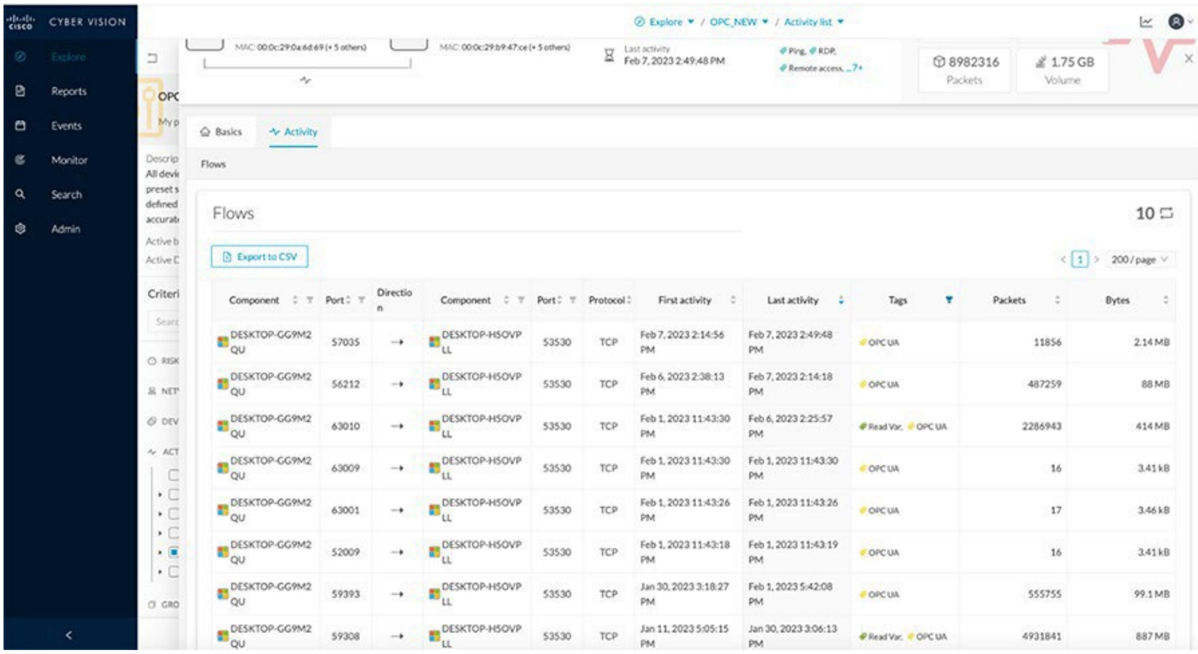


Figure 5-13 shows a more detailed view the OPC-UA traffic flow on the Cyber Vision Center dashboard.

Figure 5-13: OPC-UA Flow Detail in CVC Dashboard



Chapter 6: Implementing the Onshore Substation Network

This chapter includes the following topics:

- Onshore Substation (ONSS) Core Network Implementation
- Configuring ONSS Infrastructure Network Access
- OSS Network DMZ with Firewall

Onshore Substation (ONSS) Core Network Implementation

This section describes the steps for configurating the OSS network of the wind farm topology.

Catalyst 9500 StackWise Virtual

Configure Catalyst 9500 StackWise Virtual (SVL) switch by following the steps in Catalyst 9500 StackWise Virtual. Also complete the SVL mode configuration, layer 2 configuration, layer 3 configuration, and port-channel configuration by using the steps that are described in Chapter 3: Offshore Substation Network Implementation. After completing these configurations, enter the following CLI commands to enable ONSS and OSS network reachability to the WAN edge router:

Here is an example of a completed routing (L3) configuration for 9500 SVL switch of the ONSS:

```
interface Loopback0
 ip address 192.168.5.1 255.255.255.255
!
vlan 2001

interface Vlan2001
 vrf forwarding Management_VRF
 ip address 10.201.201.2 255.255.255.0
!
router eigrp 2001
 !
 address-family ipv4 vrf Management_VRF
  redistribute connected
  redistribute bgp 1 metric 100 1 255 1 1500
  network 10.201.201.0 0.0.0.255
  autonomous-system 900
 exit-address-family
!
!
router ospf 1
 router-id 192.168.5.1
 network 172.16.1.0 0.0.0.3 area 0
 network 192.168.2.1 0.0.0.0 area 0
 network 192.168.5.1 0.0.0.0 area 0
 network 192.168.7.1 0.0.0.0 area 0
!
vrf definition Management_VRF
 rd 100:1
 !
 address-family ipv4
  route-target export 100:1
  route-target import 100:1
  route-target export 100:1
 stitching
  route-target import 100:1
 stitching
 exit-address-family
 !
 address-family ipv6
```

```
  route-target export 100:1
  route-target import 100:1
  route-target export 100:1
 stitching
  route-target import 100:1
 stitching
 exit-address-family
!
vlan configuration 11
 member vni 5000
!
interface Vlan11
 vrf forwarding Management_VRF
 ip unnumbered Loopback0
 no autostate
!
interface Vlan201
 vrf forwarding Management_VRF
 ip address 10.10.201.1
 255.255.255.0
!
interface nve1
 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 5000 vrf Management_VRF
!
router bgp 1
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 192.168.5.2 remote-as 1
 neighbor 192.168.5.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn evpn
  neighbor 192.168.5.2 activate
  neighbor 192.168.5.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf
 Management_VRF
  advertise l2vpn evpn
  redistribute static
  redistribute connected
  redistribute eigrp 900
 exit-address-family
 !
 address-family ipv6 vrf
 Management_VRF
  redistribute connected
  redistribute static
  advertise l2vpn evpn
 exit-address-family
 !
```

Verify EVPN VXLAN BGP Core routing between OSS and ONSS core switches:

```
WF-ONSS-9500#show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag
```

```
Interface
192.168.5.2              0     100       0 ?
 * i                    192.168.5.2              0     100       0 ?
     Network     VNI       Type Peer-IP           RMAC/Num_RTs    eVNI      state flags UP time
nve1       5000     L3CP 192.168.5.2      a4b2.392a.9554 5000       UP   A/M/4 3w6d
!
WF-ONSS-9500#show bgp l2vpn evpn all
BGP table version is 67, local router ID is 192.168.7.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf Management_VRF)
 * i  [5][100:1][0][16][172.114.0.0]/17
                      192.168.5.2              0     100       0 ?
 *>i                   192.168.5.2              0     100       0 ?
 * i                   192.168.5.2              0     100       0 ?
 * i  [5][100:1][0][24][10.10.1.0]/17
                      192.168.5.2              0     100       0 ?
 *>i                   192.168.5.2              0     100       0 ?
 * i                   192.168.5.2              0     100       0 ?
 * i  [5][100:1][0][24][10.10.100.0]/17
                      192.168.5.2              0     100       0 ?
 *>i                       Next Hop            Metric LocPrf Weight Path
*>   [5][100:1][0][24][10.10.201.0]/17
                      0.0.0.0                  0          32768 ?
!
WF-ONSS-9500#ping vrf Management_VRF 10.10.100.1 source vlan 201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.201.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WF-ONSS-9500#
```

Configuring ONSS Infrastructure Network Access

Configure the ONSS C9300 stack by following the steps in Configuring OSS Infrastructure Network Access.

Similarly, configure C9300 aggregation, if required, by following the steps in Configuring FAN Ring Aggregation Switch Stack.

OSS Network DMZ with Firewall

Cisco Next Generation Firewall (NGFW) Implementation

Configure Firepower by following the steps for the OSS layer in Cisco Firepower Next Generation Firewall (NGFW) Implementation.

Turbine Vendor OPC-UA client

The OPC-UA client connects to the OPC-UA server by using either Open, a username and password, or AES-128/256 security keys.

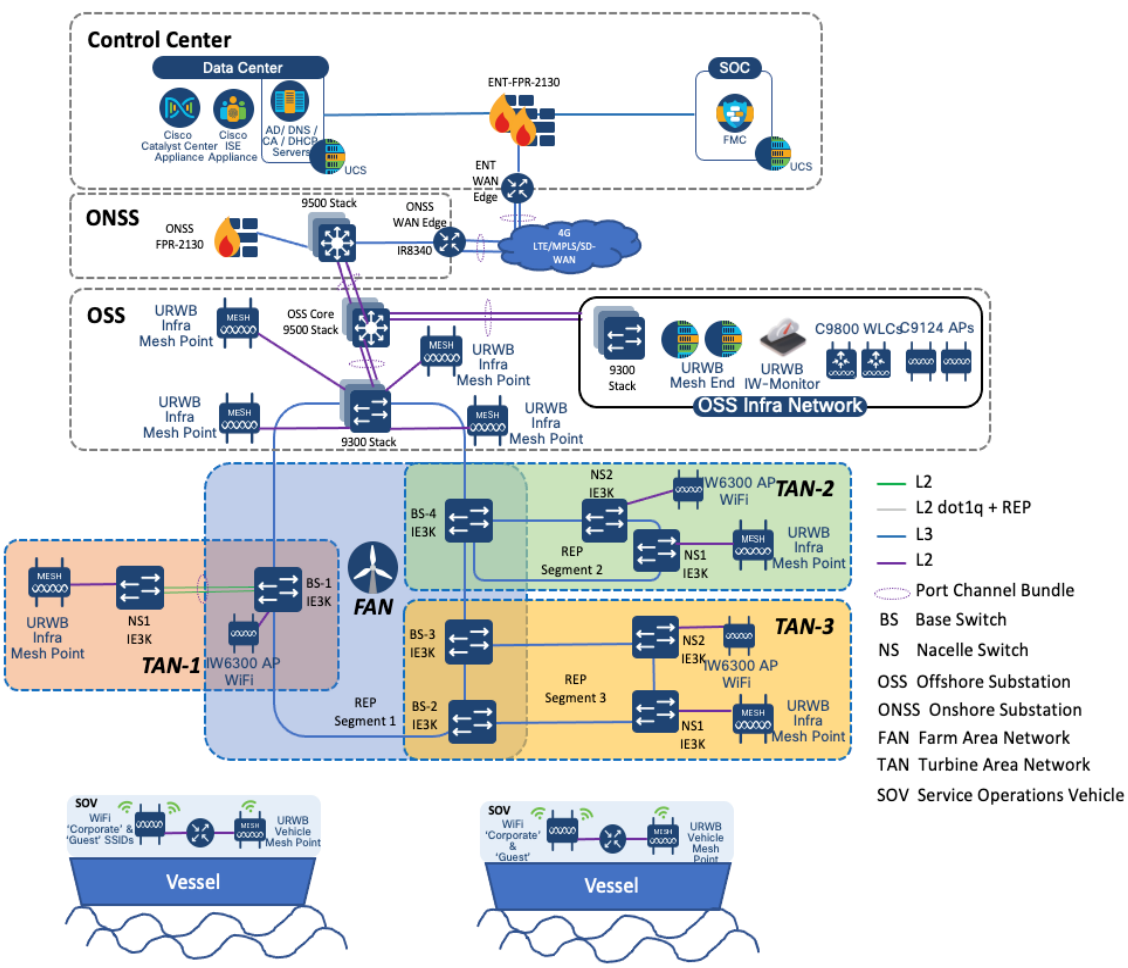
Chapter 7: Implementing Wireless Access Networks

This chapter includes the following topics:

- Offshore Wind Farm Wi-Fi Implementation
- Operating the Wireless Network
- Offshore Wind Farm URWB Implementation for SOV to OSS Connectivity

Figure 7-1 shows the overall wireless deployment architecture for offshore wind farm Wi-Fi access and URWB for vessel-to-OSS connectivity.

Figure 7-1: Offshore Wind Farm Wireless Architecture

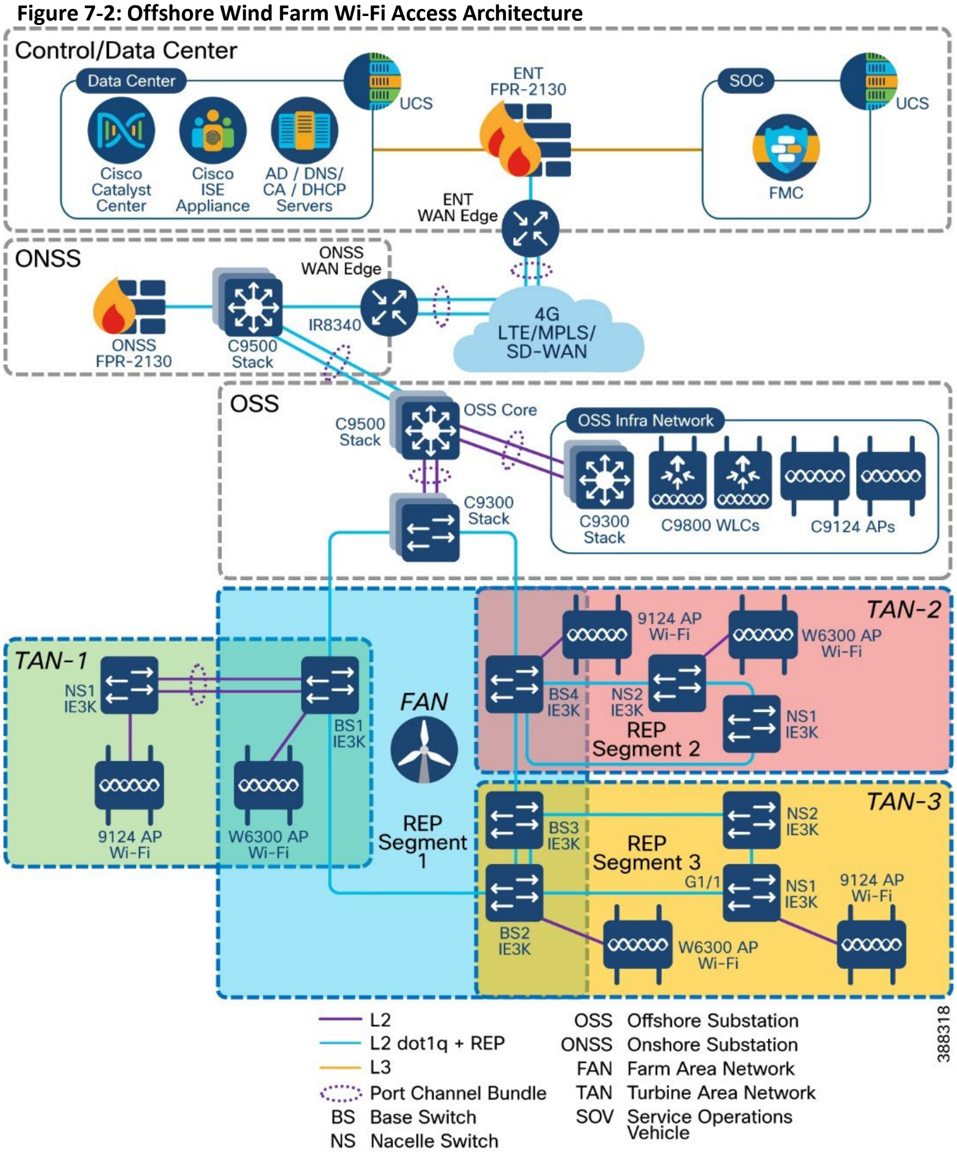


Offshore Wind Farm Wi-Fi Implementation

This section provides implementation details for offshore wind farm Wi-Fi access. Wi-Fi implementation includes the following components:

- Cisco Catalyst Center located in the control center is used to configure and manage the Wi-Fi deployment
- MSFT AD is used to manage employee user identities
- ISE is used as an AAA server for centralized policy management
- Cisco Trustsec is used for segmentation
- ISE is used to host the guest wireless portal
- C9800 WLCs are used as wireless LAN controllers
- Cisco 9124 or Cisco IW6300 Ruggedized APs can be deployed in local mode on the OSS, FAN, and TAN as needed

Figure 7-2: Offshore Wind Farm Wi-Fi Access Architecture



For detailed implementation about Cisco Catalyst Center non-fabric wireless deployment, see *Catalyst 9800 Non-Fabric Deployment using Cisco Catalyst Center*:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Catalyst-9800-Non-Fabric-Deployment-using-Cisco-DNA- Center.pdf

Configuring C9800 WLC High Availability from Cisco Catalyst Center

Catalyst 9800 Series WLCs can be configured in an active/standby high availability (HA) stateful switch-over (SSO) pair. Cisco Catalyst Center supports the ability to take two controllers of the same model, running the same OS version, and configure them into an HA SSO pair.

To configure the Catalyst 9800-40 WLCs (WLC-9800-1 and WLC-9800-2) as an HA SSO pair, follow these steps:

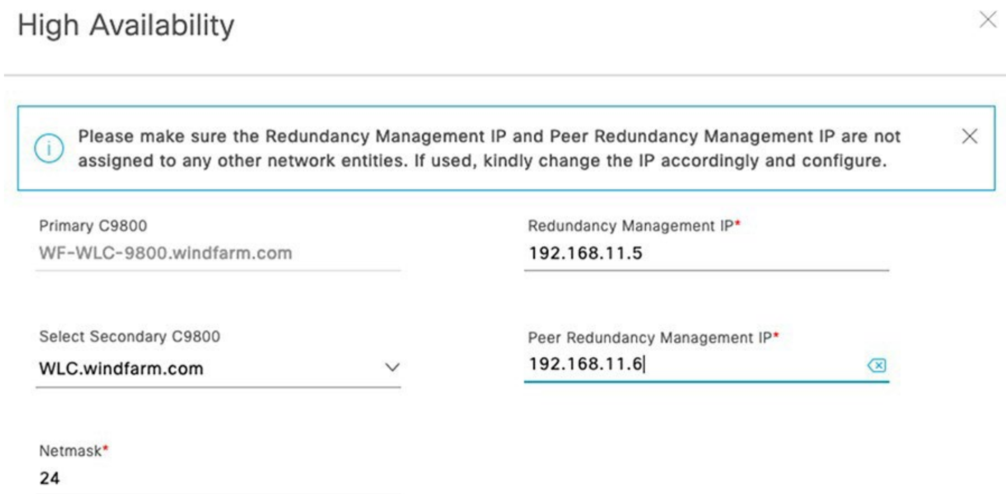
1. From the main Cisco Catalyst Center dashboard choose **Provision**.

The main provisioning screen appears, which displays the devices within the inventory. By default, the Focus: is set for **Inventory**.

2. Locate and check the check box next to the Catalyst 9800-40 WLC, which will be the primary of the HA SSO WLC pair.
3. From the drop-down menu under **Actions**, choose **Provision > Configure WLC HA**.

The **High Availability** side panel appears. An example is shown in the Fig. 7-3.

Figure 7-3: Configure C9800 WLC High Availability Using Cisco Catalyst Center



4. Enter appropriate information in the **High Availability** side panel and click **Configure HA**.

For Catalyst 9800 Series WLCs, the redundancy management IP and peer redundancy management IP addresses that need to be configured within Cisco Catalyst Center are actually the redundancy port and peer redundancy port IP addresses. These IP addresses are referred to as the local IP and remote IP addresses in the web UI of the Catalyst 9800 Series WLCs. The IP subnet for the redundancy port must be an IP subnet that is separate from any other interface on the Catalyst 9800 Series WLC. In addition, the primary and standby Catalyst 9800 Series WLCs must use the same IP subnet for the redundancy port, so the redundancy port connection must be a layer 2 connection.

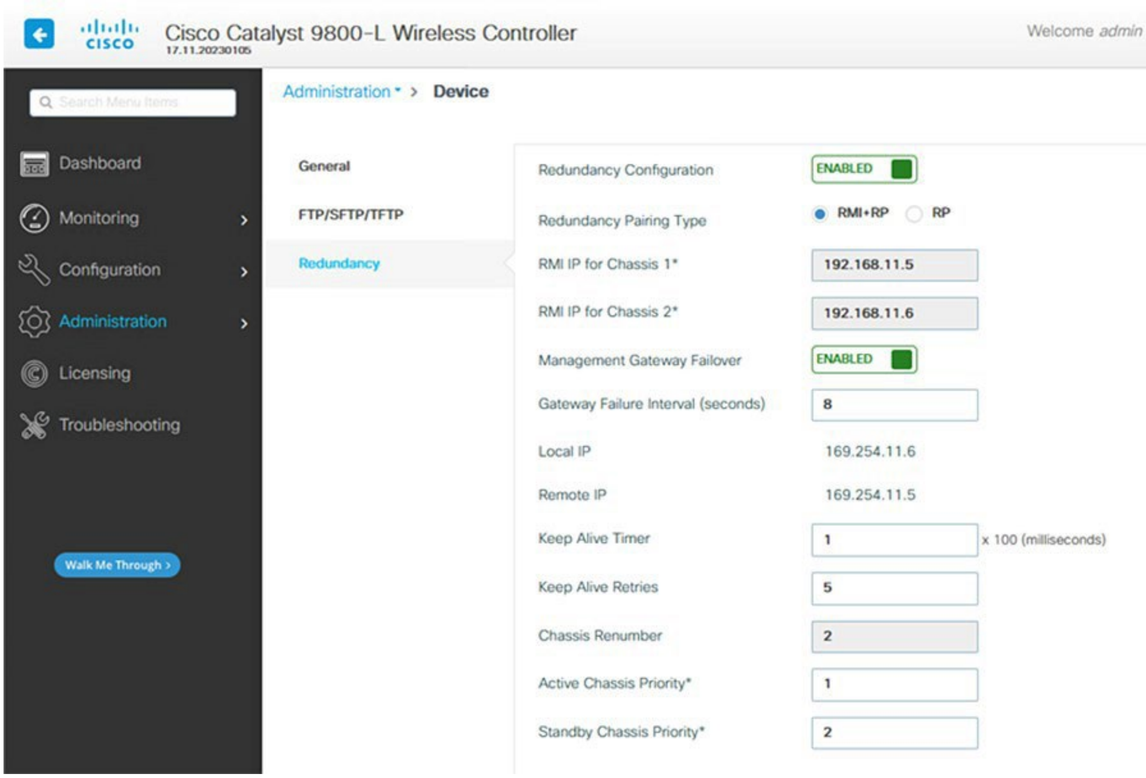
5. In the pop-up window that informs you that the WLCs will be rebooted after they are placed in high availability mode, click **OK** to continue and put the two Catalyst 9800-40 WLCs in HA SSO mode.

It takes several minutes for the WLCs to reboot and come up in HA SSO mode. All configuration from the primary Catalyst 9800-40 WLC, including the IP address of the management interface, is copied to the secondary Catalyst 9800-40 WLC. Cisco Catalyst Center then longer shows two WLCs in inventory. Instead, a single WLC HA SSO pair with two serial numbers appears in inventory.

6. Verify that the appropriate C9800 WLC SSO HA configuration is pushed down to the WLC by choosing **Administration > Device > Redundancy**.

An example is shown in Figure 7-4.

Figure 7-4: Verifying High Availability Configuration on the C9800 WLC UI



7. Verify the redundancy status on the WLC by choosing **Monitoring > General > System**.

An example is shown in Figure 7-5. You also can monitor the status on the C9800 WLC CLI by executing the **show redundancy** command as shown in Figure 7-6.

Figure 7-5: Verifying WLC High Availability Status on the WLC Monitoring Page

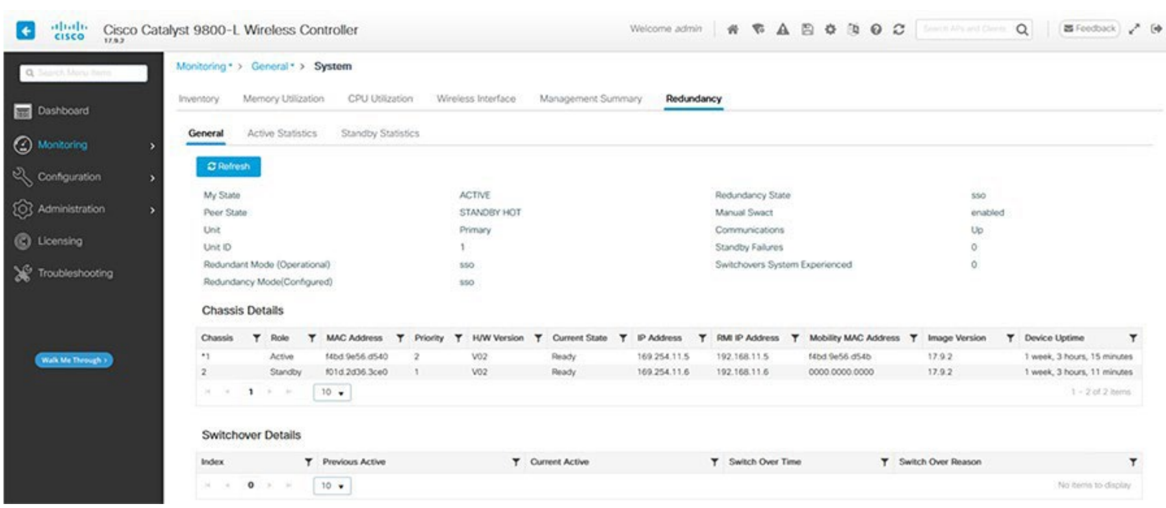


Figure 7-6: Verifying High Availability Status from the C9800 CLI

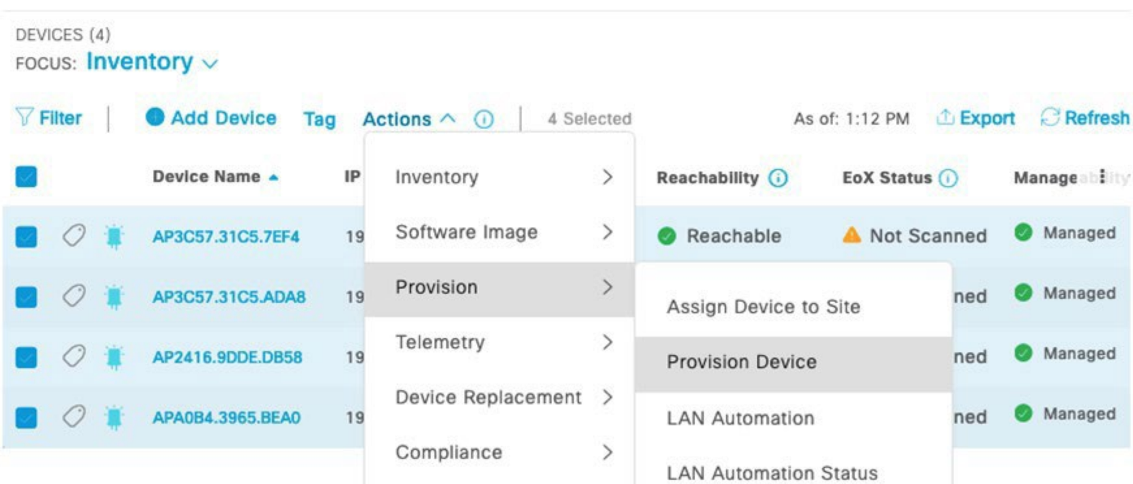
```
WF-WLC-9800#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 4 days, 2 hours, 31 minutes
Switchovers system experienced = 2
              Standby failures = 0
        Last switchover reason = active unit removed

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

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 12 minutes
                 Image Version = Cisco IOS Software [Dublin], C9800 Software (C9800_IOSXE-K9), Experimental Version 17.11.20230105:084252 [BLD
_V1711_THROTTLE_LATEST_20230105_081642:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2023 by Cisco Systems, Inc.
Compiled Thu 05-Jan-23 00:42 by mcpre
                          BOOT = bootflash:packages.conf,12;
                   CONFIG_FILE =
        Configuration register = 0x102
               Recovery mode   = Not Applicable
             Fast Switchover   = Enabled
                Initial Garp   = Enabled

Peer Processor Information :
----------------------------
              Standby Location = slot 2
        Current Software state = STANDBY HOT
       Uptime in current state = 7 minutes
                 Image Version = Cisco IOS Software [Dublin], C9800 Software (C9800_IOSXE-K9), Experimental Version 17.11.20230105:084252 [BLD
_V1711_THROTTLE_LATEST_20230105_081642:/nobackup/mcpre/s2c-build-ws 101]
Copyright (c) 1986-2023 by Cisco Systems, Inc.
Compiled Thu 05-Jan-23 00:42 by mcpre
                          BOOT = bootflash:packages.conf,12;
                   CONFIG_FILE =
        Configuration register = 0x102
```

Configuring Wi-Fi APs using Cisco Catalyst Center

This section describes the workflow for configuring APs using Cisco Catalyst Center.

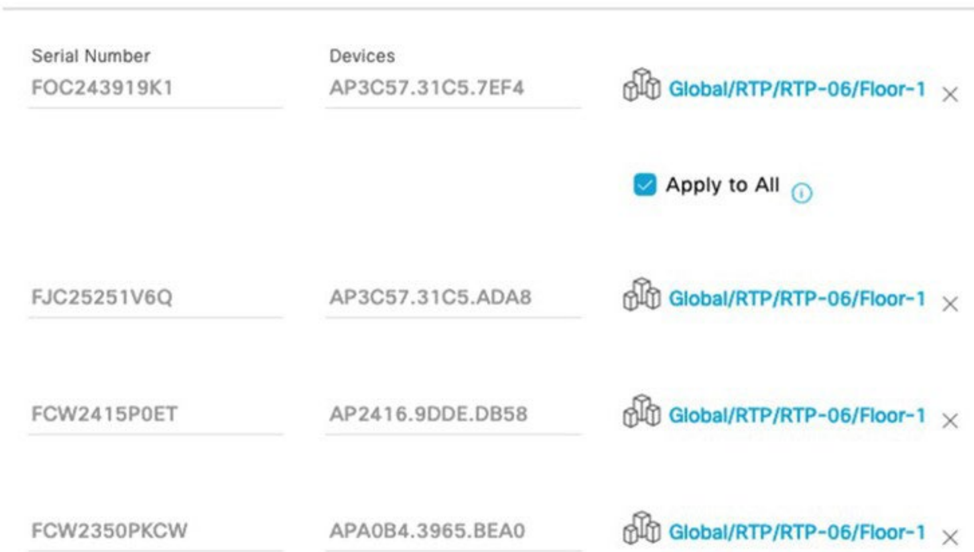
1. From the Cisco Catalyst Center Dashboard, choose **Provision > Inventory.**
2. Check the check boxes next to each AP to be provisioned and rom the corresponding drop-down menu under **Actions**, choose **Provision > Provision Device**.

Figure 7-7: Select APs to Provision



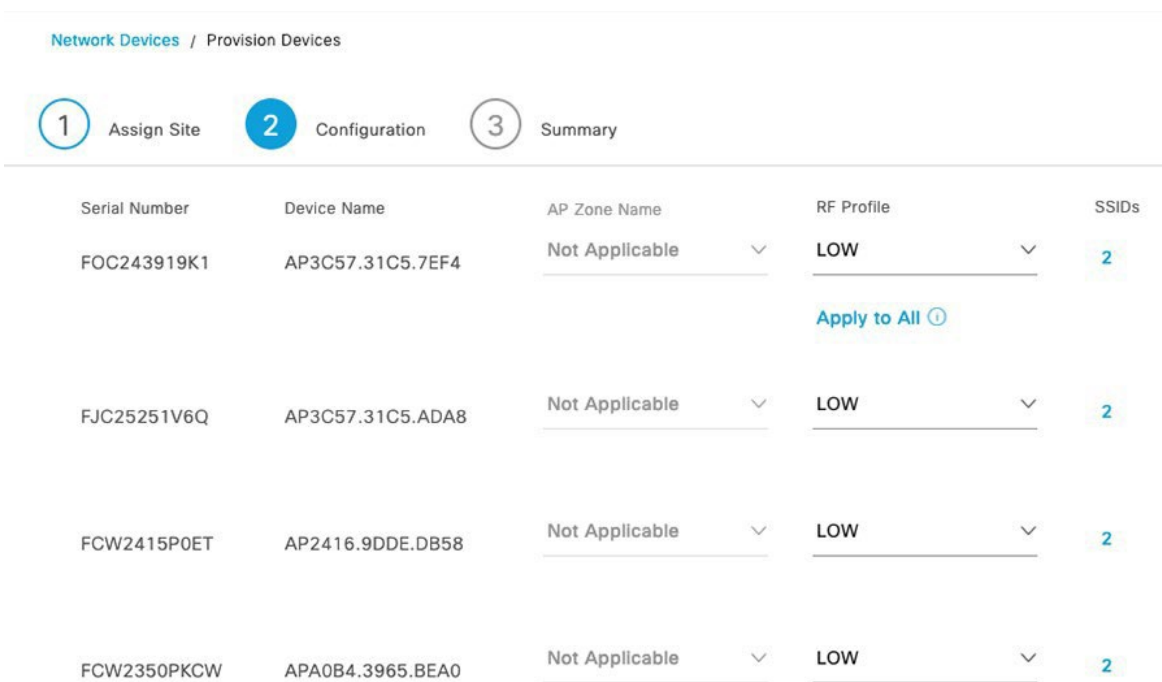
3. For each of the APs listed, click **Choose a Site**, which displays a side panel that shows the site hierarchy that is configured for Cisco Catalyst Center.

Figure7-8: Assign Each AP to a Site



4. Click **Save** to save the site assignments for the APs, then click **Next** to continue to the Configuration options.
5. From the drop-down menu in the **RF Profile** column, select the RF profile to assign to each AP.

Figure 7-9: Provisioning RF Profiles

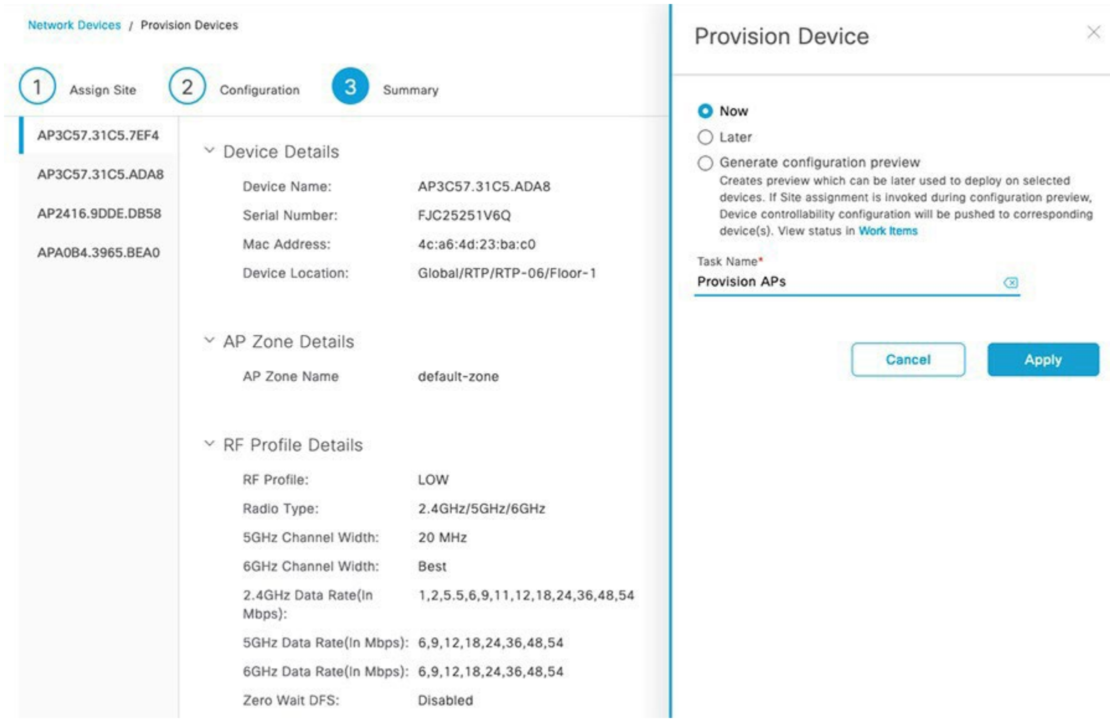


6. Click **Next** to advance to the **AP Provisioning Summary** page, and perform the following actions for each AP.

   The AP Provisioning Summary page provides a summary of the configuration to be provisioned for each AP. Click **Deploy** to provision the APs.

   Note: As a best practice, make configuration changes and provision new devices in your network during scheduled network operations change windows.

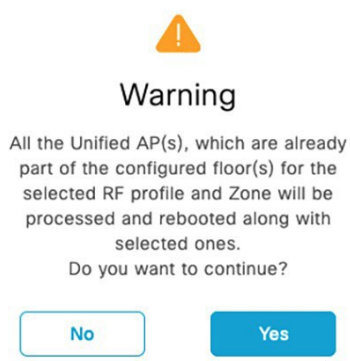
Figure 7-10: AP Provisioning Summary Page and Deploy Options



7. Click the **Now** radio button and then click **Apply** to apply the configuration.

   A **Warning** pop-up window appears, which explains that all the APs that are part of the configured floor for the selected RF profile and zone will be processed and rebooted with the selected APs.

Figure 7-11: Warning Pop-up Window

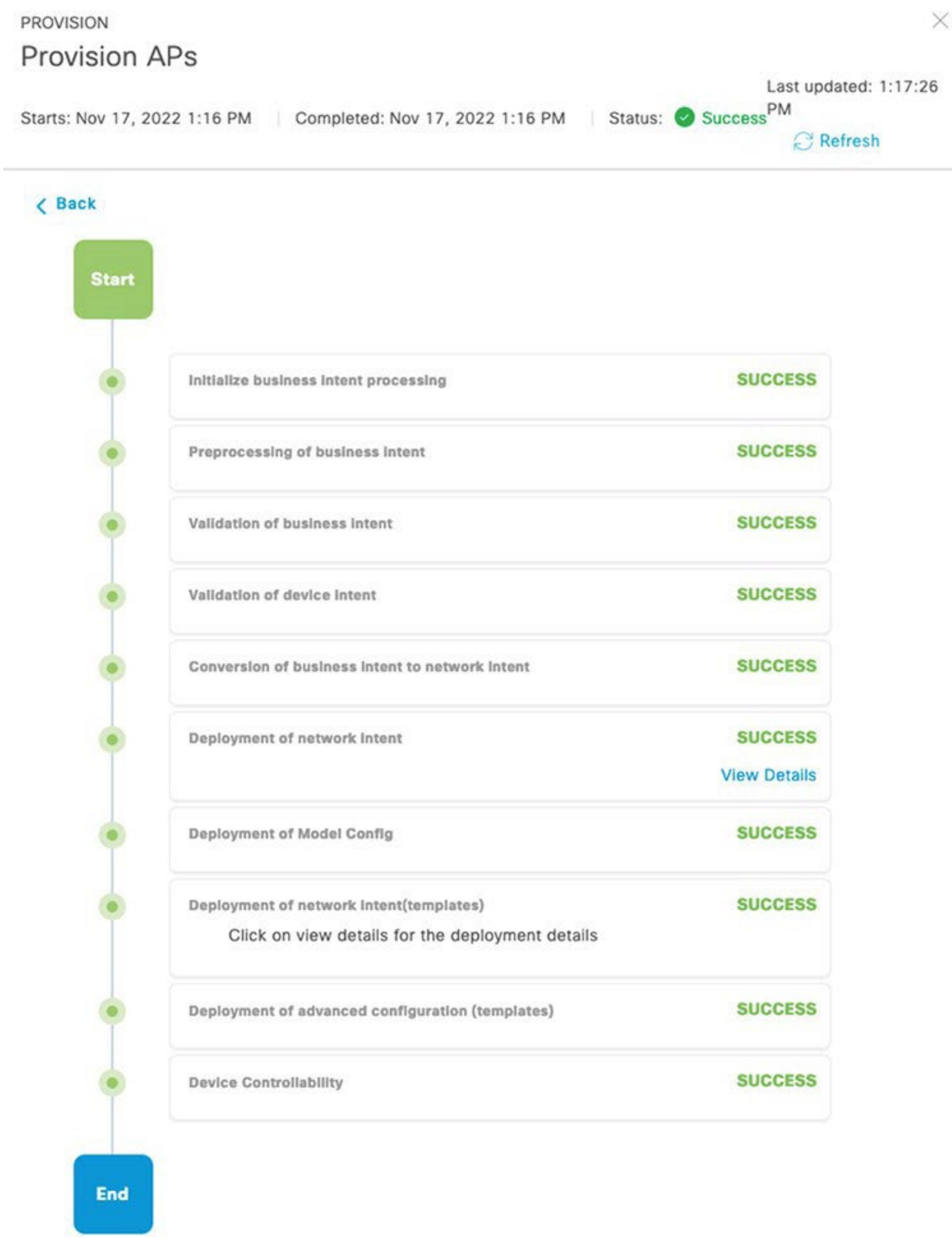


8. Click **Yes**.

   A Success pop-up screen should appear, with additional text indicating that after provisioning, the APs will reboot. Click **OK** to confirm.

9. Navigate to the Cisco Catalyst Center Task Status page to monitor the status of the “Provision APs” task.

Figure 7-12: Provision APs Task Status page



Upgrading C9800 WLC and AP Images Using Cisco Catalyst Center

This section describes the steps for upgrading the C9800 WLC and AP leveraging Cisco Catalyst Center.

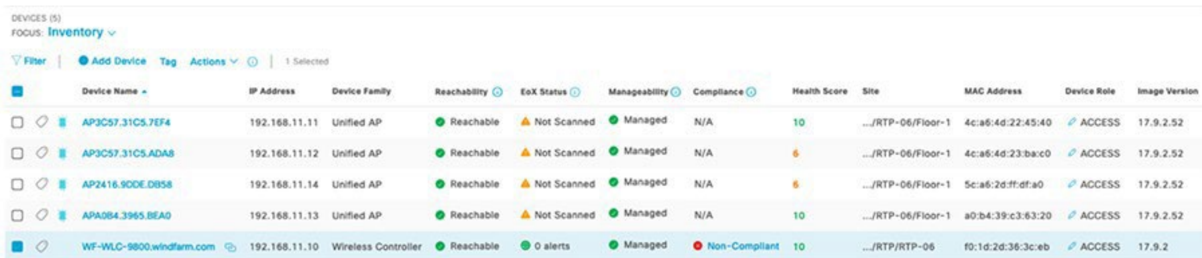
1. Upload and tag the desired C9800 WLC image as the golden image in the Cisco Catalyst Center image repository by choosing **Design > Image Repository**.

Figure 7-13: Upload and Tag the Desired C9800 WLC as the Golden Image Within the Cisco Catalyst Center Image Repository

2. Choose **Provision > Inventory**.

   Cisco Catalyst Center flags the WLC as non-compliant due to its current image not matching the Golden Image.

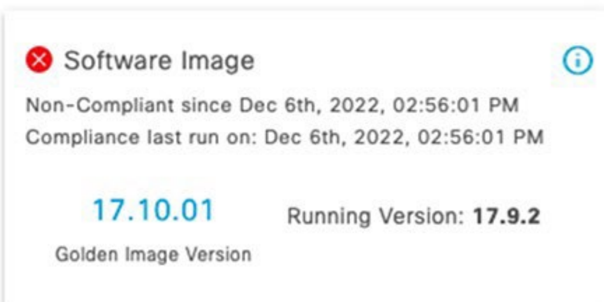
Figure 7-14: Cisco Catalyst Center Highlighting that the C9800 WLC is Non-Compliant



You can view detailed information about non-compliance of the C9800 WLC in Cisco Catalyst Center.

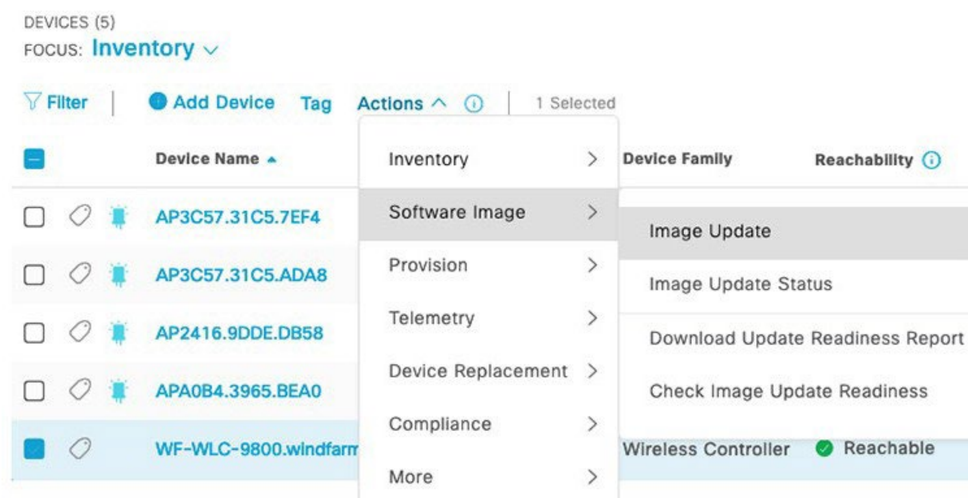
As shown in Figure 7-15, the non-compliance is due to the current running version of the C9800 WLC not matching the Golden Image version in the Cisco Catalyst Center image repository.

Figure 7-15: Details for the C9800 WLC Being Noncompliant



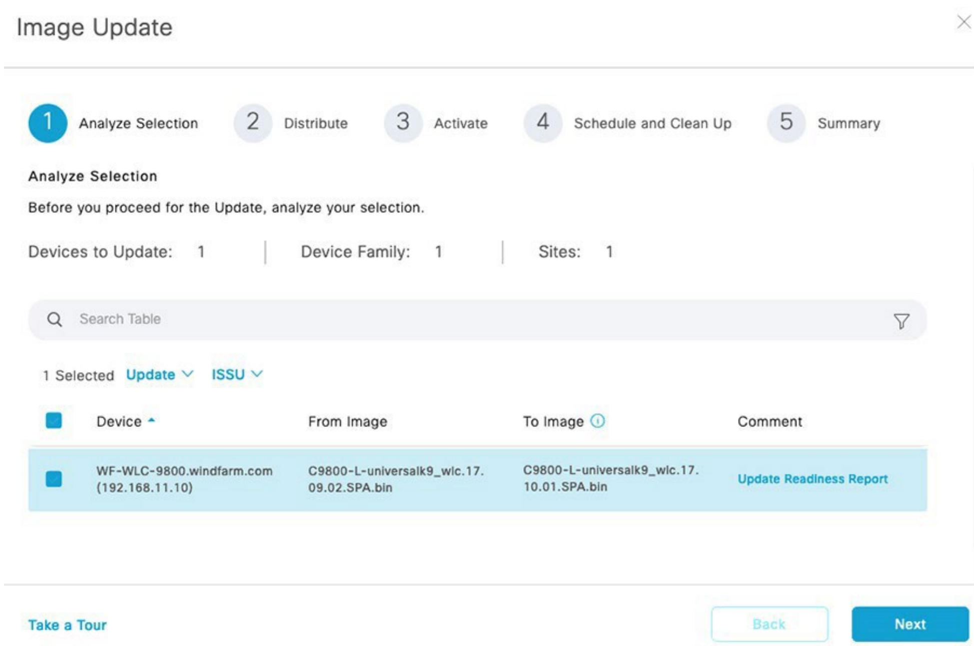
3. Navigate to the Cisco Catalyst Center **Inventory** page and check the check box for the C9800 WLC device to upgrade.

Figure 7-16: Choose the C9800 WLC to Upgrade



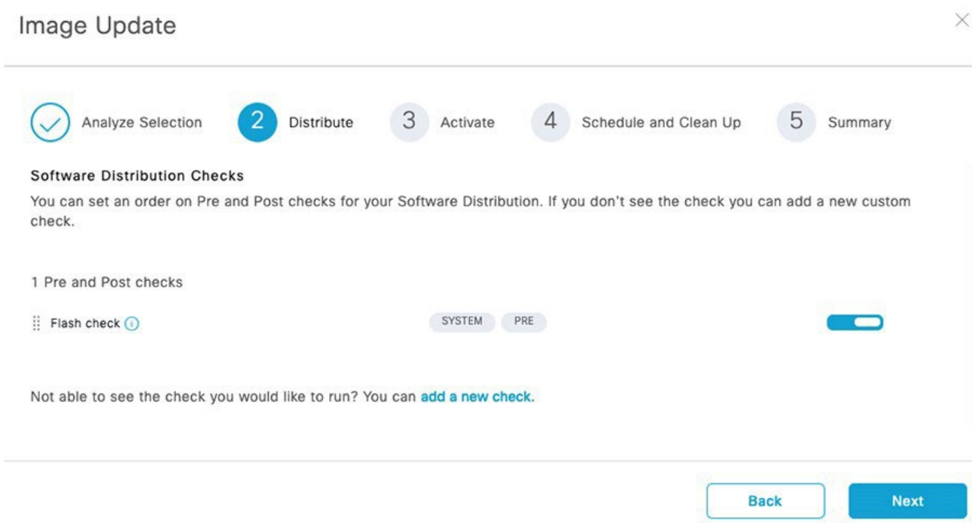
4. Review the current image on the C9800 WLC and the image being upgraded to, then click **Next**.

Figure 7-17: C9800 WLC Image Update Readiness and Analysis



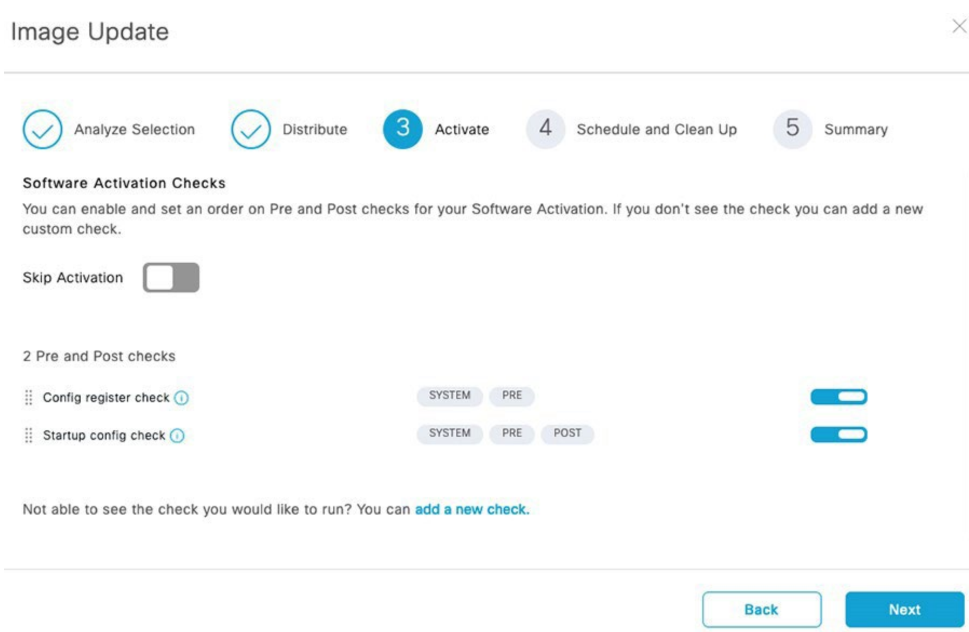
5. Configure the software distribution checks, then click **Next**.

Figure 7-18: Software Distribution Checks



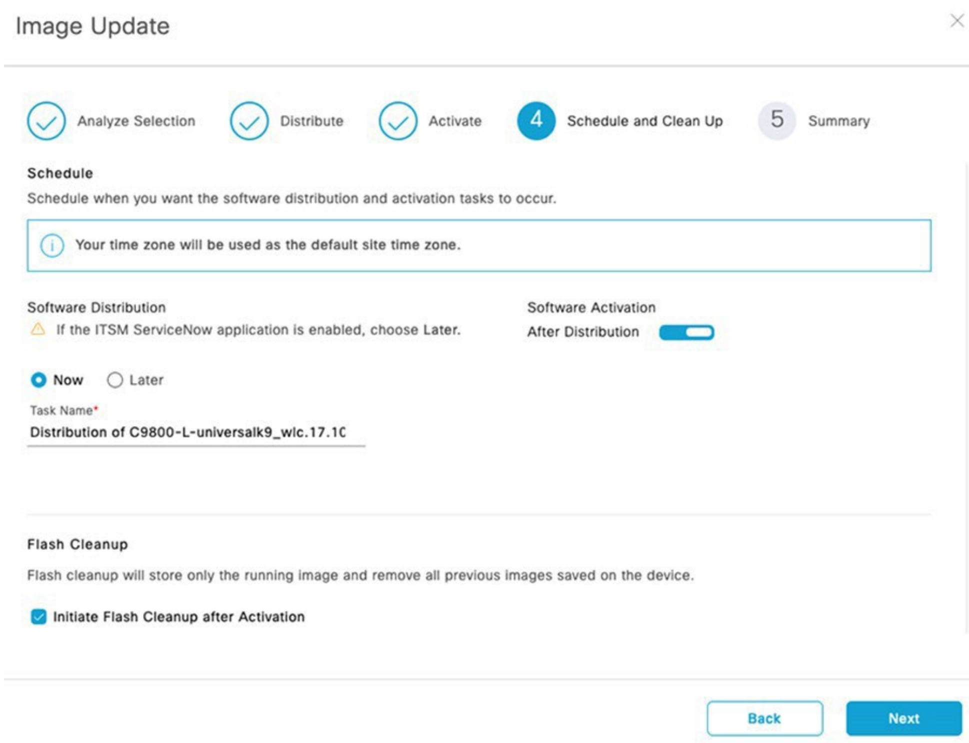
6. Configure image activation, then click **Next**.

Figure 7-19: Image Activation Configuration



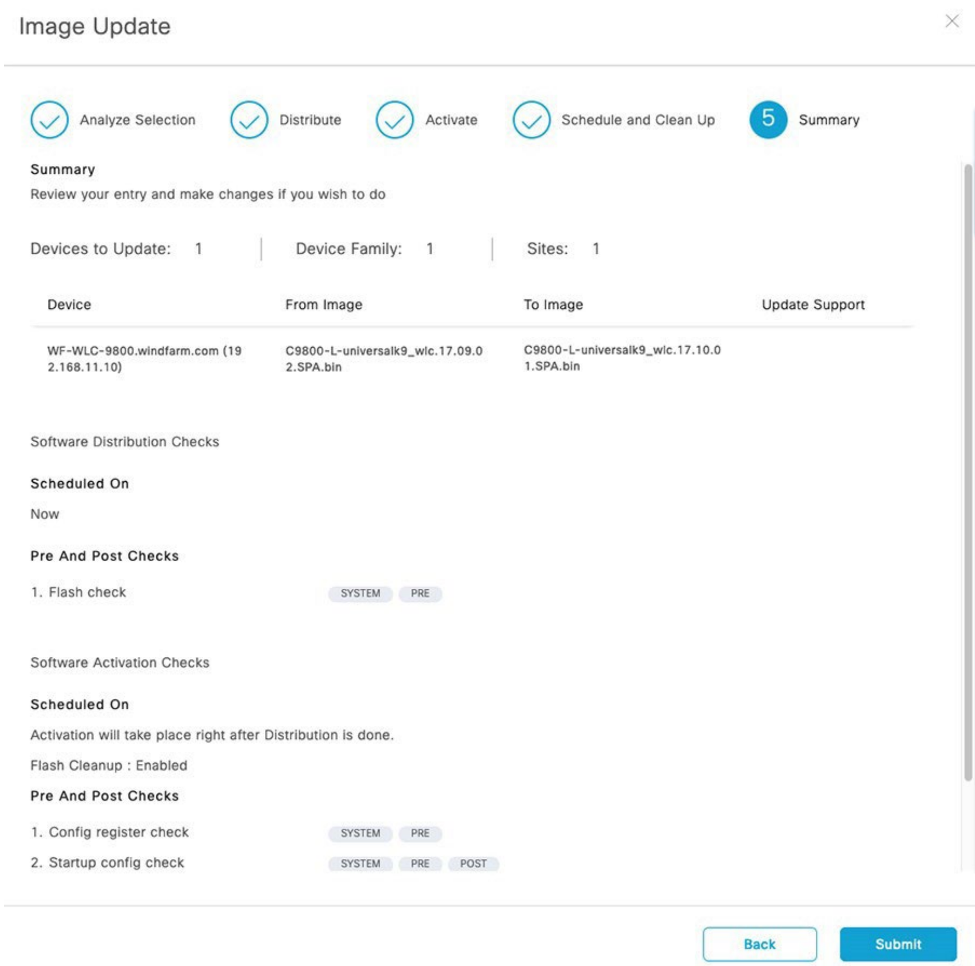
7. Configure the software distribution and activation tasks, then click **Next**.

Figure 7-20: Schedule Update and Clean Up



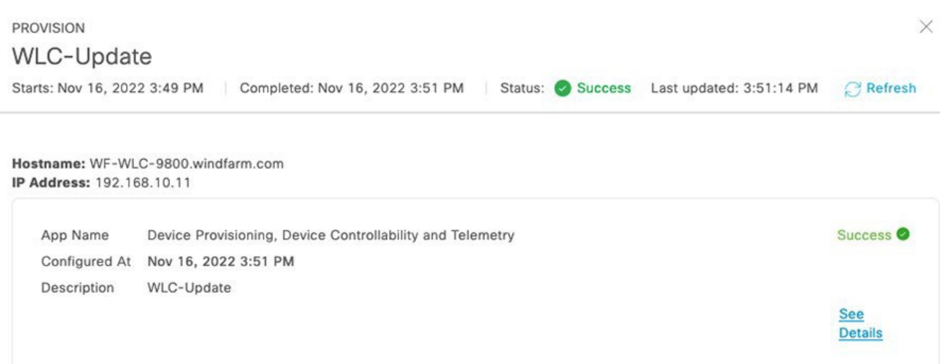
8. Review the Image Upgrade Summary, then click **Submit**.

Figure 7-21: C9800 WLC Image Upgrade Summary



9. Monitor the image upgrade process on Cisco Catalyst Center and verify that it completes successfully.

Figure 7-22: C9800 WLC Upgrade Task Status in Cisco Catalyst Center



Wi-Fi Guest User Access

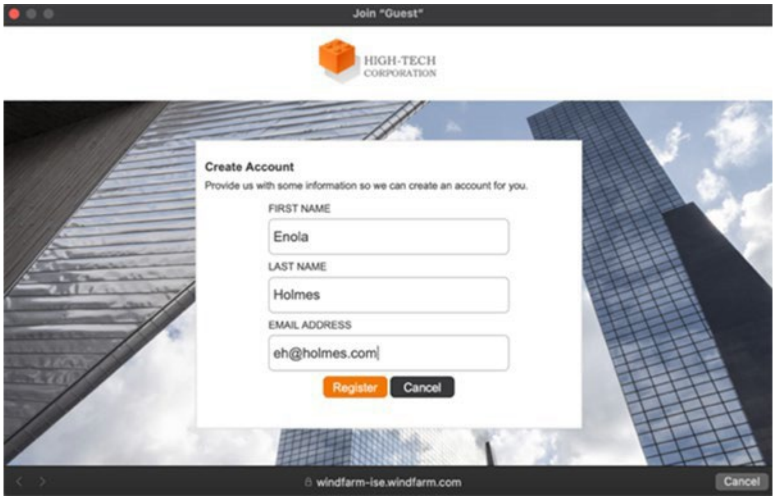
This section describes the steps that a guest user needs to perform to connect to the Guest SSID for internet access.

1. Connect to the Guest SSID.

2. In the **Guest Registration - Create Account** pop-up window, which includes options for registering guest access, enter the appropriate information and click **Register**.

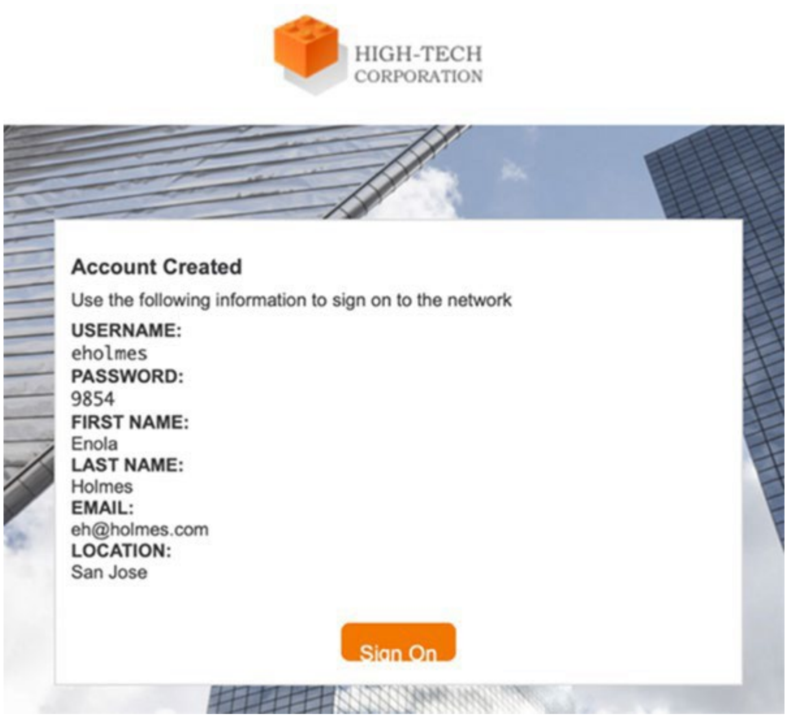
   If the pop-up window does n0t appear automatically, open a browser and navigate to the internet.

   Figure 7-23: Registering for Guest Access on Guest Registration Portal



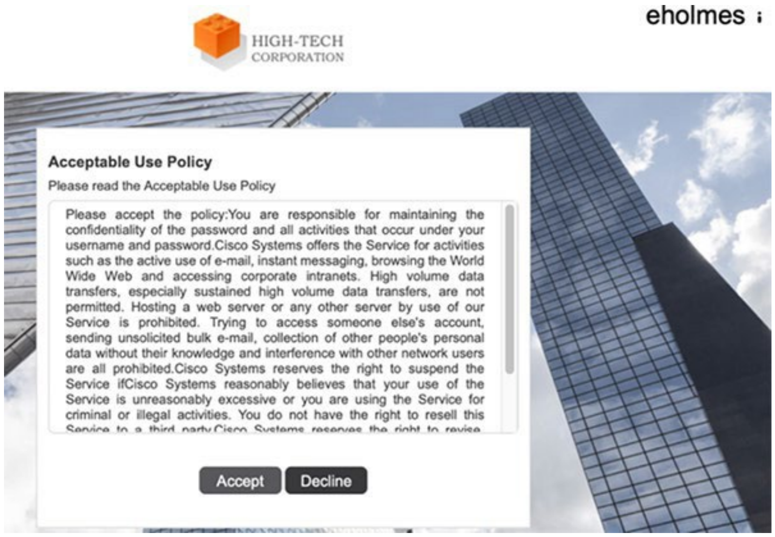
3. In the **Account Created** pop-up window, which provides the credentials for the guest user to connect to the guest SSID, click **Sign On**.

   Figure 7-24: Account Created Window



4. Review the information in the **Accept Use Policy** pop-up window and click **Accept**.

Figure 7-25: Acceptable Use Policy Window



Operating the Wireless Network

This section provides an overview of how you can use Cisco DNA Assurance to monitor and troubleshoot the WLAN deployment. Cisco DNA Assurance provides the ability to monitor the health of Cisco WLCs, APs, and wireless clients.

Cisco Catalyst Center Wireless Assurance

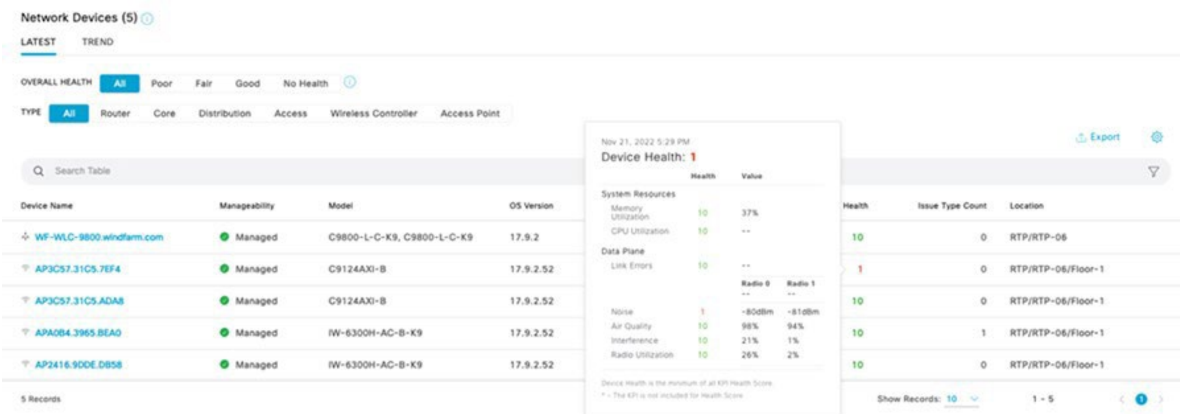
From Cisco Catalyst Center **Dashboard**, navigate to **Assurance** > **Dashboards > Health**.

The **Overall Health Dashboard** depicts the health of all the wired and wireless devices in the network.

Figure 7-26: Overall Health Dashboard

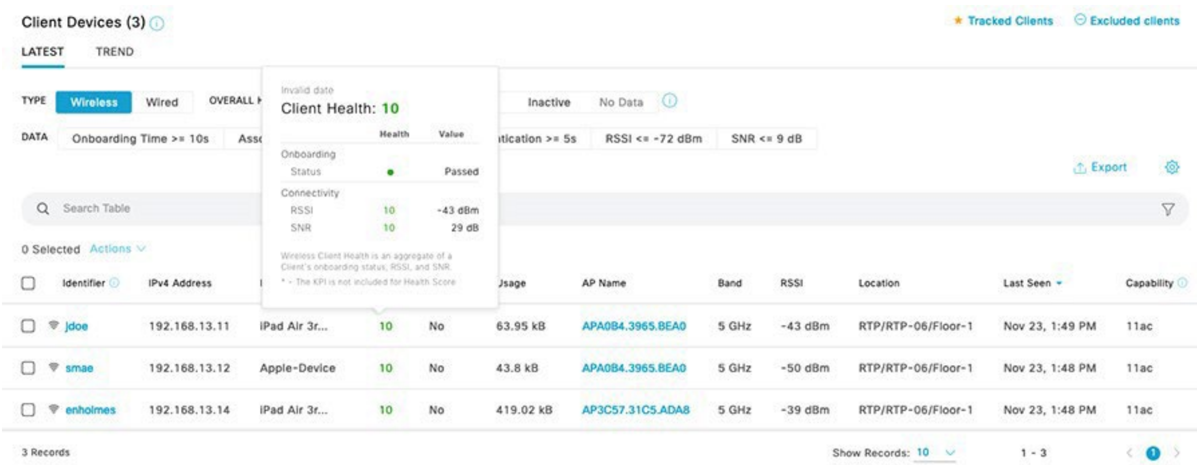
You also can view **Network Device Health**, which shows the health of wireless devices (WLCs and APs) by clicking the **Network** tab under **Assurance > Dashboards > Health**.

Figure 7-27: Viewing Wireless Devices (WLC and APs) Health



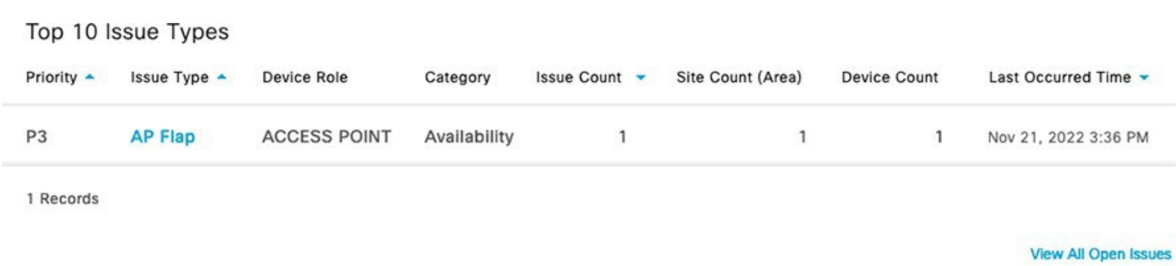
DNA Assurance also displays the health of each wireless client. Choose the **Client** tab under **Assurance > Dashboards > Health** to view client health status.

Figure 7-28: Viewing Wireless Client Health



DNA Assurance also highlights the top issues in the network at the bottom of the **Overall Health Dashboard**.

Figure 7-29: Top 10 Network Issues



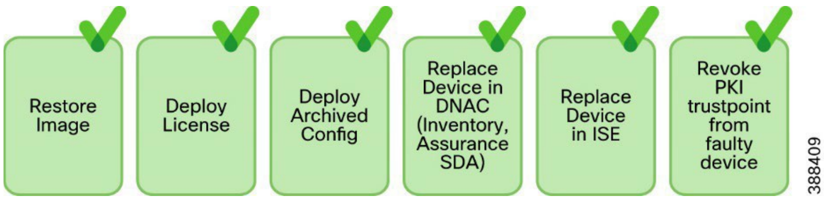
DNA Assurance also helps monitor the status of the AAA server (ISE server) and DHCP server (Active Directory) on the **Overall Health Dashboard**.

Figure 7-30: Viewing the Status of the AAA and DHCP Servers

Defective AP Replacement (RMA) using Cisco Catalyst Center

Return material authorization (RMA) is a critical part of device lifecycle management. The manual RMA procedure is time consuming. Cisco Catalyst Center RMA feature provides for the automated recovery of failed devices quickly, improving productivity and reducing operational expenses.

Figure 7-31: Cisco Catalyst Center RMA Features



Replace a Faulty Access Point

Using the Cisco Catalyst Center AP RMA feature, you can replace a faulty AP with an AP that is available in the device inventory.

This feature requires the following:

- Because the AP RMA feature supports only like-to-like AP replacements, the replacement AP must have the same model number and PID as the faulty AP.
- The replacement AP must have joined the same Cisco wireless controller as the faulty AP.
- The software image version of the faulty AP must be imported to the image repository before marking the device for replacement.
- The faulty device must be assigned to a user-defined site if the replacement device onboards Cisco Catalyst Center through plug and play (PnP).
- The replacement AP must not be in the provisioning state while triggering the RMA workflow.
- The faulty device must be in an unreachable state.

Procedure:

1. In the Cisco Catalyst Center GUI, click the Menu icon ☰ and choose **Provision > Devices > Inventory**.

   The **Inventory** page displays the device information that is gathered during the discovery process.
2. Check the check box of the faulty AP that you want to replace.
3. From the **Actions** drop-down list, choose **Device Replacement > Mark Device for Replacement**.
4. In the **Mark for Replacement** window, click the radio button next to the faulty device name.
5. From the **Actions** drop-down list, choose **Replace Device**.
6. In the **Replace Device** window, click **Start**.
7. In the **Available Replacement Devices** table, click the radio button next to the replacement device name.
8. Click **Next**.
9. Review the **Replacement Summary**, then click **Next**.
10. In the **Schedule Replacement** window, choose whether to replace the device now, or schedule the replacement for a later time, then click **Submit**.

    The RMA process begins.

11. To monitor the replacement status, under **What's Next**, click **Monitor Replacement Status**.

    The **Mark For Replacement** window lists the devices that are marked for replacement.

    Check the status of the replacement in the **Replace Status** column, which initially shows **In-Progress**.

12. Click **In-Progress** in the **Replace Status** column.

    The **Replace Status** tab shows the various steps that Cisco Catalyst Center performs as part of the device replacement.

13. In the **Marked for Replacement** window, click **Refresh** and click **Replace Status** to view the replacement status.

    If the faulty AP replacement fails, then the **Replace Status** column shows an error message with the reason for the failure.

    You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.

14. To retry the failed replacement, click the error message in the **Replace Status** column next to the device name, then click **Retry**.

15. In the **Marked for Replacement** window, click **In-Progress** against the **Replace Status** column.

    The **Replace Status** tab shows **Success** after successful replacement of the faulty AP.

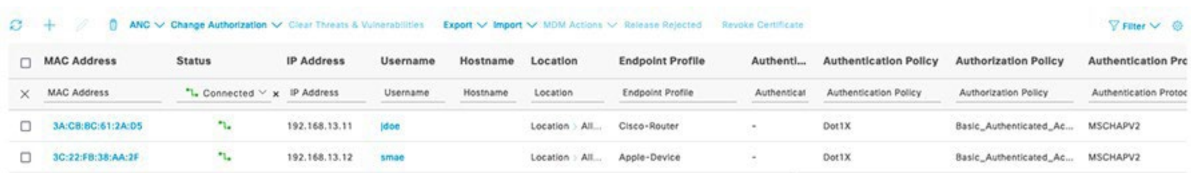
    The **Replace Status** in the **Replacement History** window shows **Replaced** after the faulty device is replaced successfully.

16. (Optional) If you do not want to replace the device, choose the device and choose **Actions > Unmark for Replacement**.

Troubleshooting Wireless Client Authentication

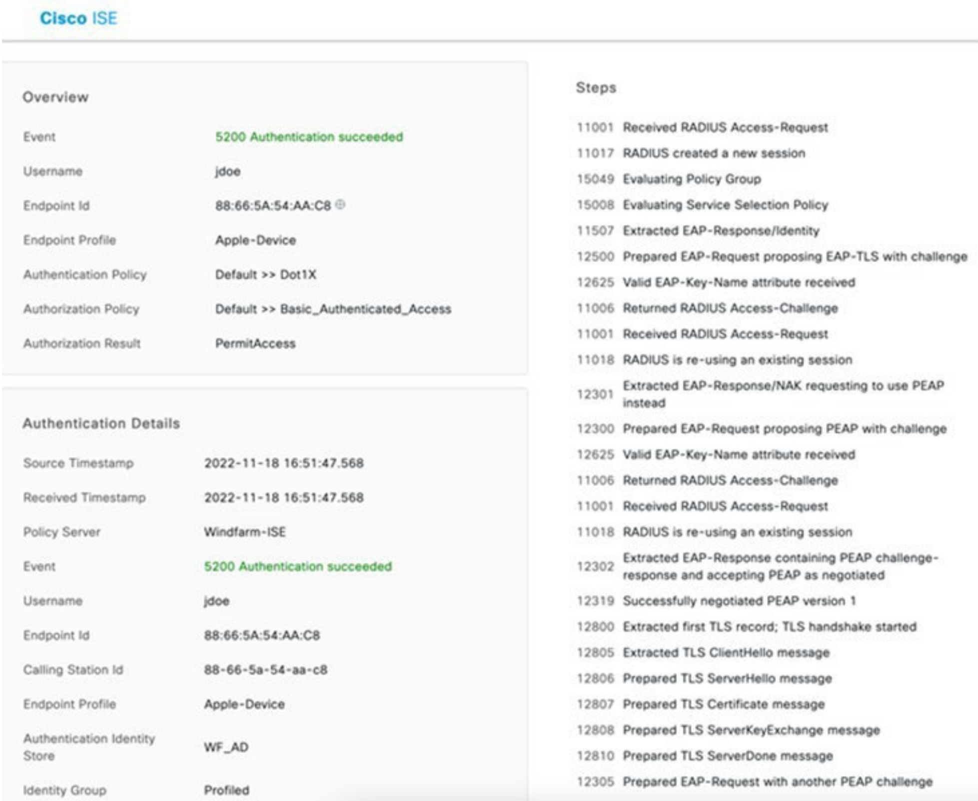
If certain wireless clients cannot successfully authenticate with the wireless network, start troubleshooting by looking at the ISE live logs. In these logs, check whether the client was successfully able to authenticate and complete the IEEE 802.1X authentication.

Figure 7-32: Verify in ISE Live Logs Whether Wireless Clients can Authenticate and Establish a Session



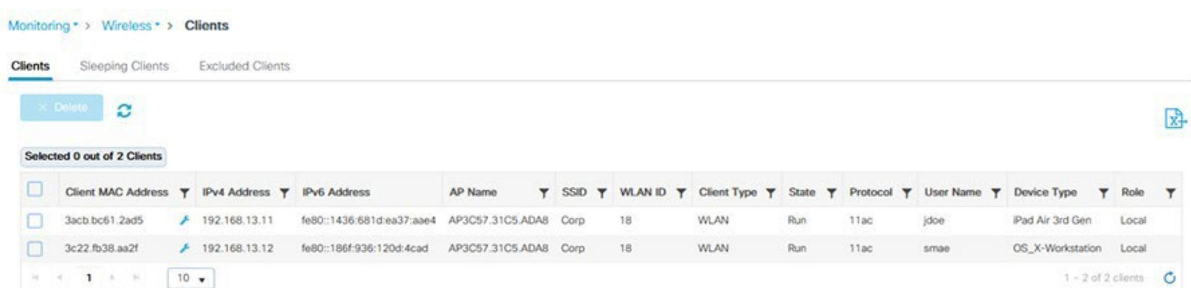
If the authentication failed, click the error for more detailed information.

Figure 7-33: Detailed Wireless Client Authentication Logs Within Cisco ISE



If the ISE authentication is successful, you can next verify whether the client is present on the WLC **Clients** page. The client should be in the Run state for it to be able to successfully pass traffic.

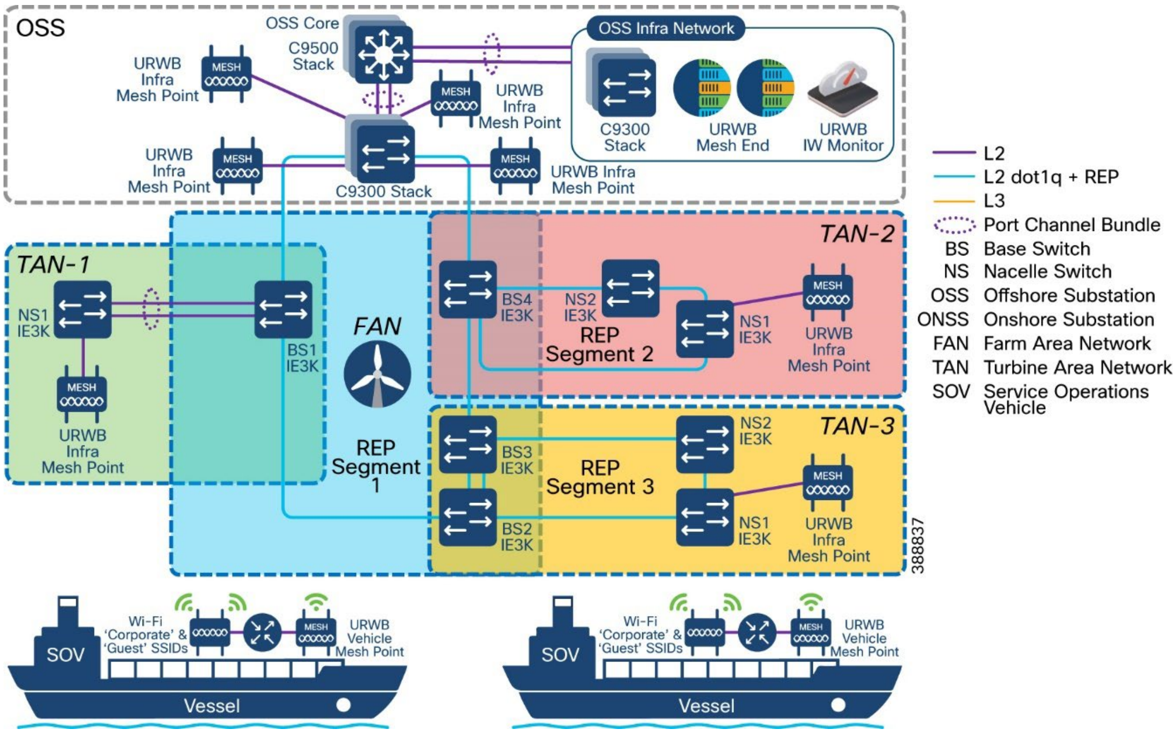
Figure 7-34: Viewing Authenticated Wireless Clients on the C9800 WLC



Offshore Wind Farm URWB Implementation for SOV to OSS Connectivity

This section provides sample configuration snippets for the offshore wind farm URWB deployment.

Figure 7-35: Offshore Wind Farm URWB Deployment for SOV to OSS Connectivity



OSS Wired Network

This section provides samples of configurations to apply to the OSS wired network to support a URWB wireless deployment for SOV to OSS wireless backhaul connectivity.

- The switch ports where URWB mesh ends are connected must be configured as trunk ports allowing both the URWB management VLAN and the traffic VLAN.
- The native VLAN for the trunk must be the URWB Management VLAN.
- The switch ports where URWB radios are connected must be configured as access ports in the URWB management VLAN.
- The Cisco Catalyst 9300 switches should be deployed as a stack.
- The Cisco Catalyst 9500 switches should be deployed as a StackWise Virtual pair.

C9500 Core-Stack

```
!
Vlan 106
 name URWB-mgmt
!
interface Vlan106
 ip address 10.10.106.1 255.255.255.0
!
interface Port-channel1
 description Connected to OSS Access 9300 Stack
 switchport mode trunk
!
interface Port-channel2
 description Connected to FAN 9300 Stack
 switchport mode trunk
!
interface TwentyFiveGigE1/0/25
 switchport mode trunk
 channel-group 1 mode active
```

```
!
interface TwentyFiveGigE1/0/26
 switchport mode trunk
 channel-group 1 mode active
!
interface TwentyFiveGigE1/0/27
 switchport mode trunk
 channel-group 2 mode active
!
interface TwentyFiveGigE1/0/28
 switchport mode trunk
 channel-group 2 mode active
!
interface TwentyFiveGigE2/0/25
 switchport mode trunk
 channel-group 1 mode active
!
interface TwentyFiveGigE2/0/26
 switchport mode trunk
 channel-group 1 mode active
!
interface TwentyFiveGigE2/0/27
 switchport mode trunk
 channel-group 2 mode active
!
interface TwentyFiveGigE2/0/28
 switchport mode trunk
 channel-group 2 mode active
!
```

C9300 Distribution Stack

```
!
vlan 106
  name URWB-Mgmt
!
interface Port-channel1
  description Connected to OSS-Core-C9500 Stack
  switchport mode trunk
!
interface GigabitEthernet1/0/1
 description connected to OSS Radio 1
switchport trunk allowed vlan 106, 217
switchport trunk native vlan 106
switchport mode trunk!

interface GigabitEthernet1/0/2
 description connected to OSS Radio 2
switchport trunk allowed vlan 106,217
switchport trunk native vlan 106
switchport mode trunk!
!
interface TenGigabitEthernet1/1/7
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface TenGigabitEthernet1/1/8
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet2/0/1
 description connected to OSS Radio 3
switchport trunk allowed vlan 106, 217
```

```
switchport trunk native vlan 106
switchport mode trunk!
!
interface GigabitEthernet2/0/2
 description connected to OSS Radio 4
switchport trunk allowed vlan 106,217
switchport trunk native vlan 106
switchport mode trunk!

!
interface TenGigabitEthernet2/1/7
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface TenGigabitEthernet2/1/8
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
```

C9300 Access Stack

```
!
vlan 106
  name URWB-Mgmt
!
interface Port-channel1
  description Connected to OSS-Core-C9500 Stack
  switchport mode trunk
!
interface GigabitEthernet1/0/1
 description connected to Mesh-End-1
 switchport trunk allowed vlan 106, 217
 switchport trunk native vlan 106
 switchport mode trunk
!
interface TenGigabitEthernet1/1/7
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface TenGigabitEthernet1/1/8
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet2/0/1
 description connected to Mesh-End-2
 switchport trunk allowed vlan 106, 217
 switchport trunk native vlan 106
 switchport mode trunk
!
interface TenGigabitEthernet2/1/7
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
interface TenGigabitEthernet2/1/8
 description Connected to OSS-Core-C9500 Stack
 switchport mode trunk
 channel-group 1 mode active
!
```

URWB Network Configuration

This section provides sample configurations for a URWB deployment to provide SOV to OSS connectivity.

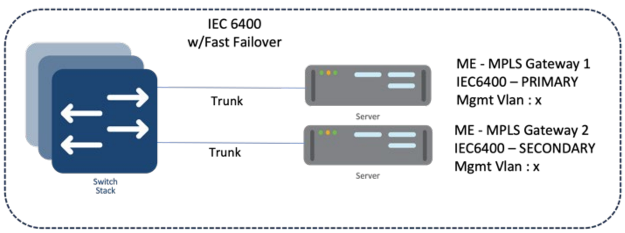
- A pair of URWB mesh ends should be deployed for redundancy and high availability.
- The switch ports where URWB mesh ends are connected must be configured as trunk ports, allowing both URWB management VLAN and traffic VLAN. The native VLAN on a trunk must be the URWB Management VLAN.
- Each mesh end should be connected to a different Cisco Catalyst 9300 switch within the stack.
- The URWB infrastructure APs on the OSS, FAN, and TAN must be configured for layer 2 (flat network) fluidity in which the infrastructure APs and the SOV APs are in the same subnet.
- All URWB APs and the mesh ends must be configured with the same passphrase.

OSS Infrastructure IW9167E/IEC6400 Mesh End

Figure 7-36 shows the deployment topology for a redundant pair of URWB IEC6400s or IW9167 mesh ends in the OSS network.

Figure 7-36: URWB IW9167E/IEC6400 Mesh End High Availability Deployment

The following example shows a snippet of the running configuration from a URWB mesh end




```
################ GENERAL CONFIG #################
Device name: OSS-9167ME-1
IP:        10.10.106.10
Netmask:  255.255.255.0
Gateway:  10.10.106.1
Nameservers:
Mesh End mode
################ FLUIDITY CONFIG ################
Fluidity enabled
Fluidity interface: none
Infrastructure mode
Backhaul-check: handoff-inhibition
Mesh-end backhaul-check: handoff-inhibition
Color: enabled, current: 0
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
################ MPLS CONFIG ###################
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
reduce-broadcast: disabled
pwlist: all
```

```
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover:  enabled
Node failover timeout:  0 ms
L2TP WAN update delay:  disabled
Preemption delay:  70 s
Virtual IP:  0.0.0.0
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255  local dynamic
MPLS tunnels:
ldp_id 519374131 debug 0 auto_pw 1
local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0 }
lsps 4################ VLAN CONFIG ####################
VLAN status: enabled
Management VID: 106
Native VID: 217
################ ADVANCED CONFIG ################
Gratuitous-arp: enabled
         Delay: 150 ms
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p disabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500
```

OSS Infrastructure IW9167E Mesh Point

The following example shows a snippet of the running configuration from a URWB 9167E mesh point radio:

```
################ GENERAL CONFIG #################
Device name: OSS-9167-1
IP:       10.10.106.11
```

```
netmask:  255.255.255.0
Gateway:  10.10.106.1
Nameservers:
Mesh Point mode
################ WIRELESS CONFIG ################
SLOT 1 Config

Interface:                enabled

Mode:                     fluidity

Frequency:                5180 MHz
Channel:                  36
Channel width:            40 MHz
Antenna number:           2
TX power level:           7
TX power:                 0 dBm
Antenna gain:             7 dBi
Maximum tx mcs:           9
High-efficiency:          enabled
Maximum tx nss:           2
RTS protection:           disabled
guard-interval:           800 ns
ampdu max length:         255
distance:                 3000 m

The ampdu Tx
priority 0:               enabled
priority 1:               enabled
priority 2:               enabled
priority 3:               enabled
priority 4:               enabled
priority 5:               enabled
priority 6:               disabled
priority 7:               disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase:               windfarm
AES encryption:           enabled
AES key-control:          disabled
Key rotation:             disabled
Key rotation timeout:     0(second)

DFS region:               B
DFS radar role:           auto
Radar detected:           0
Indoor deployment:        disable
Rx-SOP Threshold:         0 dBm(AUTO)

SLOT 2 Config

Interface:                disabled

Mode:                     fluidity

Frequency:                5300 MHz
Channel:                  60
Channel width:            40 MHz
Antenna number:           2
TX power level:           7
TX power:                 2 dBm
```

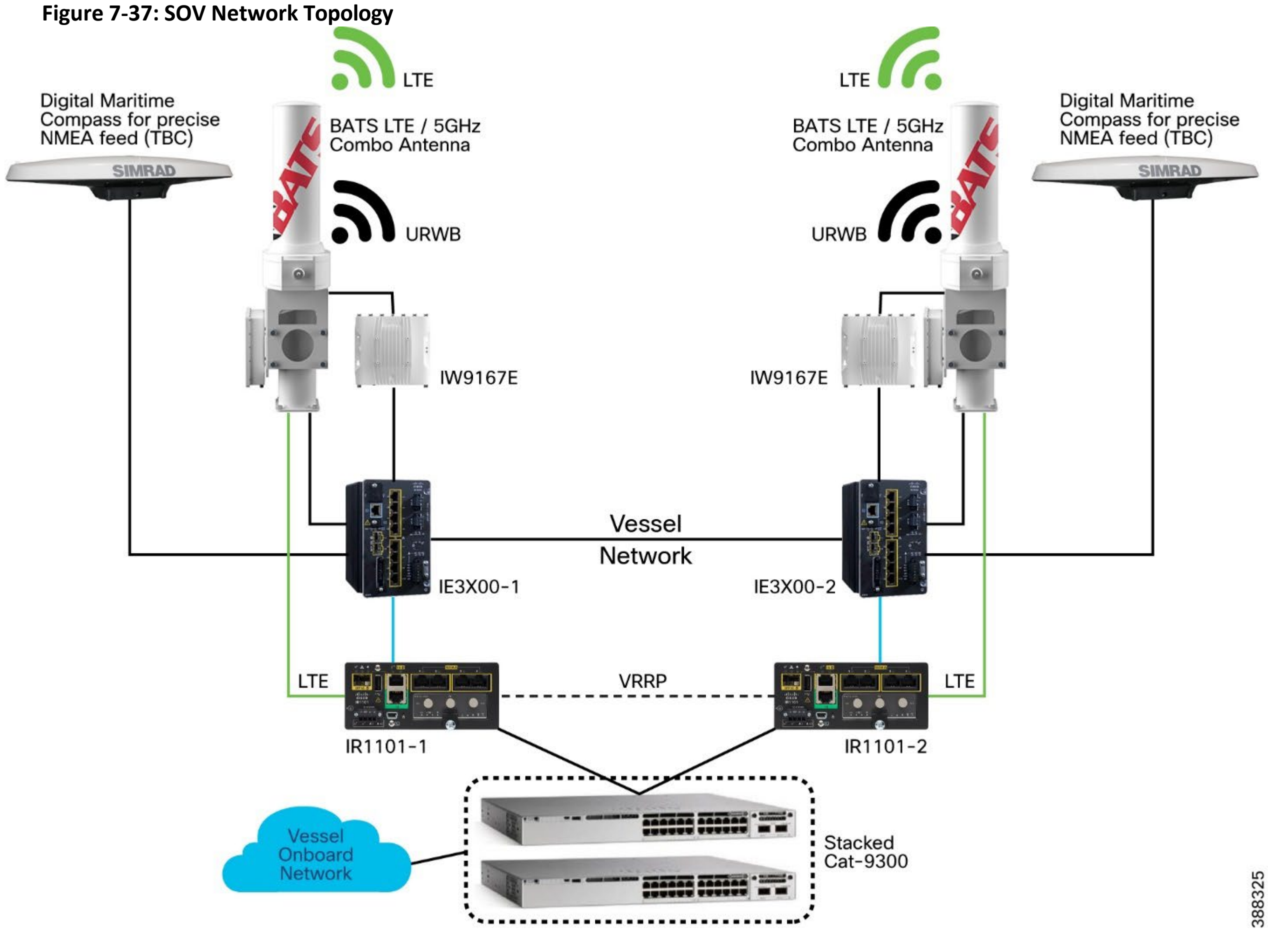
```
Antenna gain:            7 dBi
Maximum tx mcs:          9
High-efficiency:         enabled
Maximum tx nss:          2
RTS protection:          disabled
guard-interval:          800 ns
ampdu max length:        255
distance:                3000 m

The ampdu Tx
priority 0:              enabled
priority 1:              enabled
priority 2:              enabled
priority 3:              enabled
priority 4:              enabled
priority 5:              enabled
priority 6:              disabled
priority 7:              disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase:              windfarm
AES encryption:          disabled
AES key-control:         disabled
Key rotation:            disabled
Key rotation timeout:    0(second)

DFS region:              B
DFS radar role:          auto
Radar detected:          0
Indoor deployment:       disable
Rx-SOP Threshold:        0 dBm(AUTO)
################ FLUIDITY CONFIG ################
Fluidity enabled
Fluidity interface: 1
Infrastructure mode
Backhaul-check: handoff-inhibition
Mesh-end backhaul-check: handoff-inhibition
Color: enabled, current: 0
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
################ MPLS CONFIG ####################
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: enabled (broadcasting not allowed)
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover is disabled
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255  dynamic
MPLS tunnels:
ldp_id 1570886916 debug 0 auto_pw 1
```

```
local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true
static_pws { 0.0.0.0 }
lsps 4
################ VLAN CONFIG ####################
VLAN status: enabled
Management VID: 106
Native VID: 217
################ ADVANCED CONFIG ################
Gratuitous-arp: enabled
         Delay: 150 ms
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p disabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500
```

Service Operations Vessel Network

Figure 7-37 shows implementation details for the service operations vessel (SOV) network.

Figure 7-37: SOV Network Topology



SOV Wired Network

This section provides sample configuration snippets for the SOV wired network.

IE3X00-1

```
!
vlan 106
 name URWB-Mgmt
!
spanning-tree vlan 106 priority 4096
!
interface GigabitEthernet1/3
 description V-9167E-1
switchport trunk allowed
 vlan  106, 217
switchport trunk native vlan
 106
switchport mode trunk!
spanning-tree portfast
!
interface GigabitEthernet1/4
 description connected to IR1101-1 gig0/0/5
 switchport trunk allowed vlan 106
 switchport mode trunk
!
interface GigabitEthernet1/10
 description connected to IE3200-2 gig1/10
 switchport trunk allowed vlan 106
 switchport mode trunk
!
```

IE3X00-2

```
!
vlan 106
 name URWB-Mgmt
!
interface GigabitEthernet1/3
 description V-9167E-2
switchport trunk allowed
 vlan 106, 217
switchport trunk native vlan
 106
switchport mode trunk!
!
interface GigabitEthernet1/4
 description connected to IR1101-2 gig0/0/5
 switchport trunk allowed vlan 106
 switchport mode trunk
!
interface GigabitEthernet1/10
 description connected to IE3200-1 gig1/10
 switchport trunk allowed vlan 106
 switchport mode trunk
!
```

IR1101-1

```
!
vlan 106,200-201
!
interface GigabitEthernet0/0/0
 description connected to C9300 gig2/0/1
 switchport
 switchport trunk allowed vlan 106,200,201
 switchport mode trunk
 media-type rj45
!
interface GigabitEthernet0/0/5
 description connected to IE3200-1 gig1/4
 switchport trunk allowed vlan 106
 switchport mode trunk
!
interface Vlan100
 ip address 10.10.10.101 255.255.255.0
!
interface Vlan200
 ip address 192.168.0.2 255.255.255.0
 ip access-group deny201 in
 vrrp 1 ip 192.168.0.1
 vrrp 1 preempt delay minimum 10
 vrrp 1 priority 101
!
interface Vlan201
 ip address 192.168.1.2 255.255.255.0
 ip access-group deny200 in
 vrrp 2 ip 192.168.1.1
!
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 192.168.0.0
 network 192.168.1.0
!
ip access-list extended deny200
 10 deny   ip 192.168.0.0 0.0.0.255 any
 20 permit ip any any
```

```
ip access-list extended deny201
 10 deny   ip 192.168.1.0 0.0.0.255 any
 20 permit ip any any
!
```

IR1101-2

```
!
vlan 106,200-201
!
interface GigabitEthernet0/0/0
 description connected to C9300 gig1/0/1
 switchport
 switchport trunk allowed vlan 106,200,201
 switchport mode trunk
 media-type rj45
!
interface GigabitEthernet0/0/5
 description connected to IE3200-2 gig1/4
 switchport trunk allowed vlan 106
 switchport mode trunk

interface Vlan100
 ip address 10.10.10.102 255.255.255.0
!
interface Vlan200
 ip address 192.168.0.3 255.255.255.0
 ip access-group deny201 in
 vrrp 1 ip 192.168.0.1
!
interface Vlan201
 ip address 192.168.1.3 255.255.255.0
 ip access-group deny200 in
 vrrp 2 ip 192.168.1.1
 vrrp 2 preempt delay minimum 10
 vrrp 2 priority 101
!
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 192.168.0.0
 network 192.168.1.0
!
ip access-list extended deny200
 10 deny   ip 192.168.0.0 0.0.0.255 any
 20 permit ip any any
ip access-list extended deny201
 10 deny   ip 192.168.1.0 0.0.0.255 any
 20 permit ip any any
!
```

C9300

```
!
vlan 106,200-201
!
interface GigabitEthernet1/0/1
description connected to IR1101-2 gig0/0/0
 switchport trunk allowed vlan 106,200,201
 switchport mode trunk
!
interface GigabitEthernet2/0/1
description connected to IR1101-1 gig0/0/0
 switchport trunk allowed vlan 106,200,201
```

```
 switchport mode trunk
end
!
interface Vlan200
 ip address 192.168.0.5 255.255.255.0
!
interface Vlan201
 ip address 192.168.1.5 255.255.255.0
!
```

URWB Configuration

This section provides sample configuration snippets for the SOV wireless (URWB) network.

Service Operations Vessel IW9167E-1 (Mobile)

```
################ GENERAL CONFIG #################
Device name: V-9167E-1
IP:        10.10.106.21
netmask:  255.255.255.0
Gateway:  10.10.106.1
Nameservers:
Mesh Point mode
################ WIRELESS CONFIG ################
SLOT 1 Config

Interface:              enabled

Mode:                   fluidity

Frequency:              5180 MHz
Channel:                36
Channel width:          40 MHz
Antenna number:         2
TX power level:         6
TX power:               3 dBm
Antenna gain:           7 dBi
Maximum tx mcs:         9
High-efficiency:        enabled
Maximum tx nss:         2
RTS protection:         512
guard-interval:         800 ns
ampdu max length:       255
distance:               3000 m

The ampdu Tx
priority 0:             enabled
priority 1:             enabled
priority 2:             enabled
priority 3:             enabled
priority 4:             enabled
priority 5:             enabled
priority 6:             disabled
priority 7:             disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase:             windfarm
AES encryption:         enabled
AES key-control:        disabled
Key rotation:           disabled
Key rotation timeout:   0(second)
```

```
DFS region:             B
DFS radar role:         auto
Radar detected:         0
Indoor deployment:      disable
Rx-SOP Threshold:       0 dBm(AUTO)
################ FLUIDITY CONFIG ################
Fluidity enabled
Fluidity interface: 1, 2
Vehicle ID: automatic, current ID: 100017752 current role: mobile primary unit
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
Rssi low/high zones threshold: 35
Color: enabled, current: 0
Color min RSSI threshold: 20
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
################ MPLS CONFIG ####################
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: enabled (broadcasting not allowed)
reduce-broadcast: enabled
pwlist: all
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover is enabled
Node failover timeout:  0 ms
L2TP WAN update delay:  disabled
Preemption delay:  100 s
Virtual IP:  10.10.10.10
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255  dynamic
MPLS tunnels:
ldp_id 312290134 debug 0 auto_pw 1
local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id 100017752 v2v_handoff 0 v2v_pws false auto_en
true static_pws { 0.0.0.0 }
lsps 4################ VLAN CONFIG ####################
################ VLAN CONFIG ####################
VLAN status: enabled
Management VID: 106
Native VID: 217
################ ADVANCED CONFIG ################
Gratuitous-arp: enabled
         Delay: 150 ms
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p enabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500            LICENSED
```

Service Operations Vessel IW9167E -2(Mobile)

```
################ GENERAL CONFIG #################
Device name: V-9167E-2
IP:        10.10.106.22
netmask:  255.255.255.0
Gateway:  10.10.106.1
Nameservers:
Mesh Point mode
################ WIRELESS CONFIG ################
SLOT 1 Config

Interface:               enabled

Mode:                    fluidity

Frequency:               5180 MHz
Channel:                 36
Channel width:           40 MHz
Antenna number:          2
TX power level:          6
TX power:                3 dBm
Antenna gain:            7 dBi
Maximum tx mcs:          9
High-efficiency:         enabled
Maximum tx nss:          2
RTS protection:          512
guard-interval:          800 ns
ampdu max length:        255
distance:                3000 m

The ampdu Tx
priority 0:              enabled
priority 1:              enabled
priority 2:              enabled
priority 3:              enabled
priority 4:              enabled
priority 5:              enabled
priority 6:              disabled
priority 7:              disabled

Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=2 cw_max=3 txop=15
vi: aifs=1 cw_min=3 cw_max=4 txop=31
be: aifs=3 cw_min=4 cw_max=6 txop=31
bk: aifs=7 cw_min=3 cw_max=4 txop=0

Passphrase:              windfarm
AES encryption:          enabled
AES key-control:         disabled
Key rotation:            disabled
Key rotation timeout:    0(second)

DFS region:              B
DFS radar role:          auto
Radar detected:          0
Indoor deployment:       disable
Rx-SOP Threshold:        0 dBm(AUTO)
################ FLUIDITY CONFIG ################
Fluidity enabled
Fluidity interface: 1, 2
Vehicle ID: automatic, current ID: 100017753 current role: mobile secondary unit
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
Rssi low/high zones threshold: 35
Color: enabled, current: 0
```

```
Color min RSSI threshold: 20
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
################ MPLS CONFIG ####################
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: enabled (broadcasting not allowed)
reduce-broadcast: enabled
pwlist: all
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover is enabled
Node failover timeout:  0 ms
L2TP WAN update delay:  disabled
Preemption delay:  100 s
Virtual IP:  10.10.10.10
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255  dynamic
MPLS tunnels:
ldp_id 312290134 debug 0 auto_pw 1
local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id 100017752 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0
}
lsps 4################ VLAN CONFIG ####################
################ VLAN CONFIG ####################
VLAN status: enabled
Management VID: 106
Native VID: 217
################ ADVANCED CONFIG ################
Gratuitous-arp: enabled
         Delay: 150 ms
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p enabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500
```

IW Monitor

IW Monitor is a network-wide, on-premises monitoring dashboard that allows any URWB customer to proactively maintain and monitor one or more wireless OT networks. IW-Monitor displays data and situational alerts from every URWB device in a network in real time. One of the biggest advantages of IW Monitor is the ability to configure alerts for a group of radios based on certain KPIs. Imagine needing to support an application mix of automation and CCTV. The set of radios supporting the automation application can be grouped and alarms configured for KPIs such as latency, jitter, RSSI, and so on. And the group of radios that support the CCTV network can have alarms configured using different KPIs such as Link Error Rate (LER), MCS rate, and so on.

IW Monitor Dashboard

Figure 7-38 IW Monitor Dashboard

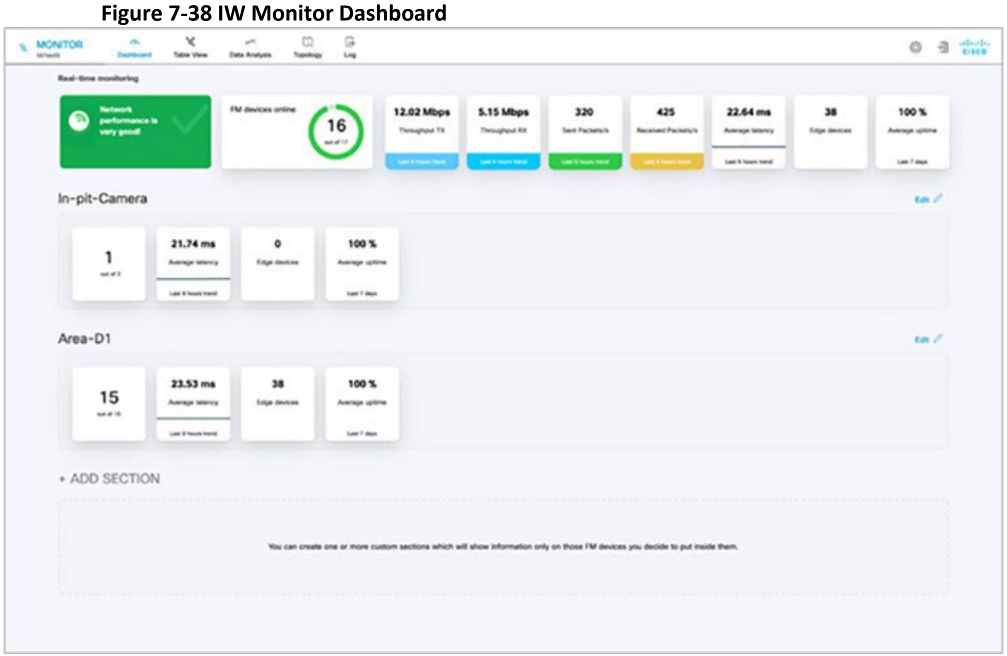
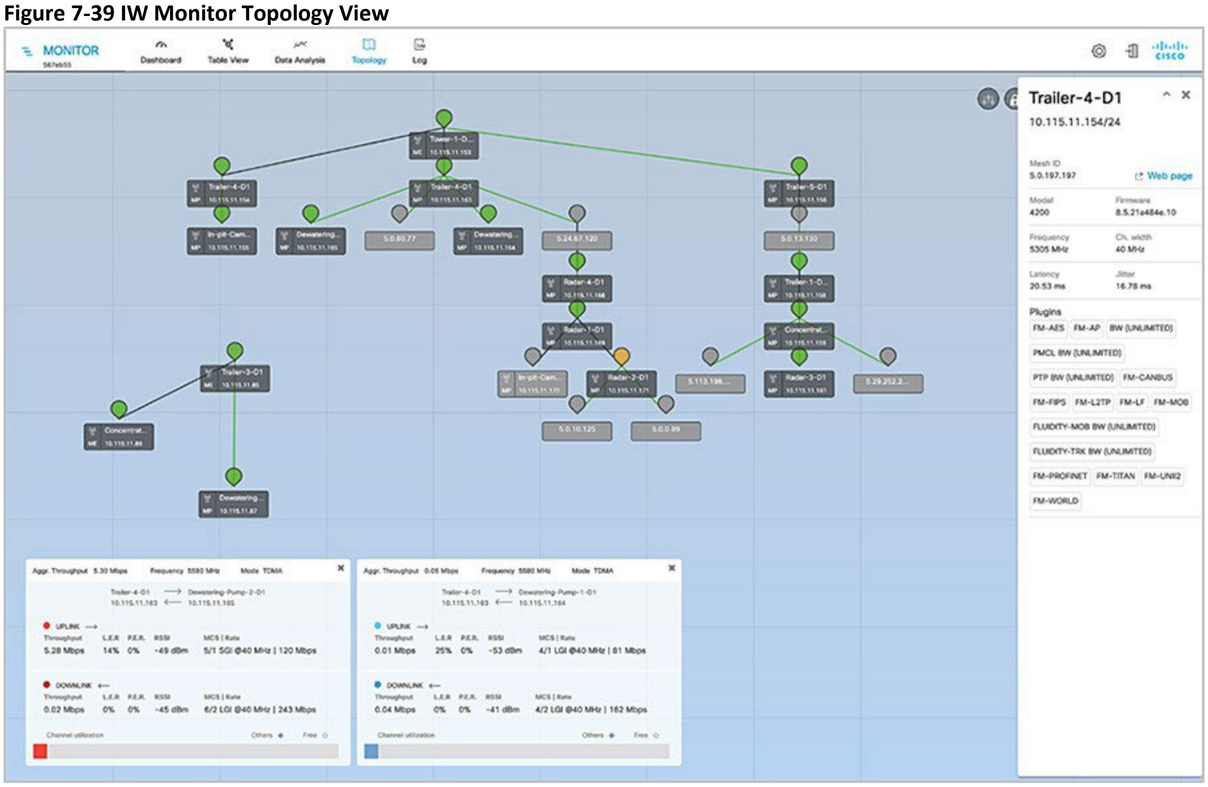


Figure 7-39 IW Monitor Topology View



For complete IW Monitor Installation steps please see the IW Monitor [User guide](#).

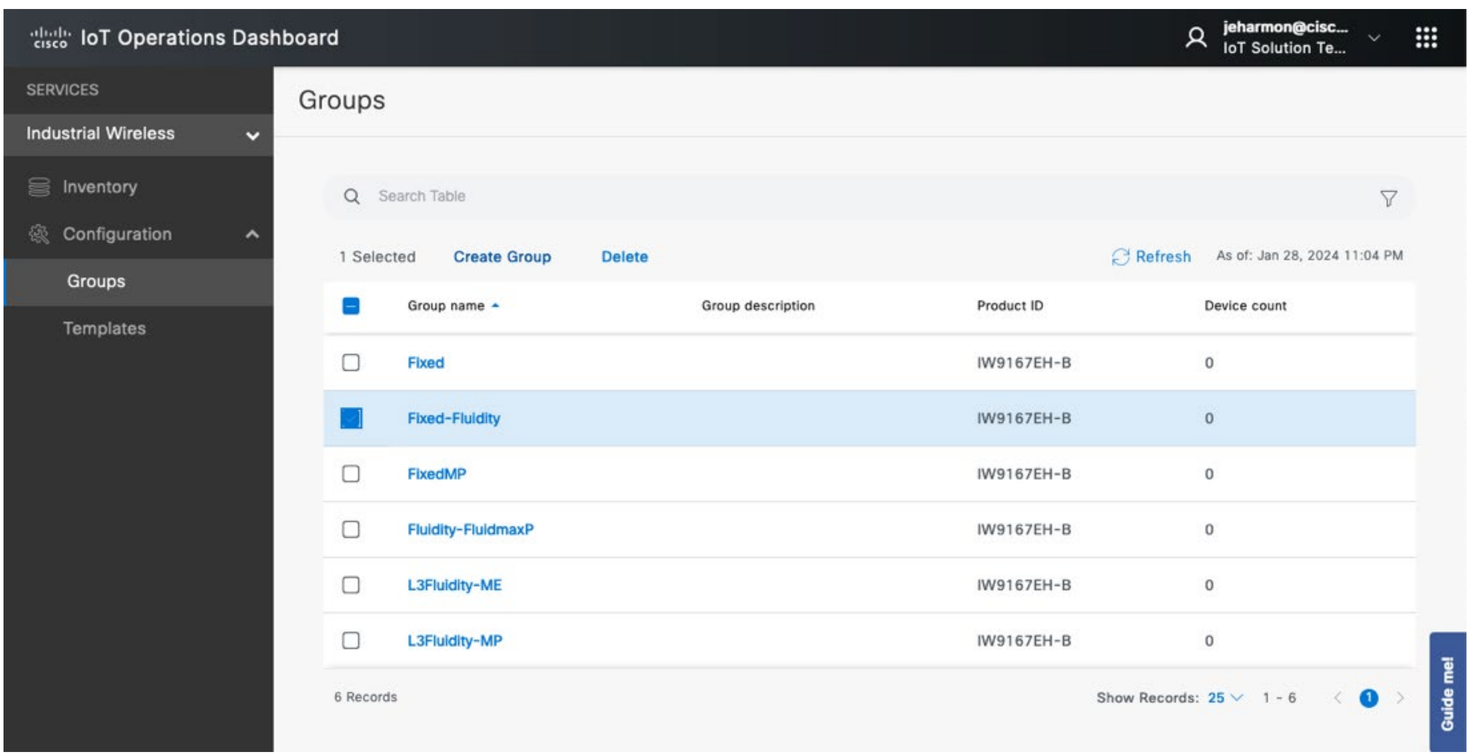
IW Service on OPERATIONS DASHBOARD

Operations Dashboard is a centralized cloud-hosted server that can be used for provisioning of an entire URWB system, including configuration, firmware upgrade, and plug-in activation. It allows all the radio configuration to be done in a single pane and uploaded to radios in real time or offline. IW service supports almost all URWB configuration options (basic and advanced). IW Service can be used to create configuration templates and apply them to multiple URWB devices of the same type. Templates can be applied in either online mode (if the URWB devices have internet access) or offline mode (if the URWB devices have no internet access). We recommend IW services for configuring URWB devices in deployments of any size.

URWB device provisioning can be done using one of two methods:

- Online Configuration method:
    - Automated template provisioning using the Operations Dashboard to push pre built configuration templates to IP reachable URWB devices.
- Offline Configuration method:
    - Operations dashboard generated configuration files, to upload locally to URWB devices.
    - Local manual configuration via the local URWB device gui.

Figure 7-40 IW Services on OD Cloud-Hosted URWB Configuration Tool



Note: For in depth IW service configuration guidance please see Operations Dashboard.

Chapter 8: Implementing WAN Backhaul and Control Center

This chapter includes the following topics:

- Implementing WAN Backhaul
- Implementing Network Control Center and Application Services

Implementing WAN Backhaul

The utility WAN is often a dedicated WAN infrastructure that connects the transmission service operator (TSO) control center with various substations and other field networks and assets. Utility WAN connections can include a variety of technologies, such as cellular LTE and 5G options for public backhaul, fiber ports to connect utility owned private networks, leased lines or MPLS PE connectivity options, and legacy multilink PPP backhaul aggregating multiple T1 and E1 circuits.

The Cisco IR8340 is used as a substation router in this solution. The router is configured as customer edge device. This implementation uses BGP protocol for the MPLS connectivity. Services such as management, SCADA, and so on are provisioned with different VRFs. The Cisco IR8340 acts as the layer 3 gateway for these services. These services and their related subnets are exchanged over the MPLS network using BGP, as the node is being configured as a customer edge router.

Detailed end-to-end configuration of all aggregation devices is out of the scope of this section. This section shows the limited configuration on the customer edge device that necessary to understand the MPLS VPN and layer 3 VPN setup. This section also describes the configurations that are required on Ethernet interfaces for them to act as MPLS WAN backhaul interfaces.

In the wind farm solution, all services from the wind farm network are aggregated in the onshore substation core switch and a redundant link is configured between the core switch and substation router to provide the layer 3 redundant gateway.

The following configurations are required in the substation router for the wind farm network to reach the control center for services.

VRF Services in the Substation Router

The following example shows the configuration for one service. Other services, such as SCADA, are configured in a similar way.

```
vrf definition Management_VRF
 rd 100:1
 route-target export 100:1
 route-target import 100:201
 !
 address-family ipv4
 exit-address-family
!

WAN configuration
interface GigabitEthernet0/0/0
 description connected PE


ip address 192.168.82.2 255.255.255.0
  load-interval 30
 negotiation auto
 mpls propagate-cos
 mpls ip
 mpls label protocol ldp
 mpls ldp discovery transport-address interface
 mpls traffic-eng tunnels
 bfd interval 50 min_rx 50 multiplier 3
```

MPLS Global Configuration

```
!
mpls label protocol ldp
```

```
mpls ldp graceful-restart
mpls ldp router-id Loopback0
```

BGP Configuration

```
interface Loopback0
 ip address 192.168.198.1 255.255.255.255

router bgp 198
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 100.100.100.1 remote-as 200
 neighbor 100.100.100.1 ebgp-multihop 2
 neighbor 100.100.100.1 update-source Loopback0
 !
address-family ipv4
  neighbor 100.100.100.1 activate
  neighbor 100.100.100.1 next-hop-self
  neighbor 100.100.100.1 send-label
 exit-address-family
!
address-family vpnv4
  neighbor 100.100.100.1 activate
  neighbor 100.100.100.1 send-community extended
  neighbor 100.100.100.1 next-hop-self
 exit-address-family
!
address-family ipv4 vrf Management_VRF
  redistribute connected
  redistribute eigrp 900
  neighbor 20.11.0.1 remote-as 200
  neighbor 20.11.0.1 activate
  neighbor 20.11.0.1 next-hop-self
 exit-address-family
```

Configuring WAN Substation using Cisco SD-WAN

The Cisco SD-WAN substation deployment is based on *Cisco SD-WAN End-to-End Deployment Guide* and expands its scope to using Cisco IR8340 as the Cisco SD-WAN edge router. This implementation supports controllers running on the Cisco cloud-managed service.

Deploying WAN Edge Routers (IR8340) using Cisco SD-WAN

For complete information about configuring WAN edge routers using Cisco SD-WAN, see *Substation Automation—The New Digital Substatation Implementation Guide*:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/SA/3-0/IG/SA_3-0_IG_v06.pdf

Configuring WAN Edge Routing for High Availability

HSRP is the Cisco standard method for providing high network availability by providing first hop redundancy for IP hosts on an IEEE 802 LAN that is configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual media access control (MAC) address and an IP address that is shared among a group of configured routers.

HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backups for each other. One of the routers is selected to be the active router and another to be the standby router. The standby router assumes control of the group MAC address and IP address if the active router fails. Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and switch virtual interfaces (SVIs).

For detailed information about HSRP configuration, see *Understand the Hot Standby Router Protocol Features and Functionality*:

https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

The wind farm solution uses a redundant link from the onshore core switch to substation routers and between substation routers.

To configure this link:

1. Configure the active router as shown in the following example.

   This example assumes that VLAN 2001 is enabled for the management_VRF.

```
Interface Vlan 2001
ip address  10.201.201.2 255.255.255.0
standby 1 ip 10.201.201.100
standby 1 priority 10
standby 1 preempt
standby 1 track 100 decrement 10
```

2. Configure the standby router as shown in the following example:

```
Interface Vlan 2001
ip address  10.201.201.3 255.255.255.0
standby 1 ip 10.201.201.100
standby 1 preempt
standby 1 track 100 decrement 10
```

3. Enter the following CLI command to track the status of the WAN interface.

   If the WAN interface on the active router goes down, the standby router becomes active. When the recovery happens, both routers go back to the states they had before the failure.

   Configure the track command cli on the global configuration on router.

   "track 100 interface GigabitEthernet 0/0/0 line-protocol"

Note: For all traffic in the core switch, the HSRP IP address that is configured on the VLAN 2001 is the gateway for the wind farm network so that when a failure occurs in the active router, the standby router uses the HSRP IP address to become the active router, and traffic automatically switches to the current active router.

Implementing Network Control Center and Application Services

This section covers the implementation of services, called *shared services*, that are common to all sites in a wind farm network. Shared services such as Cisco Catalyst Center, ISE, DHCP, and DNS, along with other vertical market-specific applications such as Cisco Cyber Vision Center, must be reachable from each site via VRF.

Configuring a DHCP Server

A dynamic host configuration protocol (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 DHCP to respond to broadcast queries by clients.

A DHCP server can be configured in the network in many ways. In a wind farm implementation, a centralized DHCP server in the control center is installed and configured on a Microsoft Windows 2016 server.

This section covers the DHCP scope and IP pools definition and discusses scope for implementing non-fabric sites in wind farm networks.

For detailed information about DHCP configuration, see *Microsoft Windows Server 2016: DHCP Server Installation & Configuration*.

After the DHCP server is successfully configured on a Microsoft Windows 2016 server, create scopes for all the devices for Cisco Catalyst Center as PnP server with options in the DHCP server.

Domain Name Server

The wind farm implementation that this document describes uses domain name servers (DNSs) that run on a Microsoft Windows 2016 server (and that are collocated on a DHCP server in wind farm control center network).

For detailed information about configuring DNS on a Microsoft Windows 2016 server, see "Implement Domain Name System" in *Exam Ref 70-741 Networking with Windows Server 2016*, which is available from the Microsoft Press Store.

Cisco Catalyst Center Installation and Configuration

Cisco Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. Cisco Catalyst Center provides a centralized management dashboard for complete control of wind farm networks.

Cisco Catalyst Center is a dedicated hardware appliance powered through a software collection of applications, processes, services, packages, and tools, and 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.

For information about installation and network configuration of Cisco Catalyst Center, see *Cisco Catalyst Center Second-Generation Appliance Installation Guide, Release 2.3.5*:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_3_5_2ndGen.html

Cisco ISE Installation and Configuration and Integration with Cisco Catalyst Center

Cisco Identity Services Engine (ISE) is a policy-based access control system that enables and enforces compliance and infrastructure security. ISE is an integral part of networks, acting as the authentication, authorization, and accounting (AAA) server for device identity management, access control, and enforcement of access policies.

In the wind farm solution, ISE is coupled with Cisco Catalyst 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 that rely on IP address access lists.

ISE Installation and Initial Configuration

A centralized standalone deployment of ISE is configured with Cisco Catalyst Center in the shared services network as shown in the network topology in Figure 2.1. ISE can be installed in various ways. OVA deployment of ISE as a virtual machine is used in this implementation.

For ISE installation instructions, see *Cisco Identity Services Engine Installation Guide, Release 3.2*:

https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/install_guide/b_ise_installationGuide32.html

After ISE installation and basic configuration is complete, ISE must be integrated with Cisco Catalyst Center. For instructions, see “Cisco Catalyst Center and Cisco ISE Integration” in *Cisco Catalyst Center Administrator Guide, Release 2.3.3*.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-3/admin_guide/b_cisco_dna_center_admin_guide_2_3_3/b_cisco_dna_center_admin_guide_2_3_3_chapter_010.html#id_54524

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

After integrating ISE with Cisco Catalyst Center using PxGrid, information sharing between ISE and Cisco Catalyst Center is enabled, including sharing of device information and group information. This sharing allows Cisco Catalyst 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 ISE and Cisco Catalyst Center, 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.

Cisco Firepower Management Center installation and Configuration

Firepower Management Center (FMC) is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for a Firepower System deployment. FMC controls the network management features on your devices, including switching, routing, NAT, VPN, and so on.

In the wind farm solution, FMC is deployed as a virtual machine. For more information, including detailed FMC configuration steps, see *Firepower Management Center Configuration Guide, Version 7.0*:

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

Cisco Cyber Vision Center Global Center

The Cisco Cyber Vision (CVC) Global Center feature allows the synchronization of several centers within a single repository. The Global Center aggregates centers into a single application and presents a summary of several center activities.

After the setup of a local Cyber Vision Center and a Global Center is complete, the local center synchronization can be initialized from the Global Center. This process consists of the enrollment of a local Cyber Vision center with a Global Cyber Vision Center. When the local center is enrolled, its data is synchronized incrementally. If needed, the local Cyber Vision Center can be unenrolled later, and Global Center then removes all data form that local center. The unenrolled center becomes available for another enrollment.

For information about installing and configuring CVC Global Center, see “Configuring the Center” in *Cisco Cyber Vision Center VM*

Installation Guide, Release 4.1.2:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/Center-VM/Release-4-1-2/b_Cisco_Cyber_Vision_Center_VM_Installation_Guide/m_Configure_the_Center_CENTER_VM_v3_4_0_0.html#topic_5722

Cisco Stealthwatch Management Console installation and Configuration

Cisco 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 related performance information. The SMC client software allows you to access the SMC's graphical user interface (GUI) from a local computer that has 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.

For more detailed information about Stealthwatch design, see "Cisco Secure Network Analytics (Stealthwatch)"in *Cisco Solution for Renewable Energy Offshore Wind Farm1.0 Design Guide*:

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/wind-farm-design-guide.pdf

For information about installing Stealthwatch Manager (also known as SMC) Virtual Edition without a datastore, see *Cisco Secure Network Analytics Virtual Edition Appliance Installation Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_4_2_VE_Appliance_Installation_Guide_DV_1_3.pdf

For information about configuring Stealthwatch Manager (also known as SMC) Virtual Edition without a datastore, see *Cisco Secure Network Analytics System Configuration Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_4_2_System_Configuration_Guide_DV_1_2.pdf

Note: Make sure to activate Cisco Smart Software Licensing for the SNA appliances (SMC and SFC) after the installation and configuration. For information about SNA licensing, see *Cisco Secure Network Analytics Smart Software Licensing Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/license/7_4_2_Smart_Software_Licensing_Guide_DV_1_0.pdf

Chapter 9: Implementing Network Management and Automation

This chapter includes the following topics:

- Preparing Cisco Catalyst Center and Switches for Device Onboarding
- FAN and TAN Ring Devices Onboarding (Day-0 Provisioning)
- Configure the FAN REP Ring Using the REP Workflow
- Day N Configurations using Cisco Catalyst Center Templates
- Adding a New Switch to a FAN REP Ring
- Network Assurance

Preparing Cisco Catalyst Center and Switches for Device Onboarding

This section provides information about discovering and onboarding wind farm devices to Cisco Catalyst Center. Cisco Catalyst Center helps make management of devices easier.

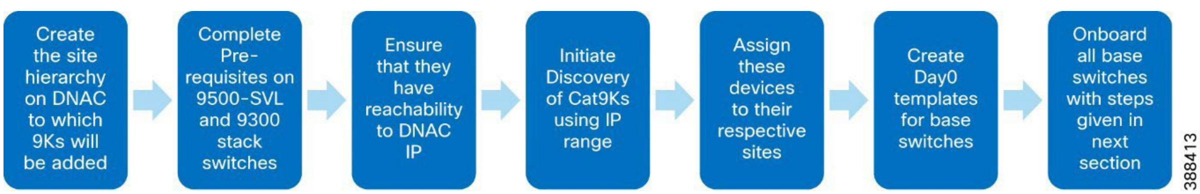
For more detailed information about Cisco Catalyst Center and related configurations, *see Cisco Catalyst Center User Guide, Release 2.3.5*:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5.html

For managing devices in a wind farm network with Cisco Catalyst Center, begin by discovering the core switches of each layer (OSS and ONSS). This section describes the discovery and onboarding of devices in the OSS network. Similar steps can be followed to discover and manage devices in the ONSS network.

Figure 9-1 shows the workflow for discovering and onboarding devices to Cisco Catalyst Center.

Figure 9-1: Workflow for Onboarding Devices to Cisco Catalyst Center



After devices are all onboarded, the 3400 FAN and TAN rings can be formed into REP rings by using a Cisco Catalyst Center workflow or templates.

To onboard devices to Cisco Catalyst Center, follow these steps:

1. Choose **Design > Network Hierarchy** to create the site hierarchy in Cisco Catalyst Center to which Cisco 9000 and 3400 devices are to be added.

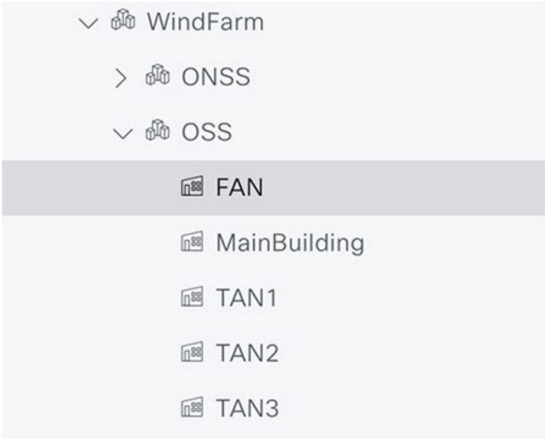
   For detailed steps and an explanation of network hierarchy, see *Cisco Catalyst Center User Guide, Release 2.3.5*:

   https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5/m_design-the-network-hierarchy.html

   The devices are segregated into different sites for easier provisioning of the devices.

   Figure 9-2 shows an example of a site hierarchy for the wind farm solution. Note that, alternatively, all devices can be added under a single site.

Figure 9-2: Site Hierarchy in Cisco Catalyst Center



2. Configure Cisco 9000 switches, as shown in the following examples:

   - Cisco 9500 SVL configuration:

```
hostname WF-OSS-C9500
username dna privilege 15 password 0 Cisco@123
enable secret 0 C!sco123
ip domain name wf.com
!
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 cisco123 RW
snmp-server user cisco default v3 auth sha cisco123 priv aes 128 cisco123
!
```

   - Cisco 9300 aggregation configuration:

```
hostname WF-OSS-C9300Agg
ip domain name wf.com
username dna privilege 15 password 0 Cisco@123
enable secret 0 C!sco123
pnp startup-vlan 101
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 cisco123 RW
snmp-server user cisco default v3 auth sha cisco123 priv aes 128 cisco123
!
netconf-yang
```

   - Cisco 9300 access:

```
hostname WF-OSS-C9300Access
ip domain name wf.com
username dna privilege 15 password 0 Cisco@123
enable secret 0 C!sco123
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 cisco123 RW
snmp-server user cisco default v3 auth sha cisco123 priv aes 128 cisco123
!
netconf-yang
```

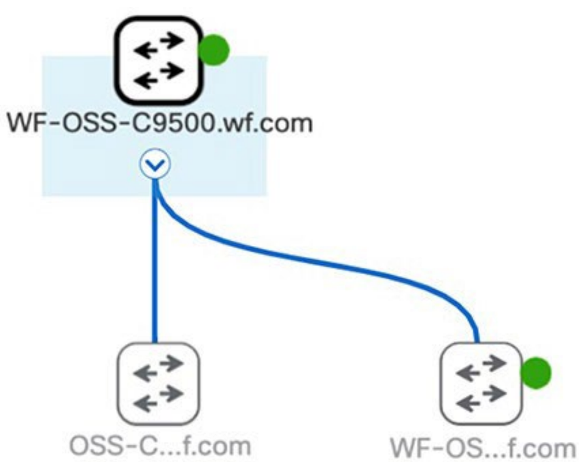
3. Verify that all three devices can reach Cisco Catalyst Center by initiating a ping to Cisco Catalyst Center from each of the three devices.
4. Perform the following actions to initiate the discovery of core switches in the OSS network.

   Similar steps can be performed to discover switches in the ONSS network.

   a. From the Dashboard menu, choose **Tools > Discovery**
   b. Click **Add Discovery** and choose the discovery type as **IP Address Range**.
   c. Enter the IP range in the management network for the devices, then click **Next**.
   d. Complete the subsequent steps by choosing the CLI credentials, SNMPv3, and Netconf port, then click **Next**.
   e. Choose **ssh protocol**, then click **Next**.
   f. Choose the site to which the devices are to be added, then click **Next**.
   g. Verify the summary, then click **Start Discovery**.

After the discovery process completes, the discovered core switches appear in the **Provision> Inventory > Topology** page.

Figure 9-3: Discovered Core Switches



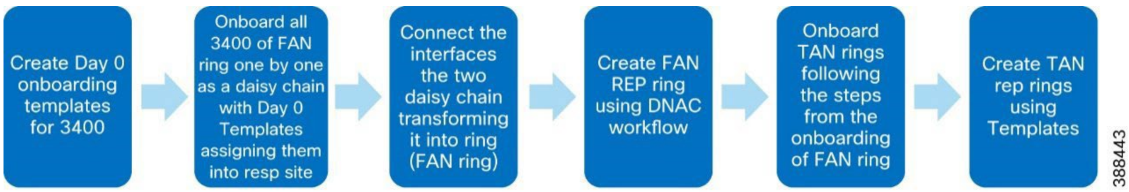
FAN and TAN Ring Devices Onboarding (Day-0 Provisioning)

FAN and TAN rings consist of 3400 switches that are onboarded to Cisco Catalyst Center as separate daisy chains that are later closed to form a ring.

As a prerequisite for onboarding the FAN and TAN rings, the intended final ring must be broken into two daisy chains to ensure that there is only one upstream switch via which the switch is being reached by Cisco Catalyst Center for PnP. The switches are sequentially onboarded to Cisco Catalyst Center one by one until the entire topology onboard is complete. For selecting the linear daisy chain for the intended final ring topology, the ring can be broken at any desired point, resulting in two daisy chains. For optimization, we recommend that the ring be broken in the middle.

Figure 9-4 shows the workflow for onboarding FAN and TAN rings to Cisco Catalyst Center:

Figure 9-4: Workflow for Onboarding FAN and TAN Rings



Create Day 0 Templates for 3400 Onboarding

Create a day 0 template that includes trunk and allowed VLAN configurations for interfaces of the 3400 switches that connect to the next 3400 of the daisy chain.

For information about creating templates in Cisco Catalyst Center, see *Cisco Catalyst Center User Guide, Release 2.3.5*:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5/b_cisco_dna_center_ug_2_3_5_chapter_01000.html

The day 0 template should include the following content:

```
pnp startup-vlan 101
  interface $interface
  switchport mode trunk
  switchport trunk allowed vlan 1-2507,2509-4094
```

Onboard the FAN Ring

1. Connect the first 3400 switches of both daisy chains (obtained by breaking the FAN ring in the middle) to be onboarded to the 9300 aggregation per the wind farm topology.

   (The two daisy chains must be connected on separate stack members of the 9300 aggregation stack to achieve full redundancy.)

2. Reload the 3400 switch to trigger the PnP if it has no previous configuration.

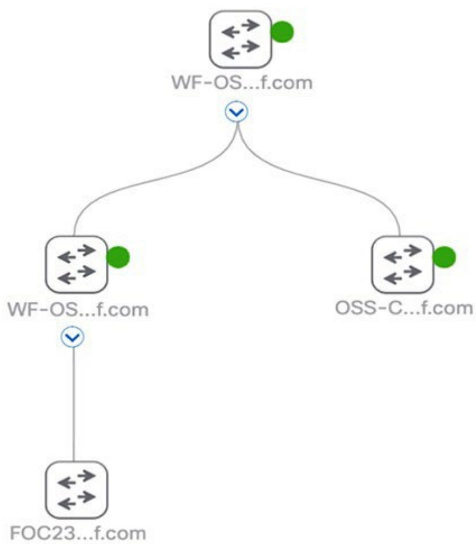
   If the 3400 switch has any existing configuration, enter the following commands on the switch to remove all configurations before starting the onboarding process:

```
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
conf t
crypto key zeroize
Yes
!
no crypto pki certificate pool
Yes
vtp mode transparent
End
write erase

Reload
no
```

3. After the switch reboots, PNP is triggered and the device appears under **Provision > Plug and Play** with a state of **Unclaimed**, check the checkbox for the device and choose **Actions > Claim**.
4. Enter the hostname and site to which the switch is to provisioned in the **Hostname** and **Site** fields.
5. Attach a day 0 template by clicking the attach symbol and choosing the template from the list of available templates.

   The **State** field for the device changes from **Planned** to **Onboarding** and then to **Provisioned** . After the device is onboarded, the device appears in the topology under **Main menu > Provision > Inventory > Topology**, as shown in figure 9-2. Nodes can be added to this chain by connecting the new 3400 to the last onboarded 3400 switch of the daisy chain and repeating the steps 1 through 4.

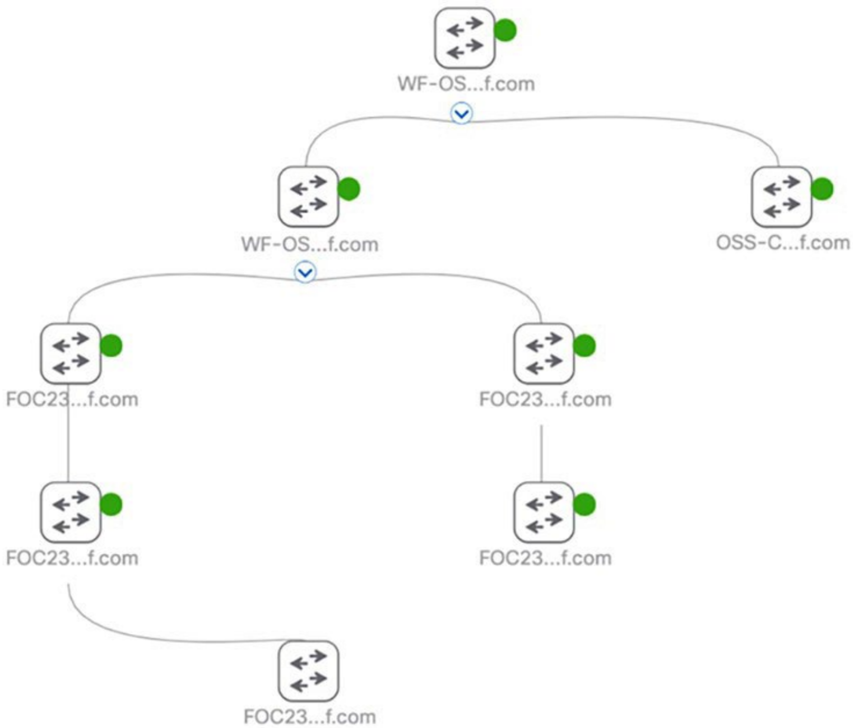
Figure 9-5: Onboarding the First 3400 Switch



After completing the previous steps, onboard the second daisy chain that was obtained from breaking the ring. To achieve redundancy, the second daisy chain starting at 9300 aggregation must be connected to the second stack member of the 9300 aggregation switch stack.

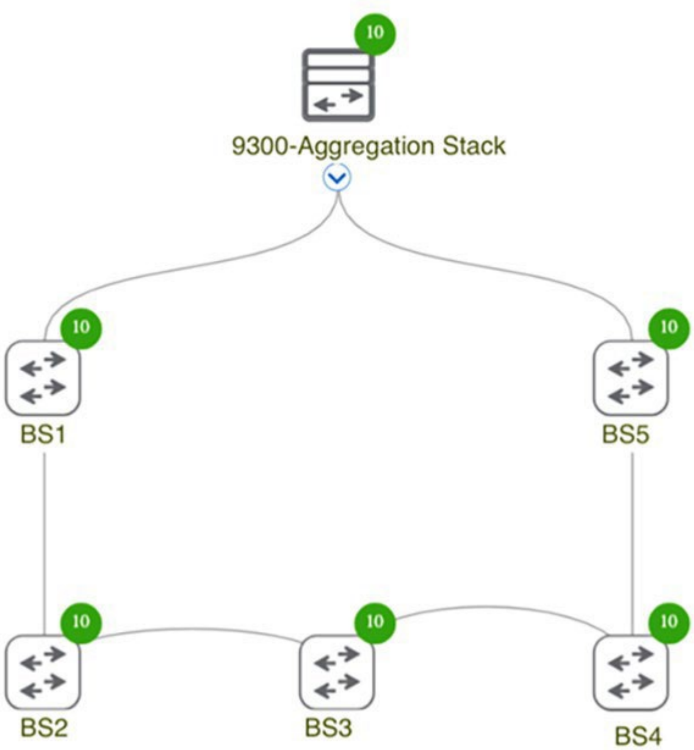
After onboarding the 3400 switches of both daisy chains of the ring is complete, verify the topology by choosing **Provision > Inventory > Topology**. The display should resemble the example shown in Figure 9-6.

Figure 9-6: Linear Daisy Chain Containing Five Nodes



Connect the interfaces of the end nodes of the two daisy chains, which transforms the two daisy chains into the FAN ring. The FAN ring topology should be as shown in Figure 9-7. You can verify the topology by choosing **Provision > Inventory >Topology**.

Figure 9-7: FAN Ring Obtained from Connecting the End Nodes of the two Daisy Chains



Configure the FAN REP Ring Using the REP Workflow

The FAN ring that is configured by the previous steps runs STP by default for loop avoidance. Configure REP on this ring by using the Cisco Catalyst Center REP workflow.

To create the FAN REP ring, follow these steps:

1. From the **Main Menu**, choose **Workflows > Configure REP Ring (Non-Fabric)**, then click **Let's Do it**.
2. Choose the root device 9300-Aggregation Stack and the two adjacent 3400s (shown as BS1 and BS5 in figure 9-4) in the next tab, then click **Next**.
3. In the **Review your REP Ring discovery selections** window, assign a name for the REP ring by entering it in the **Ring Name** field, then click **Provision**.
4. Click **Next**.

When the creation process completes, the **REP Ring Configuration is Successful** message appears.

Note: The Cisco Catalyst Center REP workflow requires that there are no subrings within the ring to be configured with REP when you begin the workflow. Therefore, we recommend onboarding TAN rings only after creating the FAN REP ring with this workflow.

Onboard TAN Switches

There are two TAN types used in the wind farm solution:

- TAN without HA, which has a 3400 switch linearly connected to a FAN switch (identified as TAN1 in the wind farm topology in Figure 2-1)
- TAN with HA, which has 3400 switches connected in two types of rings:
  - Closed REP ring (identified as TAN2 in Figure 2-1)
  - Open REP ring (identified as TAN3 in Figure 2-1)

For more information about TANs, see Configuring TAN with High Availability and REP Subtended Ring.

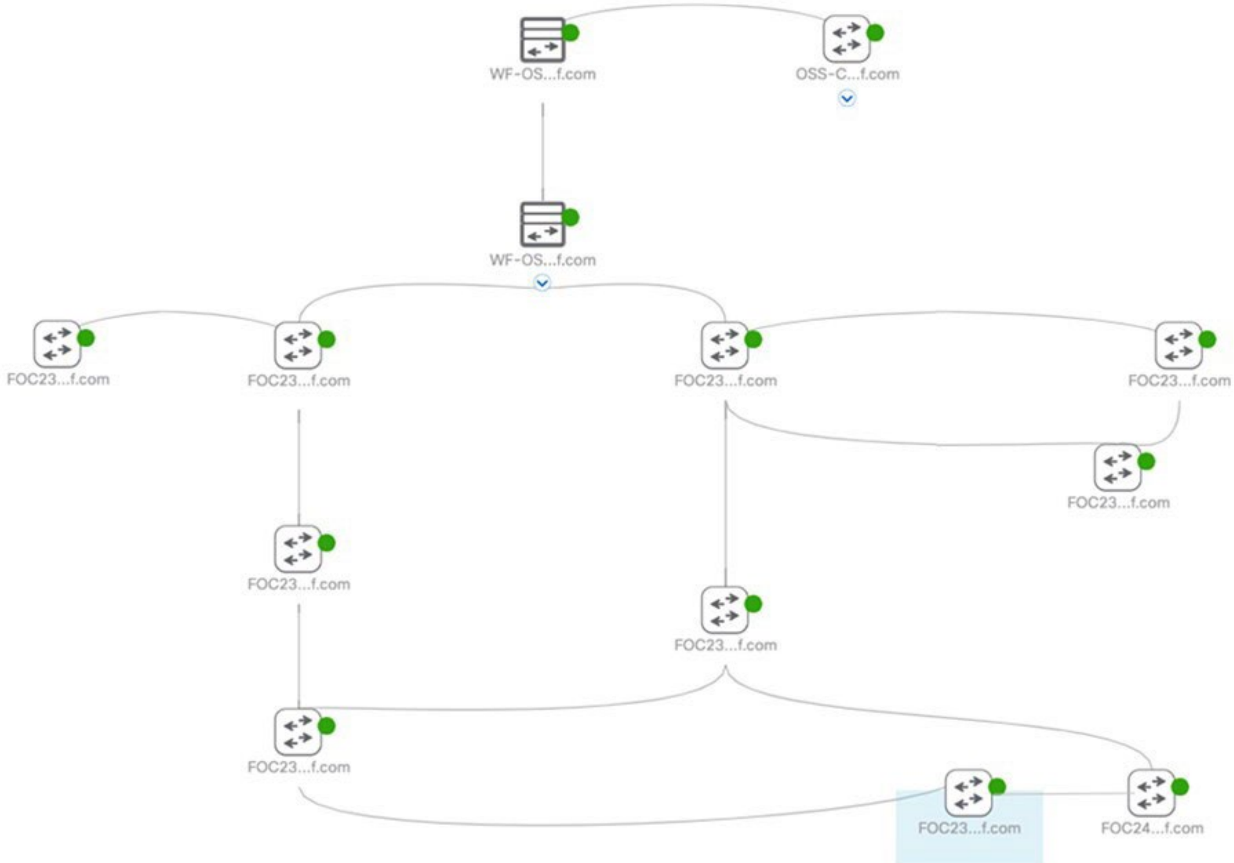
To onboard a TAN without HA (TAN1), connect the 3400 switch linearly to one of the FAN ring members (represented as BS1 in Figure 2-1) then follow Steps 2 to 4 in Onboard the FAN Ring.

To onboard TAN with HA:

- TAN2 ring onboarding: Connect two 3400 switches to a FAN ring member (represented as BS4 in wind farm topology), which acts as the edge switch for the REP closed segment. These two TAN switches are then onboarded to Cisco Catalyst Center as two separate daisy chains in the FAN ring onboarding steps. After all member switches are onboarded as a daisy chain, the interfaces of end switches are connected to close the ring.
- TAN3 ring onboarding: First connect two TAN3 ring members to two different switches of the FAN ring (identified as BS2 and BS3 in the wind farm topology), then follow the FAN ring onboarding steps. BS2 and BS3 act as edge switches for the REP open segment.

After all TAN switches are onboarded and rings are closed, verify the topology in Cisco Catalyst Center by choosing **Provision > Inventory > Topology**. Figure 9-8 shows an example topology display.

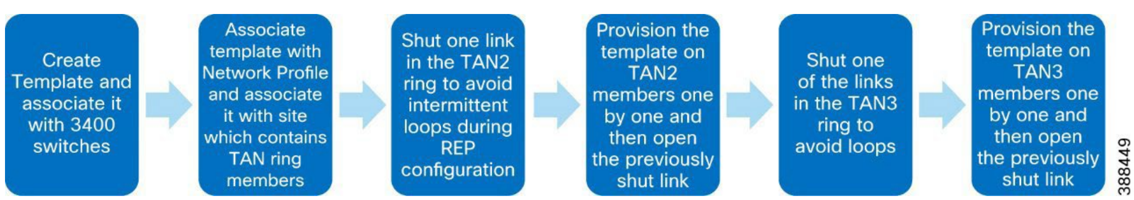
Figure 9-8: Cisco Catalyst Center Topology with all Devices Onboarded



TAN REP Ring Configuration

TAN REP rings run STP for loop avoidance by default. You can configure the TAN rings with REP by using Cisco Catalyst Center templates. Figure 9-9 shows the workflow for configuring TAN open and closed REP rings using Cisco Catalyst Center templates.

Figure 9-9: Workflow for Configuring TAN Open and Closed REP Rings



1. Perform the following actions to create a template in Cisco Catalyst Center to configure REP in the TAN rings.

   Cisco Catalyst Center templates can be used to configure REP in the TAN rings. This section covers only the configuration to be written inside the Template for configuring REP on the TAN rings. For more detailed information about creating templates in Cisco Catalyst Center see “Create Templates to Automate Device Configuration Changes” in *Cisco Catalyst Center User Guide, Release 2.3.5*:

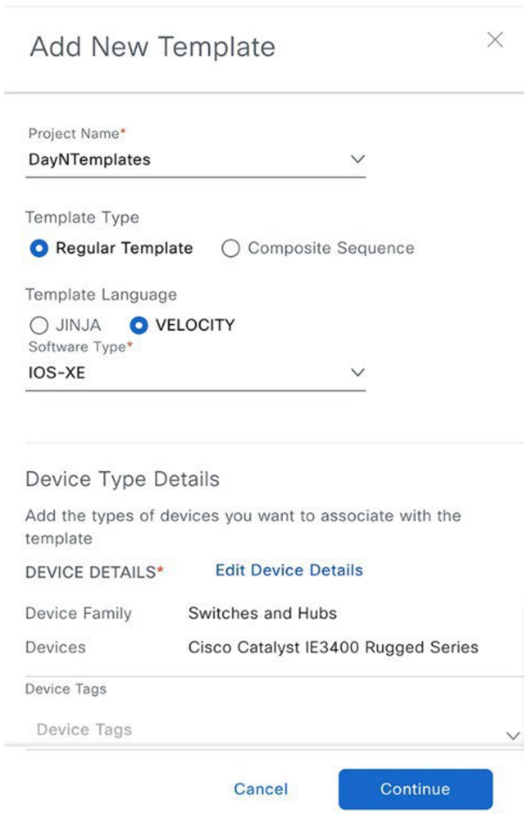
   https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5/b_cisco_dna_center_ug_2_3_5_chapter_01000.html

   a. From the Main menu, choose **Tools > Template Hub > + > Add -> New Template**.

   b. Enter the Template name as **RepRingCreation** and associate it with a project.

   c. Configure additional fields as shown in Figure 9-10, then click **Continue**.

Figure 9-10: Creating Template for Configuring REP on TAN Ring



d. Enter the contents of the template as follows:

```
#if ($apply_rep == 1)
vlan $rep_admin_vlan
exit
rep admin vlan $rep_admin_vlan

#if ($isedge == 1)
interface $int_first
rep segment $segment edge
rep stcn segment $mainRingSegId
no shut

interface $int_second
rep segment $segment edge
rep stcn segment $mainRingSegId
no shut

#else

interface range $int_first , $int_second
rep segment $segment
no shut
#end

#else
interface $int_first
no rep segment $segment

interface $int_second
no rep segment $segment

#end
```

2. Associate the template to a network profile by clicking **Attach to Network Profile** in the **Template** window.
3. Choose the network profile, click **Save**, then click **commit**.
4. Associate this network profile with the Cisco Catalyst IE3400 Rugged Series device type by choosing **Design > Network Profiles > Edit**.
5. Choose the site for the TAN ring in **Design> Network Profiles> Site.**

   The template is ready to be provisioned**.**

   Before applying REP templates on TAN switches, shut one of the links in the TAN ring to avoid any intermittent loop formation during REP configuration.

   The link can be shut either by creating a Cisco Catalyst Center template or by issuing a **shutdown** command for the interface on the switches cli. For TAN2, shut the link between BS4 and NS2 in the wind farm topology.

   The following Cisco Catalyst Center template can be created for shutting or unshutting an interface:

```
#if ($shut == 1)
finterface $int_first
shutdown
#else
interface $int_first
no shut
```

6. Apply the REP configuration template on TAN2 switches one by one, starting with the farthest switch that is reachable from Cisco Catalyst Center.

   Provision the REP template on the TAN2 switches in the following sequence:

   NS2 → NS1 → BS4

   To provision the REP configuration template:

   a. From the Main menu, choose **Provision > Inventory**.
   b. Check the checkbox next to TAN2 switch under the configuration (NS2/NS1/BS4).
   c. From the **Actions** drop down menu, choose **Provision > Provision Device**, then click **Next**.
   d. Ub the **Devices** window, choose the device to be provisioned.
   e. Enter the values for templates variables as shown in Table 9-1, click **Next**, then click **Next** in the next page that appears.

Table 9-1: TAN2 REP Configuration Template Variables

Variable Name	Use	Value
apply_rep	To apply or remove rep configuration	1/0
rep_admin_vlan	REP admin VLAN	VLAN ID to be used as REP admin VLAN
isedge	Edge port or non edge port (1 for edge port and 0 for non edge ports)	Enter **1** for BS4 (because the edge port is configured on BS4) and **0** for NS2 /NS1 (because the non-edge ports are configured on NS2/NS1 of the TAN2 ring)
int_first	First interface ID of device that is a part of the TAN ring	Interface ID used in TAN ring formation
segment	TAN REP ring segment ID	Segment ID of choice (segment ID 2 is used in the wind farm topology for TAN2 as an example)
mainRingSegId	FAN REP ring segment 1	Segment ID used in REP configuration of FAN ring (segment ID 1 is used in the wind farm topology for FAN ring as an example)

int_second	Second interface ID of the device that is a part of the TAN ring.	Second interface of the device used in TAN ring formation

f. In the **Provision Device** window, click **Apply**.

g. In the **Preview Configuration-Provision Device** window, verify the configuration preview that is generated by Cisco Catalyst Center, then click **Deploy**.

7. Repeat Step 3 to 6 for TAN3 REP ring creation by first shutting the link between BS3 and NS2 of the TAN3 ring of the wind farm topology and then provisioning the REP template in the sequence NS2 → NS1 → BS2 → BS3.

   See Table 9-2 for values of the template variables for TAN3 to be entered.

Table 9-2: TAN3 REP Configuration Template Variables

Variable Name	Use	Value
apply_rep	To apply or remove rep configuration.	1/0 (**1** to apply REP, **0** to remove REP configuration).
rep_admin_vlan	REP admin VLAN.	VLAN ID to be used as REP admin VLAN.
isedge	Edge port or non edge port. (1 for edge port and 0 for non edge port.)	Enter **1** for BS2 and BS3 and **0** for NS1 and NS2.
int_first	First interface ID of the device that is a part of the TAN ring.	Interface ID used in TAN ring formation.
segment	TAN REP ring segment ID.	Segment ID of choice (segment ID 2 is used in the wind farm topology for TAN2 as an example).
mainRingSegId	FAN REP ring segment ID.	Segment ID used in REP configuration of FAN ring (segment IS 1 is used in the wind farm topology for FAN ring as an example).
int_second	Second interface ID of the device that is a part of the TAN ring.	Second interface of the device used in TAN ring formation. Leave this field blank for switches BS2 and BS3 because only one interface of these switches is a member of the TAN3 ring.

Day N Configurations using Cisco Catalyst Center Templates

Configuration updates can be made on wind farm devices by using Cisco Catalyst Center templates. Templates can be created on Cisco Catalyst Center with configurations to add VRFs, add VLANs, create port-channels, and so on.

For more information about content to add for various configurations, see Appendix B: Cisco Catalyst Center Day N Templates.

Adding a New Switch to a FAN REP Ring

A new switch can be added to an existing FAN REP ring that has been created in Cisco Catalyst Center. To do so, follow these steps:

1. Verify that the interfaces to which the new switch is going to be connected has a REP segment ID configured and ZTP enabled by entering the command **show run interface *interface-id*** on the switch console.
2. Connect the new switch between the two existing 3400 switches using the same physical connection that was used between the existing 3400 switches.

3. Onboard the new switch by triggering PnP and ensuring that no previous configuration exists on the newly added switch.

   See the onboarding steps in FAN and TAN Ring Devices Onboarding (Day-0 Provisioning).

   Ensure that you add this new switch in the same Cisco Catalyst Center site as the FAN switches.
4. Click the **REP rings** tab and verify that the switch has been added to the REP ring automatically.

Network Assurance

Cisco Catalyst Center Assurance is used in the wind farm solution to provide a detailed view of the network. It monitors power consumption and the status of connected clients and provides network related insights.

For more information about Cisco Catalyst Center Assurance and information about enabling it, *see Cisco DNA Assurance User Guide, Release 2.3.5*:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-3-5/b_cisco_dna_assurance_2_3_5_ug.html

Chapter 10 Implementing Network Security and QoS

This chapter includes the following topics:

- Implementing Network Security
- Implementing QoS
- Implementing Multicast Traffic Support in an Offshore Substation

Implementing Network Security

Configuring Firepower Zones and Policies for OPC-UA

For information about configuring zones and policies on Firepower, see Configuring Firepower for Wind Farm Solution Use Cases.

Configuring Cisco Cyber Vision Sensors on TAN and FAN Ring

There are two types of Cyber Vision sensors: hardware and network. The hardware sensor is the Cyber Vision IOx application that is installed on a Cisco Industrial Compute Gateway 3000 (IC3000). The network sensor is the Cyber Vision IOx application that is installed on supported switches and routers. In the wind farm solution, only network sensors on IE switches are used, as described in the design.

There are three ways to install network sensors: using the switch CLI, using the switch web interface, and using Cyber Vision Center Extension. This document discusses the network sensor installation using Cyber Vision Center Extension. For additional information, see *Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300, Release 4.1.0*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/IE3400/b_Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300.html

Before installing sensors, perform the following actions on the IE switches in the FAN and TAN:

1. Ensure network reachability between the Cyber Vision Center and the IE switches in the FAN and TAN.

   A separate collection network VLAN is configured in the Management_VRF for sensors on IE switches by using switch CLLs or Cisco Catalyst Center day N templates.

2. Ensure that IE switches in the FAN and TAN are configured with the collection network VLAN.

   On a FAN ring IE3400 switch, VLAN 102 is configured for Cyber Vision sensors as shown in the following example:

   FAN-IE3400-BS1# **show vlan**

```
VLAN Name                                            Status     Ports
------ --------------------------------------------- ------------- ---------------------------------------------
1    default                                         active     Gi1/3, Gi1/4, Gi1/5, Gi1/6, Gi1/7, Gi1/8,
Gi1/9
                                                                Gi1/10, Ap1/1, Gi2/1, Gi2/2, Gi2/3,
Gi2/4, Gi2/5
                                                                Gi2/6, Gi2/7, Gi2/8
101  VLAN0101                                    active
102  CV_Sensor                                       active
1002 fddi-default                                    act/unsup
<snipped>
```

3. Configure an SVI in the collection network VLAN on the IE switch where the sensor is to be installed.

   An example SVI configuration on the collection VLAN in IE3400 switch is:

   FAN-IE3400-BS1# **show run interface Vlan 102**

```
!
interface Vlan102
 ip address 10.10.102.114 255.255.255.0
end
```

4. Verify that the IE switch can reach the CVC collection interface IP address at the OSS Infrastructure network in the CCI headquarters site.

   To do so, on the IE switch in FAN, ping the CVC collection network interface. For example:

   FAN-IE3400-BS1# **ping 10.10.100.30 source vlan 102**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.30, timeout is 2 seconds:
Packet sent with a source address of 10.10.102.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

   Note: The IP address 10.10.100.30 in this example is the IP address of the Cyber Vision Center collection network interface that is configured during the installation of CVC local in the OSS infrastructure. Also note that the CVC needs the appropriate network route and gateway configurations to ensure network connectivity to the sensor network on IE switches.

   A successful ping ensures network connectivity between the CVC (for example, the 10.10. 100.x subnet in the OSS infrastructure network) and IE switches (10.10.102.x collection network for sensors).

The following items must be configured on a switch before a Cyber Vision sensor is installed on it:

- SSH
- IOx and storage formatting
- Data export using encapsulated remote switched port analyzer (ERSPAN)
- Ports

Use the following IP address schema to bring up the CVS application on an IE3400 or IE3300 10G and integrate it to the CVC.

CVC:

Admin interface (eth0): 10.104.206.225

Collection interface (eth1): 10.10.100.30

Collection network gateway: 10.10.100.1

NTP: 10.10.100.1

FAN IE3400 base switch:

Admin IP address: 10.10.102.100

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: 10.10.112.101

Collection subnet mask: 24

Collection gateway: 10.10.112.100

Collection VLAN number: 102

Prerequisite for the sensor application installation on the IE3400 are the following. Configure these items by using an SSH client or the console port.

- Configure access to SSH
- Configure basic parameters

The following steps show the configuration that is needed on IE3400 switches for the sensor installation to then register it with the CVC:

1. Format sdflash and enable IOx on the IE switch by using the following CLI commands:

   FAN-IE3400-BS1# **format sdflash: ext4**

   FAN-IE3400-BS1# **show sdflash: filesys**

   Filesystem: **sdflash**

   Filesystem Path: **/flash11**

   Filesystem Type: **ext4**

   Mounted: **Read/Write**

   FAN-IE3400-BS1# **configure terminal**

   FAN-IE3400-BS1#(config)# **iox**

   FAN-IE3400-BS1#(config)# **end**

   FAN-IE3400-BS1# **show 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 v19.03.13-ce           : Running
   ```

2. Use the following commands to configure a VLAN for traffic mirroring.

   This configuration ensures that the AppGigabitEthernet port for communications can reach the IOx virtual application so that traffic can be received inside an IOx application.

   configure terminal

   vtp mode off

   vlan 2508

   remote-span

   end

   !

   interface AppGigabitEthernet 1/1

   switchport mode trunk

   exit

   !

3. Exclude Capture VLAN 2508 on all trunk interfaces in the IE3400 switch, except the AppGigabitEthernet 1/1 interface:

   interface GigabitEthernet1/1

   switchport trunk allowed vlan 1-2507,2509-4094

   switchport mode trunk

   end

4. 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.

5. Save the configuration:

   wr mem

For more information, see “Initial Configuration” section in *Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300*:

https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/IE3400/b_Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300/m_Installation_procedures_IE3400_Catalyst_9300_v3_4_0_0.html#topic_5146

6. Perform the steps in the “Procedure with the Cyber Vision sensor management extension” section in *Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300, Release 4.1.0*:

   https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/IE3400/b_Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3300_10G_Cisco_IE3400_and_Cisco_Catalyst_9300/m_Installation_procedures_IE3400_Catalyst_9300_v3_4_0_0.html#topic_5701

OT Flow detection using Cyber Vision Sensors

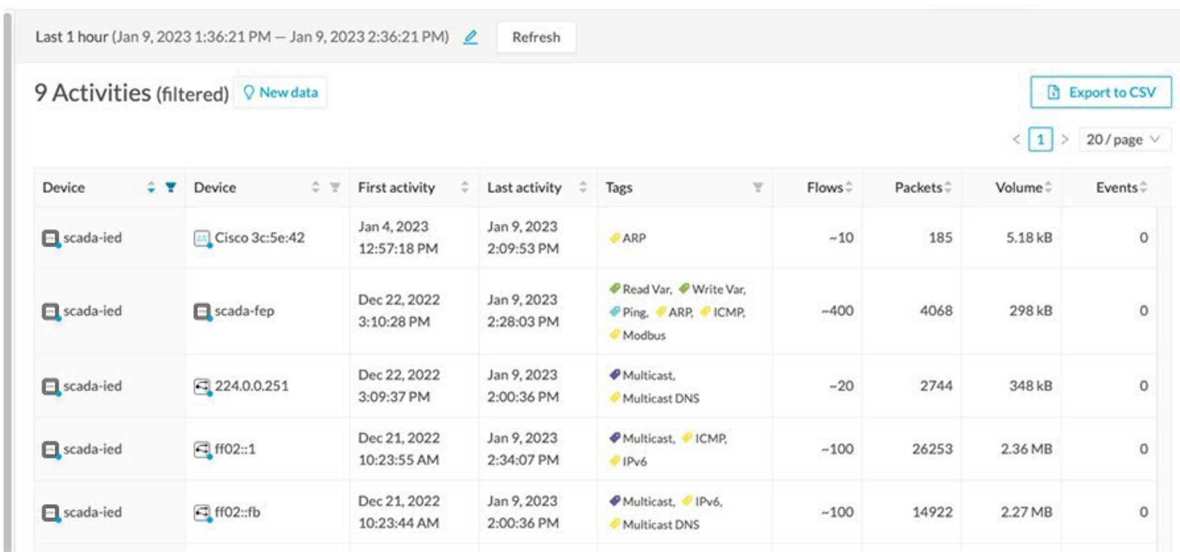
After the Cyber Vision sensor is running on the FAN IE switch, you can view the data that is collected from the sensor on the CVC Dashboard. For example, a SCADA IED device that is connected to a FAN ring base switch sends MODBUS IP traffic to a SCADA FEP server in the OSS infrastructure. This OT flow can be detected by a sensor monitoring the IED port traffic on the IE switch.

To see sensor data, follow these steps:

1. On the CVC Dashboard, choose **Explore - All data**.
2. Click **Activity List**.
3. Click a flow in the list to see more about the flow.

Figure 10-1 shows an OT flow device in the CVC Dashboard.

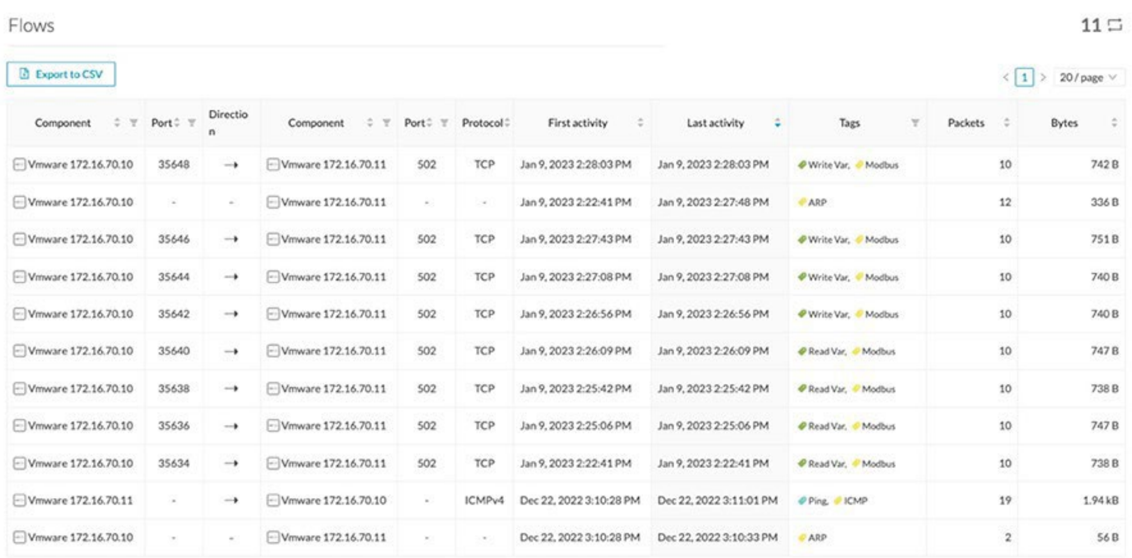
Figure 10-1: CVC Dashboard View of Activities



Device	Device	First activity	Last activity	Tags	Flows	Packets	Volume	Events
scada-ied	Cisco 3c:5e:42	Jan 4, 2023 12:57:18 PM	Jan 9, 2023 2:09:53 PM	ARP	~10	185	5.18 kB	0
scada-ied	scada-fep	Dec 22, 2022 3:10:28 PM	Jan 9, 2023 2:28:03 PM	Read Var, Write Var, Ping, ARP, ICMP, Modbus	~400	4068	298 kB	0
scada-ied	224.0.0.251	Dec 22, 2022 3:09:37 PM	Jan 9, 2023 2:00:36 PM	Multicast, Multicast DNS	~20	2744	348 kB	0
scada-ied	ff02::1	Dec 21, 2022 10:23:55 AM	Jan 9, 2023 2:34:07 PM	Multicast, ICMP, IPv6	~100	26253	2.36 MB	0
scada-ied	ff02::fb	Dec 21, 2022 10:23:44 AM	Jan 9, 2023 2:00:36 PM	Multicast, IPv6, Multicast DNS	~100	14922	2.27 MB	0

Activities in CVC Dashboard 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.

Figure 10-2: CVC Dashboard view of OT Flow Details



Flows 11

Export to CSV

20 / page

Component	Port	Direction	Component	Port	Protocol	First activity	Last activity	Tags	Packets	Bytes
Vmware 172.16.70.10	35648	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:28:03 PM	Jan 9, 2023 2:28:03 PM	Write Var, Modbus	10	742 B
Vmware 172.16.70.10	-	-	Vmware 172.16.70.11	-	-	Jan 9, 2023 2:22:41 PM	Jan 9, 2023 2:27:48 PM	ARP	12	336 B
Vmware 172.16.70.10	35646	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:27:43 PM	Jan 9, 2023 2:27:43 PM	Write Var, Modbus	10	751 B
Vmware 172.16.70.10	35644	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:27:08 PM	Jan 9, 2023 2:27:08 PM	Write Var, Modbus	10	740 B
Vmware 172.16.70.10	35642	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:26:56 PM	Jan 9, 2023 2:26:56 PM	Write Var, Modbus	10	740 B
Vmware 172.16.70.10	35640	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:26:09 PM	Jan 9, 2023 2:26:09 PM	Read Var, Modbus	10	747 B
Vmware 172.16.70.10	35638	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:25:42 PM	Jan 9, 2023 2:25:42 PM	Read Var, Modbus	10	738 B
Vmware 172.16.70.10	35636	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:25:06 PM	Jan 9, 2023 2:25:06 PM	Read Var, Modbus	10	747 B
Vmware 172.16.70.10	35634	→	Vmware 172.16.70.11	502	TCP	Jan 9, 2023 2:22:41 PM	Jan 9, 2023 2:22:41 PM	Read Var, Modbus	10	738 B
Vmware 172.16.70.11	-	→	Vmware 172.16.70.10	-	ICMPv4	Dec 22, 2022 3:10:28 PM	Dec 22, 2022 3:11:01 PM	Ping, ICMP	19	1.94 kB
Vmware 172.16.70.10	-	-	Vmware 172.16.70.11	-	-	Dec 22, 2022 3:10:28 PM	Dec 22, 2022 3:10:33 PM	ARP	2	56 B

The traffic flows that are detected by Cyber Vision sensors are displayed in CVC Dashboard, which you access by choosing **Explore > All data > Activity list**.

For more information about MODBUS and DNP3 OT assets visibility, see “OT Asset Visibility” in *Grid Security Implementation Guide*:

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 Stealthwatch (SNA) NetFlow

In a wind farm network, NetFlow is enabled on Cisco IE switches (IE3400) in the TAN and FAN to monitor network traffic flows. NetFlow can also be enabled on the nacelle and base switches by using the Cisco Catalyst Center day N template feature.

The Cisco IE 3400 switch supports full Flexible NetFlow. The NetFlow feature is an embedded instrumentation within the Cisco IOS-XE software stack to help characterize network flows. It provides visibility into the traffic that flows through a switch or router. Enabling NetFlow provides a trace of every traffic flow in the network without the need for SPAN ports.

All packets with the same source and destination IP addresses, source and destination ports, protocol interface, and class of service are grouped into a flow, and packets and bytes are then tallied and stored in the NetFlow cache. The cache can be exported to a system such as Cisco Stealthwatch, where deeper analysis of the data can be performed to identify threats or malware.

NeFlow Configuration on an IE3400

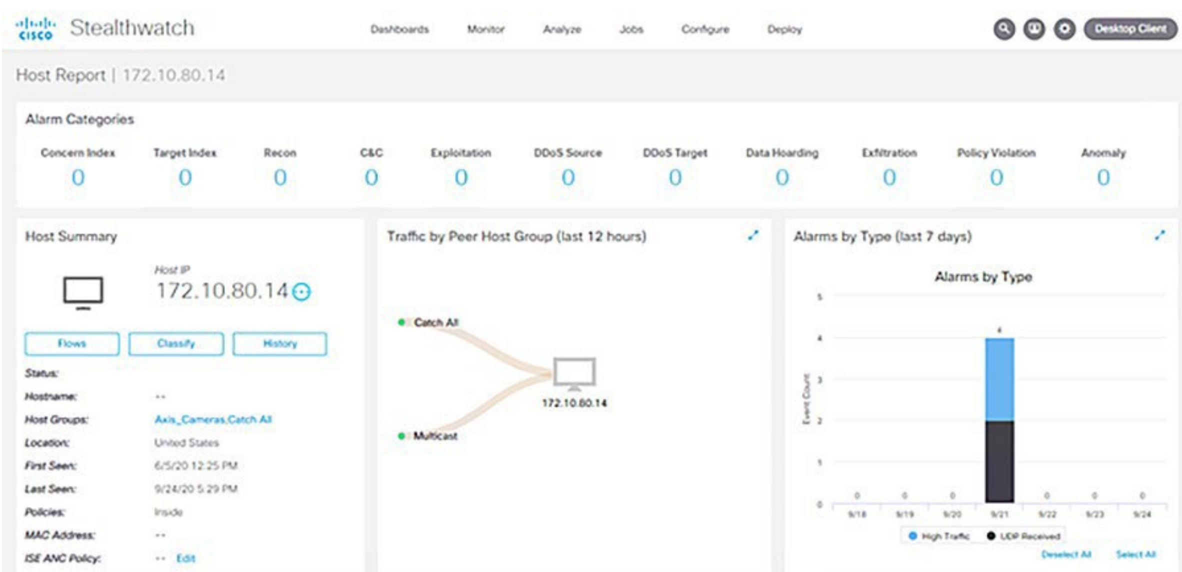
```
ip flow-export destination fc_ip fc_port

##Configure the Flow Record##
flow record fnf-rec
match ipv4 tosmatch 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_ip
 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 of Traffic Flow Monitoring

You can verify the traffic flow monitoring on the SMC dashboard. Figure 10-3 shows an example host report for traffic.

Figure 10-3: Stealthwatch Management Console Dashboard Host Report



Integrating Stealthwatch with Identity Services Engine

The Cisco Stealthwatch Management Center (SMC) can be integrated with the Cisco Identity Services Engine (ISE) using pxGrid. When integrated with ISE, the SMC learns user session information (IP address, username bindings), static Trustsec mappings, and adaptive network control (ANC) mitigation actions for quarantining endpoints.

To integrate Cisco Stealthwatch with ISE, see *Cisco Secure Network Analytics ISE and ISE-PIC Configuration Guide 7.4.2*:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/ISE/7_4_2_ISE_Configuration_Guide_DV_1_0.pdf

Implementing QoS

OSS QoS Configuration for OSS C9300 and C9500 Switches

To configure QoS for C9300 and C9500 switches in the OSS, perform the following steps. Operational technology traffic is matched based on access lists. Other incoming traffic is matched based on DSCP markings.

1. Create an access list to match incoming OT traffic.
2. Create an input class map to match OT traffic based on an ACL and to match other traffic types based on DSCP values.
3. Create an input policy map to set the DSCP values.
4. Allocate bandwidth to different traffic types in the output policy map so that voice traffic is sent in a priority queue.
5. Assign the input and output policy map to the switch.

OSS QoS Configuration for the OSS C3400 Switches

1. Create an access list to match incoming OT traffic.
2. Create an input class map to match OT traffic based on an ACL and to match other traffic types based on DSCP values.
3. Create an input policy map to set the DSCP values.
4. Allocate bandwidth to different traffic types in the output policy map so that voice traffic is sent in a priority queue.
5. Assign the input and output policy map to the switch.

Implementing Multicast Traffic Support in an Offshore Substation

This section describes how to enable support for multicast traffic in an OSS. To enable multicast communication in the wind farm topology between devices across Firepower, configure the 9500-SVL as a rendezvous point for multicast and enable IGMP on Firepower.

Figure 10-4 shows the workflow for enabling multicast.

Figure 10-4: Workflow for Enabling Multicast

To configure devices in the OSS network to enable multicast:

1. Configure the 9500-SVL for multicast.

   Enter the following commands on the 9500 SVL switch CLI to enable multicast on the switch:

```
ip multicast-routing vrf Management_VRF
ip pim rp-address 10.10.100.1
ip pim vrf Management_VRF rp-address 10.10.100.1
ip route vrf Management_VRF 10.10.106.0 255.255.255.0 10.10.100.3

interface Vlan100
ip pim sparse-mode
```

2. Allow multicast through Firepower.

   Because Firepower does not allow multicast traffic through it, configure an access policy to allow it. For more information about multicast configuration in Firepower, see “Multicast Routing for Firepower Threat Defense” in *Firepower Management Center Configuration Guide, Version 6.1*:

   https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/multicast_routing_for_firepower_threat_defense.html

3. Configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host.

   Note: You cannot specify a destination security zone for the rule.

Figure 10-5: Permitting Multicast in an Access Policy

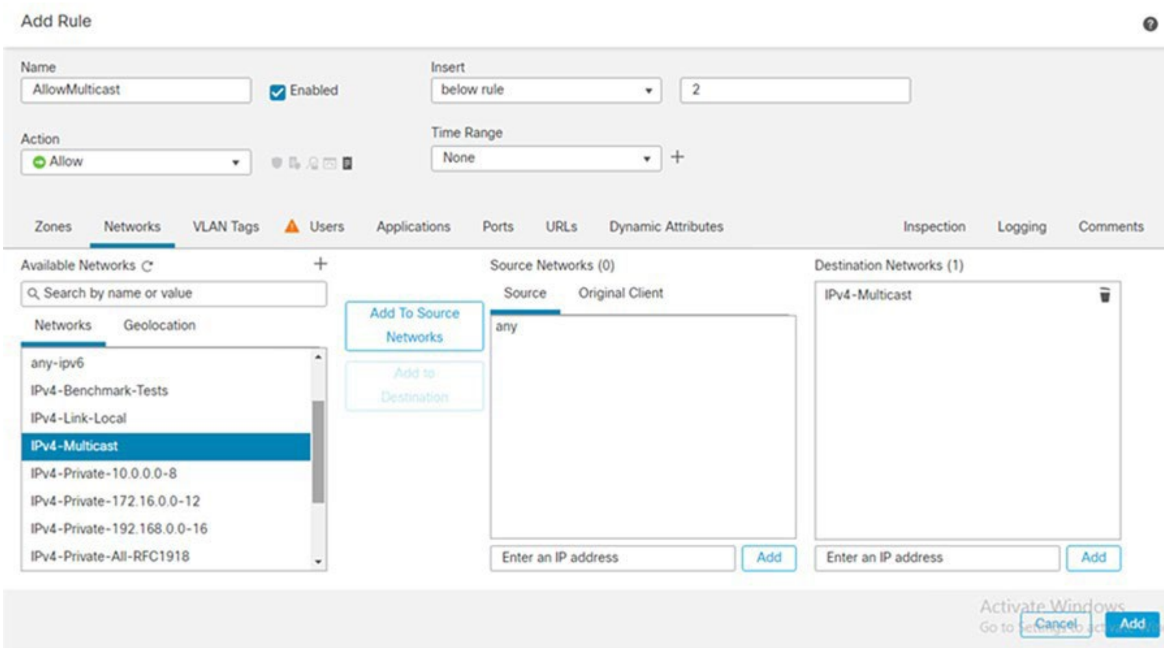
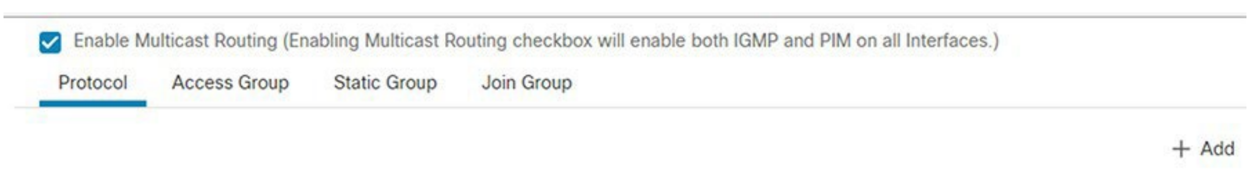


Figure 10-6 shows how an added policy appears.

Figure 10-6: Access Policy with Multicast Traffic Allowed

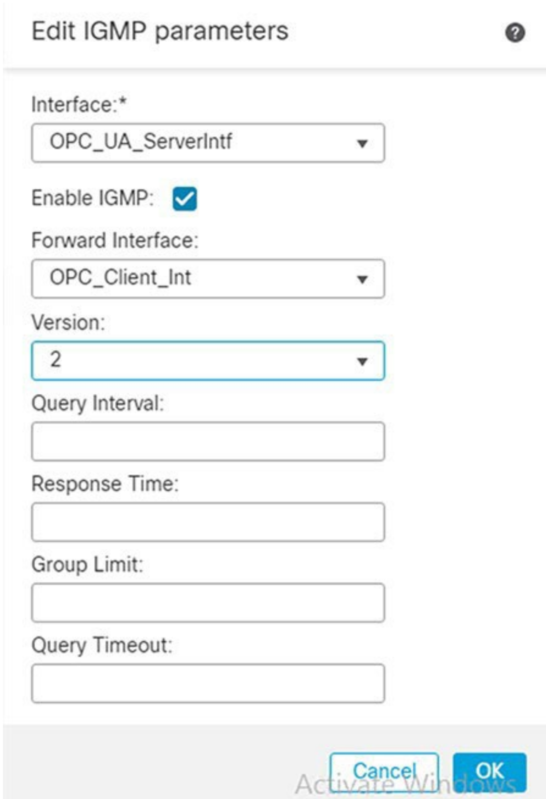
4. Click **Save**.
5. Perform the following actions to enable IGMP on Firepower:
   a. From the Main menu, choose **Routing > Multicast Routing > IGMP**.
   b. Check the checkbox for enabling multicast routing as shown in figure 10-7.

   Figure 10-7: Enabling Multicast



   c. Configure IGMP protocol by clicking **+ Add** at the top right of the page and add the IGMP parameters as shown in figure 10-5, then click **OK**.

Figure 10-8: Configuring IGMP



d. Click **Save**, then click **Deploy** in the Main menu.

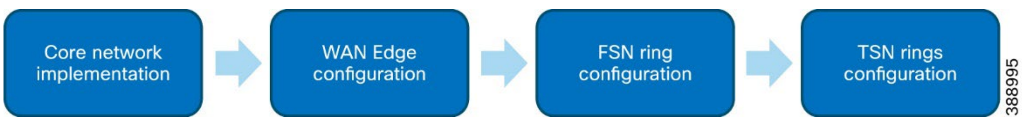
Chapter 11 Turbine Operator Network Implementation

Turbine operator Scada network is parallel network built and operated by Turbine manufacturer. For more details on Turbine operator network refer to the design guide Design Guide Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 at the following link:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf

This network implementation is broken into flow as shown in the diagram below:

Figure 11-1 Network implementation flow for Turbine operator Scada

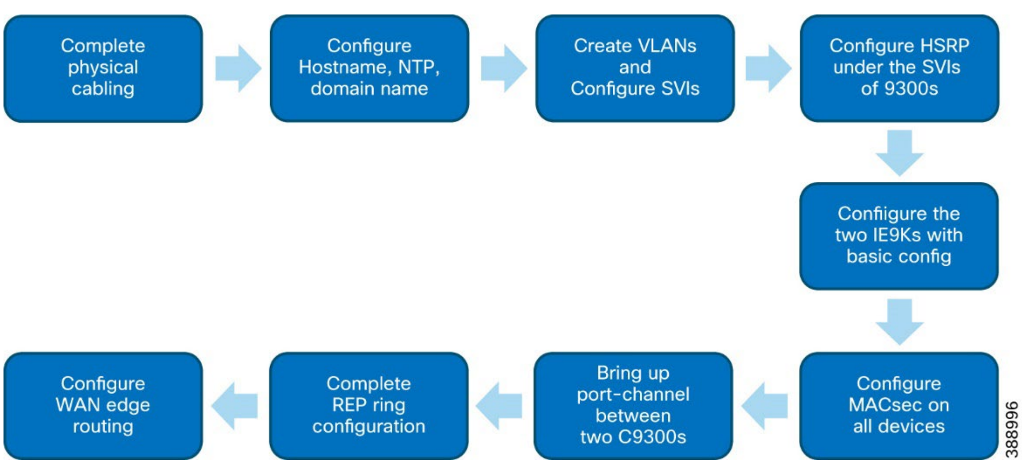


Turbine Operator Core Network Implementation

Cisco Catalyst 9300 switches are used as core switches along with Cisco Industrial Ethernet 9300 in a ring topology . For redundancy, HSRP is configured between the 9300s. These switches are Active-Standby pair and in the event of failure of the Active Catalyst 9300, the standby takes over and provides connectivity to the WAN. Refer to the section Turbine Operator Network Design in the design guide for more details.

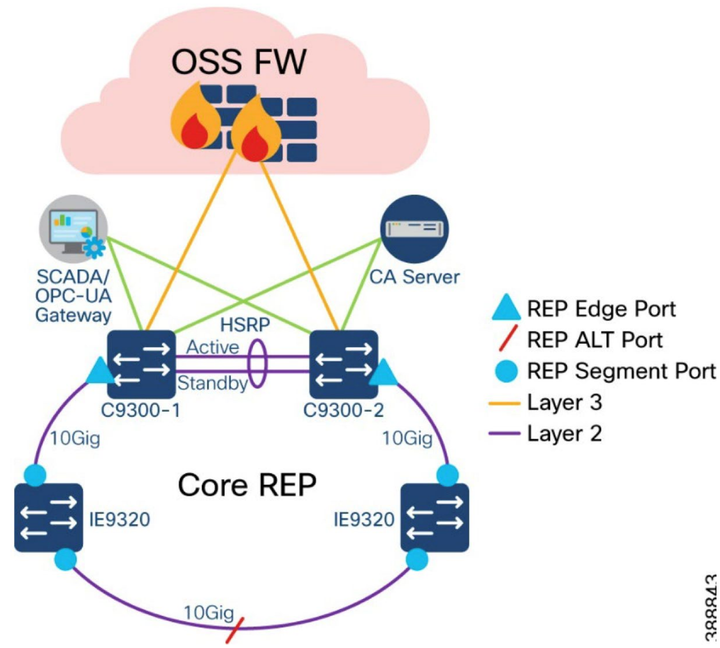
The configuration steps of core switches is shown in the diagram below:

Figure 11-2 Configuration sequence for Core network devices



1. Complete physical cabling of the devices as per the topology below:

Figure 11-3 substation core network topology



2. Complete hostname, NTP and domain configuration on all core switches. Following is an example configuration for the same :

```
hostname <device_hostname>
ntp server <server-ip>
ip domain name <domain_name>
```

3. Configuring SVIs on 9300s

C9300-1:

```
!
vlan 5
!
interface Vlan5
 ip address 10.5.1.2 255.255.0.0

 !

vlan 10
!
interface Vlan10
 ip address 10.10.1.2 255.255.255.0
!
Vlan 20
interface Vlan20
 ip address 10.20.1.2 255.255.0.0
!
Vlan 111
interface Vlan111
```

```
 ip address 10.111.1.2 255.255.255.0
!
```

C9300-2:

```
!
vlan 5
!
interface Vlan5
 ip address 10.5.1.3 255.255.0.0
  !
vlan 10
!

interface Vlan10
 ip address 10.10.1.3 255.255.255.0
!
Vlan 20
interface Vlan20
 ip address 10.20.1.3 255.255.0.0
!
Vlan 111
interface Vlan111
 ip address 10.111.1.3 255.255.255.0
!
```

4. Configuring HSRP

HSRP is to be configured under the SVIs created in the preceding step as shown in the configs below:

C9300-1:

```
interface Vlan5
standby 5 ip 10.5.1.1

!
interface Vlan10
standby 1 ip 10.10.1.1



!
interface Vlan20
standby 20 ip 10.20.1.1
!
interface Vlan111
standby 111 ip 10.111.1.1
!
```

Repeat the same on C9300-2

Verify the HSRP config by issuing the following command on either or both the switches:

```
SCADA-C9300-1 #show standby brief
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri P State    Active          Standby         Virtual IP
Vl5          5    100   Standby 10.5.1.3        local           10.5.1.1
```

```
Vl10         1    105   Active  local          10.10.1.3       10.10.1.1
Vl20         20   100   Standby 10.20.1.3      local           10.20.1.1
Vl111        111  100   Active  local          10.111.1.3      10.111.1.1
```

The HSRP Virtual IP will be used default gateway for the respective vlans

5. Configuring IE9Ks

IE9K-1:

```
Vlan 10,20,11
interface Vlan111
 ip address 10.111.1.4 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.111.1.1
```

IE 9K-2:

```
Vlan 10,20,11
interface Vlan111
 ip address 10.111.1.5 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.111.1.1
```

6. Configuring MACsec

   To configure MACsec refer to the section **Configuring MACSec** in this guide.

7. Bringing up port-channel between the two core C9300 and configuring it as trunk port

   Configure the two links between the C9300 switches as port-channels as shown below:

   C9300-1:

```
interface TenGigabitEthernet1/0/22
 channel-group 1 mode active

     interface TenGigabitEthernet1/0/24
channel-group 1 mode active


  interface Port-channel1
 switchport mode trunk
```

Repeat the same on C9300-2

Verify the port-channel using the command `show etherchannel summary`.

8. Configuring REP ring

   REP ring configuration can be started from either of the C9300 and completing it in a clockwise or anti-clockwise way.

C9300-1:

```
interface TenGigabitEthernet1/1/1
 switchport mode trunk
 rep segment 1 edge
```

IE9k-1:

```
interface TenGigabitEthernet1/0/27
 switchport mode trunk
 rep segment 1
!
interface TenGigabitEthernet1/0/28
 switchport mode trunk
 rep segment 1
```

IE9k-2:

```
interface TenGigabitEthernet1/0/27
 switchport mode trunk
 rep segment 1
!
interface TenGigabitEthernet1/0/28
 switchport mode trunk
 rep segment 1
```

C9300-2:

```
interface TenGigabitEthernet1/1/1
 switchport mode trunk
 rep segment 1 edge
```

This will bring up REP ring which can be verified by issuing show rep topology in any of the four switches

```
show rep topology
REP Segment 1
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
SCADA-C9300-1-Y819               Te1/1/1    Pri  Open
WF-SCADA-IE9320-1                Te1/0/27        Open
WF-SCADA-IE9320-1                Te1/0/28        Open
WF-SCADA-IE9320-2                Te1/0/28        Open
WF-SCADA-IE9320-2                Te1/0/27        Open
WF-SCADA-C9300-2-Y2WQ            Te1/1/1    Sec  Alt
```

Configuring WAN Edge Routing

For configuring WAN Edge routing , OSPF is configured on the Firewall facing interface of C9300s as well as on the Firepower .Following workflow gives the sequence of configuration :

Figure 11-4 WAN Edge routing configuration

1. Configuring routing on C9300s

Following is the config to be applied on both 9300s to enable routing :

```
router ospf 1
network 10.0.0.0 0.0.255.255 area 0
```

2. Configuring routing on the Firepower

For configuring Firepower with routing refer to section “Configure the OSPFv2 Process and Areas “ of the Firepower configuration guide at the following link:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/fdm/fptd-fdm-config-guide-700/fptd-fdm-ospf.html

3. Allowing ports in the Firepower to enable communication

The ports to be allowed for OPC-UA communication are: 4840, 5020

Add these ports by following the steps listed in the section *Configuring Firepower for Wind Farm Solution Use Cases* in this guide and deploy the changes.

This completes WAN edge routing.

Configuring FSN Ring

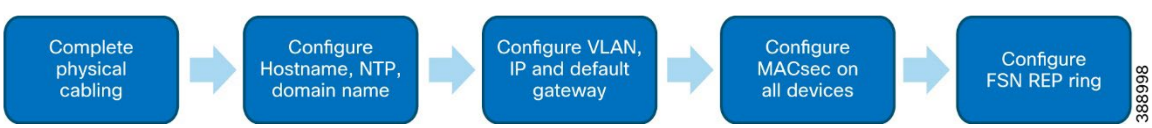
In the turbine operator network, the IE3400 and/or IE3100 Series switches as the base SCADA switch from each wind turbine is connected in a ring topology using a 1G fiber cable with Cisco Industrial Ethernet 9300 switches to form a farm area SCADA network (FSN) ring. A REP is configured in the FSN ring to provide FAN resiliency for faster network convergence if a REP segment fails. For understanding more on FSN design refer to *Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide*:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf?dtid=odicdc000509

section Farm Area SCADA Network (FSN) Design.

Following is the sequence of steps to bring up the FSN ring :

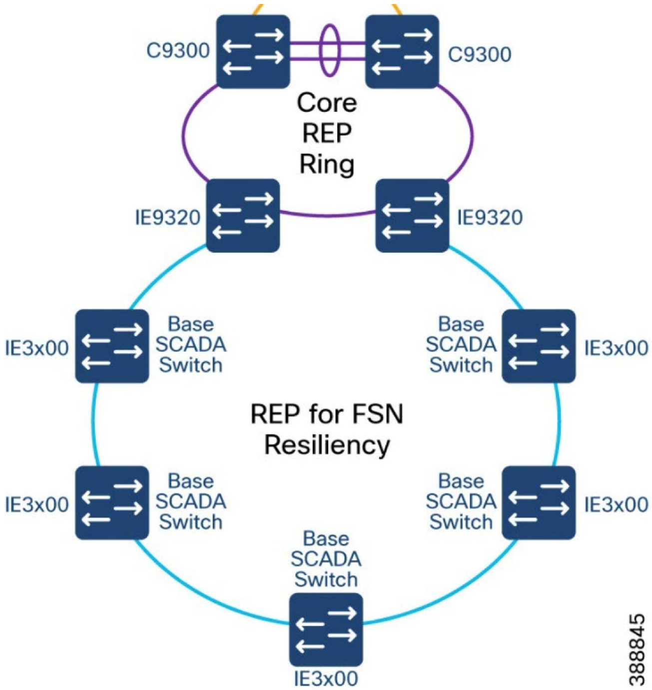
Figure 11-5 Workflow for FSN ring configuration



1. Complete physical cabling

Connect the devices to the IE9K of the core REP ring as shown in Figure 11-6.

Figure 11-6 FSN ring connection



2. Complete hostname,NTP and domain configuration on all switches .Following is an example configuration for the same :

```
hostname <device_hostname>
ntp server <server-ip>
ip domain name <domain_name>
```

3. Configure vlan, IP and default gateway

   Configure the vlans, management vlan interface and gateway on all switches of the FSN ring using the config below:

```
Vlan 10,20,111
Interface vlan 111
Ip address <ip_address>
```

4. Configure MACsec

   To configure MACsec refer to the section *Configuring MACSec* in this guide

5. Configuring REP on FSN ring

FSN ring is configured with open REP segment configuration. The edge port for this REP segment will be configured on the two IE9Ks.We will begin configuring REP from the left IE9K (referred to as IE9K-1 in the config) and proceed with device configuration in an anti clockwise direction.

Following is the configuration on each of the devices of the FSN ring:

IE9K-1:

```
interface TenGigabitEthernet1/0/25
 switchport mode trunk
 rep segment 100 edge
```

Base Scada Switch1:

```
Int range gi 1/1-2
 switchport mode trunk
  rep segment 100
```

IE9K-2:

```
interface TenGigabitEthernet1/0/25
 switchport mode trunk
 rep segment 100 edge
```

This completes the REP configuration on the FSN ring. Verify the REP topology by issuing show rep on any of the switches above:

```
WF-SCADA-FSN-3400-Y1FB#sh rep topo
REP Segment 100
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
WF-SCADA-IE9320-1                Te1/0/25   Pri  Open
WF-SCADA-FSN-3400-Y1FB           Gi1/2           Open
WF-SCADA-FSN-3400-Y1FB           Gi1/1           Open
3400-P48G                        Gi1/1           Open
3400-P48G                        Gi1/2           Open

WF-SCADA-FSN03-V0NS              Gi1/2           Open
WF-SCADA-FSN03-V0NS              Gi1/1           Open
WF-SCADA-FSN04-Y2BT              Gi1/2           Open
WF-SCADA-FSN04-Y2BT              Gi1/1           Open
WF-SCADA-FSN05-V0SZ              Gi1/2           Open
WF-SCADA-FSN05-V0SZ              Gi1/1           Open
WF-SCADA-IE9320-2                Te1/0/25   Sec  Alt
```

Configuring TSN Rings

In offshore wind farms, each wind turbine has a Cisco IE3400 switch deployed at the turbine nacelle for turbine operator network connectivity to various SCADA endpoints in the turbine operator network. For details on it, refer to the section Turbine SCADA Network (TSN) Design of the design guide Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide.

There are two types of TSN rings in the turbine operator network, and both of them is described below.

TSN non-HA

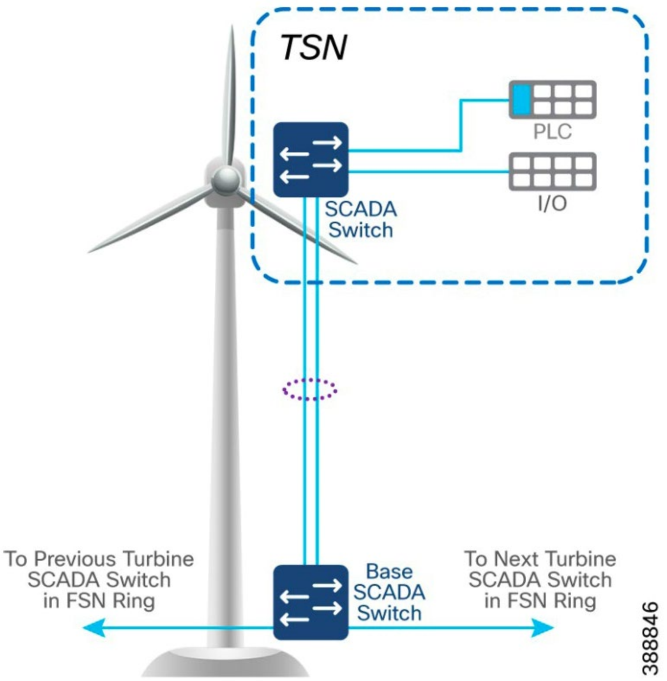
The following diagram shows the sequence to configure TSN non-HA

Figure 11-7 Workflow for TSN non-HA configuration

1 Complete physical cabling.

Physical cabling of switch to a Base Scada Switch is done with two links for redundancy as shown in diagram below.

Figure 11-8 TSN non HA topology connection



2 Complete hostname, NTP, and domain configuration on all switches. Following is an example configuration for the same.

```
hostname <device_hostname>
ntp server <server-ip>
ip domain name <domain_name>
```

3 Configure MACsec.

To configure MACsec refer to the section Configuring MACSec in this guide

4 Configure port-channel.

The two links going to Base Scada Switch are configured as port-channel as shown in config below.

SCADA Switch:

```
interface range GigabitEthernet1/1-2
 channel-group 1 mode active
```

Base SCADA Switch:

```
interface range GigabitEthernet1/3-4
 channel-group 1 mode active
end
```

5 Complete vlan, interface, and layer 2 configs:

Configure the switches as shown below:

SCADA swtich:

```
Vlan 10,20,111
interface vlan 111
ip address <ip_address>
int port-channel 1
switchport mode trunk
```

Base SCADA Switch:

```
int port-channel 1
switchport mode trunk
```

This completes the configuration of TSN non-HA.

Configuring TSN HA:

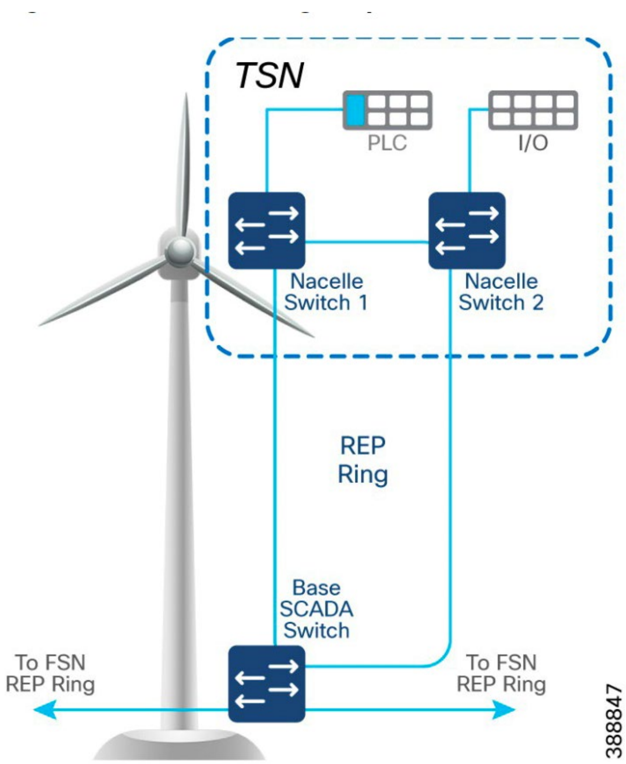
The following diagram describes the sequence for TSN HA configuration:

Figure 11-9 Workflow for configuring TSN HA

1. Completing physical cabling

Physical cabling of switches to a Base Scada Switch forms a closed ring as shown in Figure 11-10 below.

Figure 11-10 TSN HA topology connection



2. Complete hostname, NTP and domain configuration on all switches. Following is an example configuration for the same:

```
hostname <device_hostname>
ntp server <server-ip>
ip domain name <domain_name>
```

3. Configure vlan and interface

```
Vlan 10,20,111
interface vlan 111
ip address <ip_address>
```

4. Configure MACsec

   To configure MACsec refer to the section Configuring MACSec in this guide

5. Configure REP segment.

   A closed REP segment is configured with edge ports on Base Scada switch. Following are configurations for the devices of the TSN HA ring.

   Base SCADA Switch:

```
interface GigabitEthernet1/3
 switchport mode trunk
rep segment 101 edge
```

```
interface GigabitEthernet1/4
 switchport mode trunk
 rep segment 101 edge
```

Nacelle Switch1:

```
interface GigabitEthernet1/4
 switchport mode trunk
 rep segment 101
!
interface GigabitEthernet1/1
 switchport mode trunk
 rep segment 101
```

Nacelle Switch2:

```
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment 101
interface GigabitEthernet1/3
 switchport mode trunk
 rep segment 101
```

Verify the REP topology by issuing `show rep topology` in any of the above switches of TSN HA ring.

```
sh rep topology
REP Segment 101
BridgeName                         PortName   Edge Role
---------------------------------- ---------- ---- ----
3400-P48G                          Gi1/4      Pri  Open
SCADA-TSN-Y0ZJNAcelleSw1           Gi1/4           Open
SCADA-TSN-Y0ZJNAcelleSw1           Gi1/1           Open
WF-SCADA-TSN-Y1SL                  Gi1/2           Open
WF-SCADA-TSN-Y1SL                  Gi1/3           Open
3400-P48G                          Gi1/3      Sec  Alt
```

This completes TSN HA ring configuration.

Configuring Private VLANs

PVLANs provide Layer 2 isolation between ports within the same VLAN . In offshore wind farms, turbine operator SCADA network is micro-segmented using Private VLANs. For details on this refer to the section : Network micro-segmentation using Private VLAN in the Design Guide Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1.

A PVLAN uses VLANs in the following three ways:

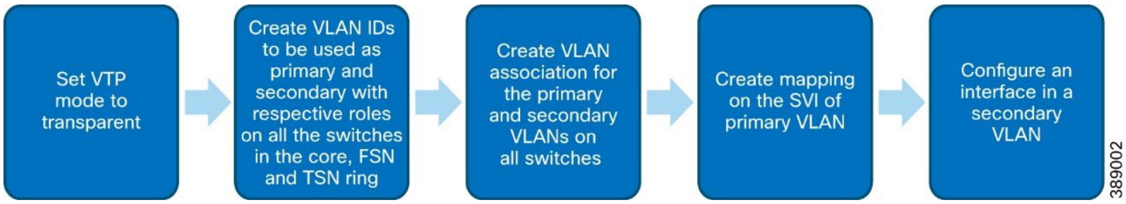
- As a primary VLAN—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.
- As an isolated VLAN—Carries traffic from isolated ports to a promiscuous port.
- As a community VLAN—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN

To learn more about PVLANS refer to the link that follows:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/pvlans.pdf

To configure PVLAN in Turbine Operator SCADA network follow the sequence shown in diagram below:

Figure 11-11 Workflow for configuring Private-vlan



1. Setting VTP mode

Before PVLAN configuration, the VTP mode on the device must be set to **transparent**

```
!
vtp mode transparent
!
```

2. Creating primary and secondary vlans

```
vlan 10
 name PrivateVLANvlan
  private-vlan primary

vlan 101
  private-vlan isolated
```

Repeat the above on all switches in the Core,FSN and TSN ring of the Turbine Operator SCADA network

3. Creating association between primary and secondary vlan

```
vlan 10
  private-vlan association 101
```

4. Creating mapping on the SVI of primary vlan

Following cli must be entered on the two C9300s which are configured with vlan 10 SVIs:

```
interface Vlan10
private-vlan mapping 101
```

5. Configuring an interface in a secondary vlan

To configure an interface in a isolated or community port configure it as private vlan host followed by primary vlan id and isolated or community vlan id. Following is an example:

```
interface GigabitEthernet1/3
switchport private-vlan host-association 10 101
```

Alternatively, the port can also be configured as **promiscuous**.

The private vlan configuration can be verified by issuing "show vlan private-vlan"

```
Show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      101       isolated          Gi1/3
```

Note: The primary as well as the secondary vlans must be allowed on all trunk port in the network.

This completes the PVLAN configuration.

Configuring MACSec

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. MACsec was developed to allow authorized systems to connect and then encrypt data that is transmitted across the wire and to keep a man-in-the-middle from being able to insert frames on to the wire. MACsec does not authorize the systems connecting to the network, it enables those systems to encrypt traffic destined for the network. MACsec, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

For details on MACsec and its use refer to the section *MACsec Encryption in Turbine Operator Network* in the Design Guide.

MACsec can be configured with either key based encryption or certificate based encryption. To learn details about these methods refer to the link below:

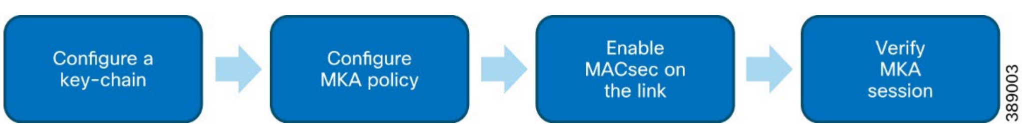
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_3/b_security_17-3_iot_switch_cg/m-macsec-protocol.html

Note: MACSec is not supported on IE3100 Series switches. IE3100 switches should not be mixed with IE3400 to form the rings if MACsec is to enabled in the ring.

Configuring Pre-shared key-based Macsec

In this method a key-chain is configured that is used by MACsec for encryption. Following is the workflow to configure pre-shared key based MACsec:

Figure 11-12 Workflow for configuring pre-shared key based MACsec



The following configurations are to be completed on all switches in the Turbine operator network:

1. Configure a key-chain as shown in example below

```
key chain MAC-SEC macsec
 key 4000000000000000000000000000000000000000000000000000000000000000
  cryptographic-algorithm aes-128-cmac
  key-string 7 106D283F2034332D29270B0D010B1213074324372524067A7975715E2039307C08
  lifetime local 00:00:00 Jan 1 1993 infinite
```

2. Configure an mka policy as shown below:

```
mka policy MKA-POLICY
 key-server priority 150
 sak-rekey interval 65535
```

3. Enable macsec on the link using the keychain and mka policy as shown below:

For C9300 &IE9320 :

```
Macsec network-link
mka policy MKA-POLICY
 mka pre-shared-key key-chain MAC-SEC
```

For 3400:

```
Macsec
mka policy MKA-POLICY
 mka pre-shared-key key-chain MAC-SEC
```

Note: To enable macsec on C9300 and IE9320 use the cli command: `macsec network-link` and for platforms 3400 use the command: `macsec`

4. Verify the macsec session using the command: `show mka session`

Configuring certificate-based MACsec

This section covers the configuration of certificate based MACsec in brief. To learn details about the same refer to the link below:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16-6/macsec-xe-16-6-book/macsec-xe-16-6-book_chapter_010.pdf

For configuring certificate based MACsec , a CA server must be first setup. Certificate can be obtained from the CA, in the following two ways :

1. Manual installation of certificates from a CA
2. Certificate installation via SCEP

We have used a windows server for manual certificate generation and a Cisco router for automatic certificate generation via SCEP .

To know how to install a windows CA server refer to the link below:

https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

To know how to configure a cisco router as a CA server refer to the link below:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/50282-ios-ca-ios.html

Pre-requisites for configuring certificate based MACsec:

i. All devices must be synchronized to the same NTP
ii. A CA server should be in ready state .For details on CA server configuration refer to the link below: https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/211322-IOS-PKI-Deployment-Guide-Certificate-Ro.html

iii. Certificates on each IOS XE device must be issued by the same CA
iv. Certificates can be obtained using SCEP or manual enrollment
   a. Certificates must contain the following X509 Usages
      Digital Signature
   b. Key Encipherment
v. Certificates must contain the following Extended Key Usages
   a. Server Auth
   b. Client Auth
vi. Device must be configured with a hostname, Domain Name, DNS IP Addresses & NTP
vii. the access-session is configured as closed or in multiple-host mode

Manual installation of certificates from a CA

Manual certificate generation involves the following steps shown in Figure 11-13:

Figure 11-13 Workflow for generating certificate on a switch

For detailed steps refer to the link below :
https://community.cisco.com/t5/networking-knowledge-base/creating-a-csr-authenticating-a-ca-and-enrolling-certificates-on/ta-p/4436090

1. Generating a key-pair

   Generate a key pair for use in trustpoint as shown in the example below:

```
crypto key generate rsa modulus 4096 label my-4096rsa-key
    !
```

2. Creating Trustpoint

   Following commands show an example for creation of trustpoint

```
crypto pki trustpoint my-trustpoint
enrollment terminal pem
C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN= WF-SCADA-IE9320-1.wf.com
subject-alt-name WF-SCADA-IE9320-1.wf.com
serial-number none
     ip-address none
     revocation-check none
rsakeypair my-4096rsa-key
```

3. Generating CSR

   A Certificate Signing Request will be created and the same will be displayed on the screen .This CSR needs to be copied to a file and saved it with file_name.cer .Following is the command to generate CSR and display it on the screen:

```
crypto pki enroll my-trustpoint
```

4. Obtaining CA root certificate

   For authenticating the CA , the CA certificate must be installed on the device using the following command:

```
crypto pki authenticate my-trustpoint
```

5. Importing device certificate

In this step the file that was given by the CA on submission of CSR is going to be imported on the device using the command below:

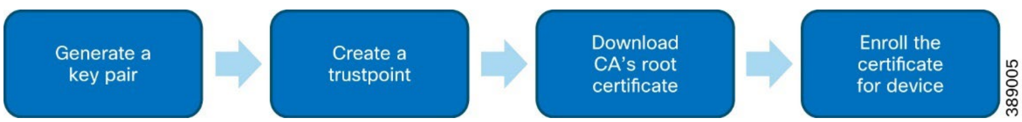
```
crypto pki import my-trustpoint certificate
```

With this, the device is now ready to use the certificate for MACsec configuration

Certificate installation via SCEP

For installing a certificate via SCEP complete the sequence shown in following diagram:

Figure 11-14 Workflow for configuring SCEP



For detailed step refer to the link below:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-cert-enroll-pki.html

1. Generate key-pair
   Generate a key pair as covered in Manual certificate install section.

```
crypto key generate rsa modulus 4096 label my-4096rsa-key
!
```

2. Create a trustpoint with enrolment URL pointing to the reachable CA as shown in example below:

```
crypto pki trustpoint CA
 enrollment url http://10.20.200.1:80
 serial-number
 ip-address none
 subject-name CN=Y819
 revocation-check none
 rsakeypair my-4096rsa-key
 hash sha512
```

3. Downloading the CA root certificate
   Download the CA root certificate by issuing the command shown below:

```
crypto pki authenticate <TRUSTPOINT_NAME>
```

example: `crypto pki authenticate my-trustpoint>`

4. Enrolling the certificate

Issue the below command to enroll the device certificate

```
crypto pki enroll  <TRUSTPOINT_NAME>
```

example : `crypto pki enroll  my-trustpoint`

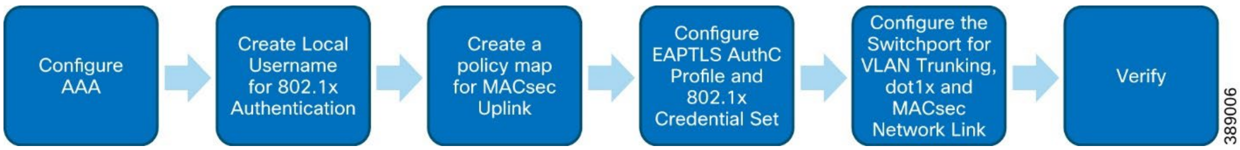
The certificate should be successfully obtained. Verify the same using the following cli:

```
show crypto pki certificates verbose my-trustpoint
```

Certificate based MACsec configuration

After certificates have been installed on the devices, MACsec can be configured as shown in the diagram below:

Figure 11-15 Workflow for configuring certificate based MACSec



1. Configuring AAA

```
Following is the example configuration to configure AAA:
conf t
    aaa new-model
    aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
    aaa authorization credential-download MACSEC-UPLINK local
    aaa authentication dot1x MACSEC-UPLINK local
    aaa authorization network MACSEC-UPLINK local
    !
    end
```

2. Creating Local Username for 802.1x Authentication

This username will be referenced in the dot1x Cred Set section below.

```
aaa attribute list MUST-SECURE
      attribute type linksec-policy must-secure
    !
    username usr-macsec aaa attribute list MUST-SECURE
    !
```

3. Creating a policy map for MACsec Uplink

Configure the policy-map that will be applied to interfaces that connect the switches

```
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
      event session-started match-all
        10 class always do-until-failure
          10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
      event authentication-failure match-all
        10 class always do-until-failure
          10 terminate dot1x
          20 authentication-restart 10
      event authentication-success match-all
        10 class always do-until-failure
          10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
    !
```

4. Configuring EAPTLS AuthC Profile and 802.1x Credential Set

Enable dot1x in this section and create authentication profiles:

```
dot1x system-auth-control
    !
    eap profile EAP-PROFILE
      method tls
      pki-trustpoint my-trustpoint
```

```
        !
        !
        dot1x credentials DOT1X-CREDS
          username usr-macsec
          pki-trustpoint my-trustpoint
        !
```

5. Configuring the Switchport for VLAN Trunking, dot1x & MACsec Network Link

```
    interface g1/1
          switchport mode trunk
          macsec network-link
          authentication periodic
          authentication timer reauthenticate 1800
          access-session host-mode multi-host
          access-session closed
          access-session port-control auto
          dot1x pae both
          dot1x credentials DOT1X-CREDS
          dot1x supplicant eap profile EAP-PROFILE
          dot1x authenticator eap profile EAP-PROFILE
          service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
        !
```

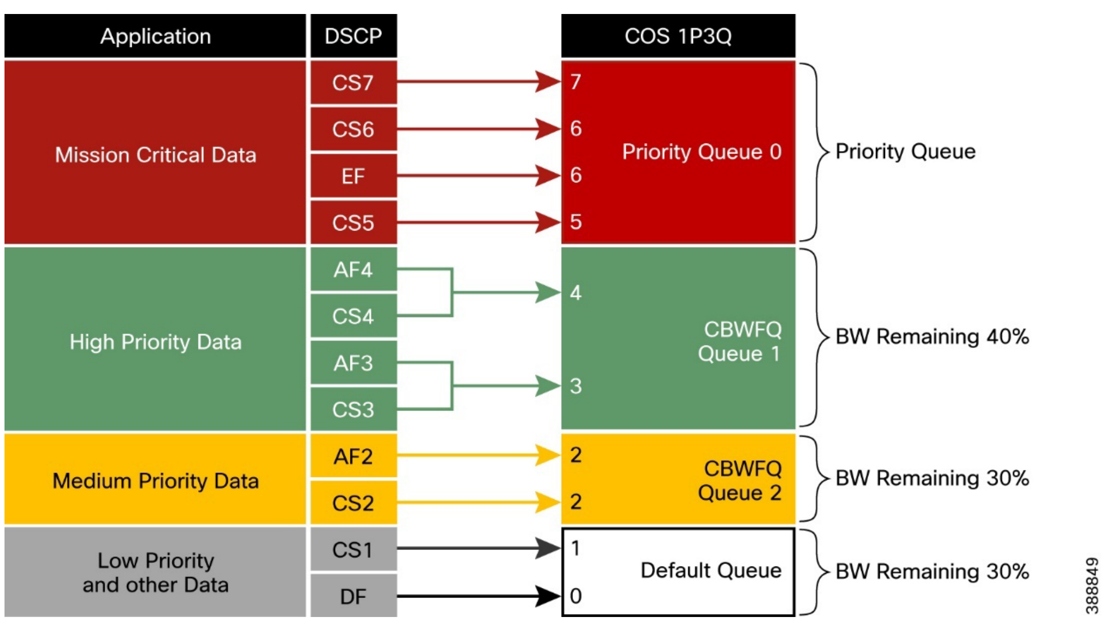
6. Verification

Verify that the macsec session is established by issuing a show mka session

Implementing Quality of Service

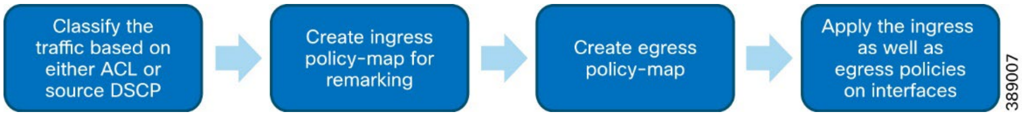
The WindFarm turbine operator network uses the QoS model described in the section TSN Quality-of-Service Design of the Windfarm Design Guide to guarantee network performance and operation by streamlining traffic flow, differentiating network services, and reducing packet loss, jitter, and latency.
The following diagram shows the QoS model implemented on FSN and TSN rings:

Figure 11-16 QoS design for IE switches in TSN and FSN



For configuring QoS in the Turbine Operator Network use the following workflow:

Figure 11-17 QoS configuration sequence



1. Classifying the traffic

Traffic can be classified using the source marked DSCP value or by configuring an access-list to segregate traffic based on source ip and matching against this access-list. Following is configuration required this step.

```
ip access-list standard 1
 10 permit 10.1.10.0 0.0.0.255

class-map match-any MCD
 match dscp cs5  ef  cs6  cs7
class-map match-any LPD
 match dscp default  cs1
class-map match-any MPD
 match dscp cs2  af21  af22  af23
class-map match-any HPD
 match dscp cs3  af31  af32  af33  cs4  af41  af42  af43
 match access-group 1
class-map HPD_Output
match dscp CS4
```

2. Creating ingress policy-map for remarking

   An input policy-map is to be created to use the above created class-maps and setting the dscp value as per the QoS design. Following is an example configuration:

```
policy-map WF_SCADA_Ingress_Policy
class MCD
 set ip dscp EF

 class HPD
  set ip dscp CS4

 class MPD
set ip dscp CS2
class LPD
set ip dscp CS1
```

3. Creating Egress policy-map

An output policy-map is to be created as per the QoS design. Following is an example configuration:

```
policy-map WF_SCADA_Egress_Policy
 class MCD
  priority
 queue-limit 48 packets
 class HPD_Output
  bandwidth remaining percent 40
queue-limit 48 packets
 class MPD
  bandwidth remaining percent 30
queue-limit 48 packets
 class LPD
  bandwidth remaining percent 30
queue-limit 272 packets
```

4. Applying the Ingress and Egress policies on interface

The following is the example configuration to apply the policies on the interfaces

```
int range gi 1/1-10
service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
```

This completes QoS configuration on the devices.

Implementing Multicast in Offshore Substation

This section describes how to enable support for multicast traffic in an turbine operator network. To enable multicast between devices configure the C9300s in the core network as a rendezvous point for multicast . For details on how to configure multicast refer to the link below:
https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x_3800x/software/release/12-2_52_ey/configuration/guide/swmcast.html

Figure 11-18 Workflow for Enabling Multicast

1. Enable multicast on C9300s

Enter the following commands on the 9300s to enable multicast:

```
ip multicast-routing
```

2. Enabling PIM under SVIs of C9300

Enter the following commands under interface vlan on both C9300s:

```
interface Vlan5
ip pim sparse-mode
```

3. Configuring RP

RP Address has to be configured on the C9300s. Following is the example config:

```
ip pim rp-address 10.5.1.1
```

The source can be connected on the core ring and destination in FSN/TSN ring to send/receive the multicast.

This completes the multicast implementation for the Turbine operator network.

Appendix A: Configuration Examples

This appendix includes the following topics:

- WAN PE Configuration
- WAN HER Configuration
- FAN Ring Switch Configuration (Non Edge Switch that is Not a Part of TAN Rings)
- QoS on IE-3400
- QoS on FAN Aggregation and on the OSS and ONSS (C-9300/C-9500)

WAN PE Configuration

```
hostname PE
!
boot-start-marker
boot system bootflash:asr900rsp2-universalk9_npe.17.05.01.SPA.bin
boot-end-marker
!
vrf definition Management_VRF
 rd 100:1
 route-target export 100:1
 route-target import 100:201
 !
 address-family ipv4
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition VRF_PLANTLINK
 rd 199:105
 route-target export 199:105
 route-target import 199:105
 !
 address-family ipv4
 exit-address-family
!
card type e1 0 1
no logging console
enable password ivsg@123
!
no aaa new-model
ethernet evc Czech_3
!
clock timezone IST 5 30
!
no ip domain lookup
ip domain name asr903-Auto-PE.cisco.com
!
login on-success log
!
mpls ldp explicit-null
mpls ldp graceful-restart
mpls ldp session protection
mpls traffic-eng tunnels
multilink bundle-name authenticated
```

```
xconnect logging pseudowire status
!
license udi pid ASR-903U sn FOX1749P8CB
license boot level metroaggrservices
no license smart enable
memory free low-watermark processor 5603
!
spanning-tree extend system-id
sdm prefer default
diagnostic bootup level minimal
!
username admin privilege 15 password 0 ivsg@123
!
redundancy
 mode sso
 main-cpu
  standby console enable
!
bfd-template single-hop ISIS-BFD
 interval min-tx 4 min-rx 4 multiplier 3
!
bfd-template single-hop bfd-tunnel1
 interval min-tx 100 min-rx 100 multiplier 3
!
bfd-template single-hop bfd-tunnel2
 interval min-tx 4 min-rx 4 multiplier 3
!
bfd-template single-hop bfd-tunnel3
 interval min-tx 4 min-rx 4 multiplier 3
!
controller wanphy 0/0/0
!
controller E1 0/1/0
 framing no-crc4
 clock source internal
 linecode ami
 channel-group 1 timeslots 1-31
 no snmp trap link-status
!
controller E1 0/1/1
 no snmp trap link-status
!
controller E1 0/1/2
 no snmp trap link-status
!
controller E1 0/1/3
 no snmp trap link-status
!
controller E1 0/1/4
 no snmp trap link-status
!
controller E1 0/1/5
 no snmp trap link-status
!
controller E1 0/1/6
 no snmp trap link-status
!
controller E1 0/1/7
 no snmp trap link-status
!
controller wanphy 0/2/8
!
controller voice-port 0/3/0
!
controller voice-port 0/3/1
```

```
!
controller voice-port 0/3/2
!
controller voice-port 0/3/3
!
controller voice-port 0/3/4
!
controller voice-port 0/3/5
!
transceiver type all
 monitoring
cdp run
!
lldp run
!
class-map match-any vlan104
 match vlan 104
class-map match-any vlan105
 match vlan 105
class-map match-any vlan106
 match vlan 106
class-map match-any vlan107
 match vlan 107
class-map match-any vlan101
 match vlan 101
class-map match-any vlan102
 match vlan 102
class-map match-any vlan103
 match vlan 103
class-map match-any vlan108
 match vlan 108
!
policy-map Access_ingress
 class vlan101
  police cir 128000 bc 8000
   conform-action transmit
   exceed-action drop
 class vlan102
  police cir 128000 bc 8000
   conform-action transmit
   exceed-action drop
 class vlan103
  police cir 256000 bc 8000
   conform-action transmit
   exceed-action drop
 class vlan104
  police cir 512000 bc 16000
   conform-action transmit
   exceed-action drop
 class vlan105
  police cir 1024000 bc 32000
   conform-action transmit
   exceed-action drop
 class vlan106
  police cir 20000000 bc 625000
   conform-action transmit
   exceed-action drop
 class vlan107
  police cir 100000000 bc 3125000
   conform-action transmit
   exceed-action drop
 class vlan108
  police cir 200000000 bc 6250000
   conform-action transmit
   exceed-action drop
```

```
 class class-default
!
pseudowire-class TE3
 encapsulation mpls
!
pseudowire-class PW64
 encapsulation mpls
!
interface Loopback0
 ip address 192.168.201.10 255.255.255.255
!
interface Loopback1
 ip address 192.168.199.3 255.255.255.255
!
interface Loopback100
 ip address 100.100.100.1 255.255.255.255
!
interface Port-channel1
 ip address 192.168.119.1 255.255.255.0
 no negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
 lacp max-bundle 2
!
interface Multilink1
 ip address 11.11.11.1 255.255.255.0
 ppp multilink
 ppp multilink group 1
!
interface pseudowire1
 encapsulation mpls
 neighbor 3.3.3.3 3
 mtu 1508
 control-word include
!
interface pseudowire2
 encapsulation mpls
 neighbor 17.17.17.17 28
 bandwidth 2144 persistent
!
interface pseudowire3
 encapsulation mpls
 neighbor 2.2.2.2 4
 bandwidth 64 persistent
!
interface TenGigabitEthernet0/0/0
 no ip address
 shutdown
!
interface Serial0/1/0:1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface GigabitEthernet0/2/0
 ip address 192.168.81.2 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
 load-interval 30
 negotiation auto
 cdp enable
 mpls ip
 mpls label protocol ldp
 mpls ldp discovery transport-address 192.168.201.10
 mpls traffic-eng tunnels
```

```
!
interface GigabitEthernet0/2/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/2
 no ip address
 negotiation auto
 cdp enable
 bfd interval 50 min_rx 50 multiplier 3
 channel-group 1
!
interface GigabitEthernet0/2/3
 no ip address
 negotiation auto
 cdp enable
 bfd interval 50 min_rx 50 multiplier 3
 channel-group 1
!
interface GigabitEthernet0/2/4
 description connected to gig0/0/1 Sumatra-PP-1-pravm
 no ip address
 negotiation auto
 service instance 2011 ethernet
  encapsulation dot1q 2011
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2011
 !
interface GigabitEthernet0/2/5
 description connected to sumatra-PP-1-Pravm gig0/0/0
 ip address 192.168.82.1 255.255.255.0
 load-interval 30
 negotiation auto
 cdp enable
 mpls ip
 mpls label protocol ldp
 mpls ldp discovery transport-address interface
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/2/6
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/7
 no ip address
 negotiation auto
 cdp enable
!
interface TenGigabitEthernet0/2/8
 no ip address
 shutdown
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 10.104.56.179 255.255.255.192
 negotiation auto
!
interface BDI2011
 vrf forwarding Management_VRF
 ip address 20.11.0.1 255.255.255.0
!
router eigrp 1
 bfd interface GigabitEthernet0/2/2
 bfd interface GigabitEthernet0/2/3
 bfd interface Port-channel1
```

```
 network 11.11.11.1 0.0.0.0
 network 192.168.119.1 0.0.0.0
 network 192.168.201.10 0.0.0.0
!
router eigrp 100
 bfd all-interfaces
 network 100.100.100.1 0.0.0.0
 network 192.168.82.0
 network 192.168.83.0
!
router ospf 1
 router-id 192.168.201.10
 network 11.11.11.0 0.0.0.255 area 0
 network 192.168.119.0 0.0.0.255 area 0
 network 192.168.201.10 0.0.0.0 area 0
!
router bgp 200
 bgp log-neighbor-changes
 no bgp default route-target filter
 neighbor 192.168.198.1 remote-as 198
 neighbor 192.168.198.1 ebgp-multihop 2
 neighbor 192.168.198.1 update-source Loopback100
 neighbor 192.168.201.6 remote-as 200
 neighbor 192.168.201.6 update-source Loopback0
 !
 address-family ipv4
  bgp redistribute-internal
  network 192.168.199.3 mask 255.255.255.255
  redistribute eigrp 1
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.198.1 soft-reconfiguration inbound
  neighbor 192.168.198.1 send-label
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 next-hop-self
  neighbor 192.168.201.6 send-label
 exit-address-family
 !
 address-family vpnv4
  bgp redistribute-internal
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 send-community extended
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.201.6 activate
  neighbor 192.168.201.6 send-community extended
  neighbor 192.168.201.6 next-hop-self
 exit-address-family
 !
 address-family ipv4 vrf Management_VRF
  redistribute connected
  neighbor 20.11.0.2 remote-as 198
  neighbor 20.11.0.2 activate
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip tftp source-interface GigabitEthernet0
ip ssh source-interface Loopback1
ip ssh version 2
ip route 8.18.2.1 255.255.255.255 8.8.8.8
ip route 8.18.3.1 255.255.255.255 18.18.18.18
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.104.56.129
!
```

```
ip explicit-path name R356_working enable
 index 1 next-address 192.168.6.1
 index 2 next-address 192.168.3.2
!
ip explicit-path name R324176 enable
 index 1 next-address 192.168.7.2
 index 2 next-address 192.168.5.2
 index 3 next-address 192.168.5.1
 index 4 next-address 192.168.2.2
 index 5 next-address 192.168.2.1
 index 6 next-address 192.168.1.1
!
ip explicit-path name R654 enable
 index 1 next-address 192.168.6.1
 index 2 next-address 192.168.4.1
 index 3 next-address 4.4.4.4
!
ip explicit-path name R6174 enable
 index 1 next-address 192.168.7.2
 index 2 next-address 192.168.5.1
 index 3 next-address 4.4.4.4
!
ip explicit-path name R4176 enable
 index 1 next-address 192.168.7.2
 index 2 next-address 192.168.5.2
!
logging alarm informational
logging host 10.64.66.32 vrf Mgmt-intf
!
snmp-server community private RW
snmp-server community public RO
snmp-server host 10.64.66.31 vrf Mgmt-intf version 2c public
!
l2vpn xconnect context 3_6_6_6_6
 member pseudowire1
!
l2vpn xconnect context XCon_28_17.17.17.17
 member pseudowire2
!
l2vpn xconnect context XCon_4_2.2.2.2
 member pseudowire3
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 password ivsg@123
 login
 transport input ssh
line vty 5 149
 login
 transport input ssh
!
network-clock synchronization automatic
network-clock synchronization ssm option 2 GEN1
network-clock synchronization mode QL-enabled
network-clock wait-to-restore 5 global
network-clock log ql-changes
esmc process
ntp server 192.168.119.2
!
End
```

WAN HER Configuration

```
hostname Substation-HER
!
boot-start-marker
boot system bootflash:asr1000-universalk9.17.03.04a.SPA.bin
boot-end-marker
!
vrf definition Management_VRF
 rd 100:1
 route-target export 100:201
 route-target import 100:1
 !
 address-family ipv4
  import ipv4 unicast map GRT-VRF-INTERNET
  export ipv4 unicast map VRF-GLOBAL
 exit-address-family
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition VRF_BUSINESS
 rd 199:104
 route-target export 199:104
 route-target import 199:104
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_GRIDMON
 rd 199:102
 route-target export 199:102
 route-target import 199:102
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_MGMT
 rd 199:101
 route-target export 199:101
 route-target import 199:101
 !
 address-family ipv4
 exit-address-family
!
vrf definition VRF_PLANTLINK
 rd 199:105
 route-target export 199:105
 route-target import 199:105
 !
 address-family ipv4
  import ipv4 unicast map GLOBAL-TO-VRF_PLANTLINK
 exit-address-family
!
vrf definition VRF_SCADA
 rd 199:111
 route-target export 199:111
 route-target import 199:111
 route-target import 101:111
```

```
 !
 address-family ipv4
  route-target export 199:111
  route-target import 199:111
  route-target import 101:111
 exit-address-family
!
vrf definition VRF_TSCADA
 rd 199:103
 route-target export 199:103
 route-target import 199:103
 !
 address-family ipv4
 exit-address-family
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
aaa session-id common
clock timezone IST 5 30
clock calendar-valid
!
ip name-server 64.104.128.236 72.163.128.140
ip domain name isg.cisco.com
!
ip dhcp pool ASR1002-HX-DHCP
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.1
 dns-server 64.104.128.236 72.163.128.140
!
ip dhcp pool ASR1002-HX-MPLS-POOL
 network 192.168.6.0 255.255.255.0
 dns-server 64.104.128.236 72.163.128.140
!
ip dhcp pool SUMATRA-vEDGE-001-MPLS
 network 192.168.7.0 255.255.255.0
 default-router 192.168.7.1
 dns-server 64.104.128.236 72.163.128.140
!
ip dhcp pool CSR1000vEdge-001
 network 192.168.85.0 255.255.255.0
 dns-server 64.104.128.236 72.163.128.140
 default-router 192.168.85.1
!
ip dhcp pool IR1101-cEDGE
 network 192.168.8.0 255.255.255.0
 dns-server 64.104.128.236 72.163.128.140
 default-router 192.168.8.1
!
login on-success log
ipv6 unicast-routing
l2tp-class L2TP_TUNNEL_TEST
 hidden
 authentication
 digest secret 0 cisco@123 hash SHA1
 hello 100
 hostname Substation-HER
 password cisco@123
 receive-window 50
 retransmit retries 10
 timeout setup 400
!
```

```
subscriber templating
!
mpls label protocol ldp
mpls ldp igp sync holddown 1
mpls traffic-eng tunnels
multilink bundle-name authenticated
!
key chain DMVPN
 key 1
  key-string dmvpn
!
crypto pki trustpoint TP-self-signed-1965877644
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1965877644
 revocation-check none
 rsakeypair TP-self-signed-1965877644
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki certificate chain TP-self-signed-1965877644
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31393635 38373736 3434301E 170D3139 30313033 32333337
  31305A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39363538
  37373634 34308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100C714 B6672F20 6FCACB2D B50D37FD ACC82BB6 48FA3370 596AA888
  CE960E65 D29D7C0A 73576B28 B1F4DABA D1D95B46 E8050E39 405D92AF 5AA18ACE
  949BB18F 71750675 1727640A 332D8936 816B8DAC 7D8AA1D8 1CB2A298 694ABF7D
  16041846 50D8CE7F 0DA680C4 FE36C0E7 4E5AE910 36A6861F 2BF1CCA0 D0B0875F
  96AF3DED 6E523CC1 00BCA192 E76C8A22 5D65FAED 821586A3 337D7A2C 4B85179B
  957CF4BE 2F3A3F24 914FAAF3 C9BC548D 7ACA7978 F22A1D04 5C3E463A E7E05DE2
  84D74AAF 0E67216A 34259D3C DD49ABED 8C8A5DD1 EDF8A994 16C056E2 88FE2C39
  2F193213 C2C710D1 ADB65FF7 A10269F0 95FC10EF C188AD79 5F81A51E CD1F431E
  0420B145 9C750203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14F597FF AFE97D33 10450784 DE51AE65 AFC9E0D3
  98301D06 03551D0E 04160414 F597FFAF E97D3310 450784DE 51AE65AF C9E0D398
  300D0609 2A864886 F70D0101 05050003 82010100 02020A8F AFC4E554 4A3CB2C8
  BACABCAE 7E35E8EF DD6674B7 064D1B78 15C134BA 03F64CBE 92052784 D07BF4C7
  2C58E4DE 52AD9CE1 24803B1F 2FDF695A 9FD5C1D1 6A7B8D0F 5B5B4309 123DE3EF
  CC864675 1DDCD32A 648D5F12 1DA10E63 3CD7F9C8 E1A400E6 A66AE5E0 FE015FAC
  4856AAB1 257EFEB7 E72D9E35 25BB7C0A 85210008 10A44487 121FB976 A1925CF9
  254F2A85 D13BE095 91BBDBFD DB7C597F B26E2F81 2145E044 A12FF215 5EA46005
  0D9F948F 5D934357 A03FCB29 0B6722CF E1B3FA28 69D5B0B5 7CE738B2 9C422EF9
  42ECB5F1 F6A0646E 4689A9F0 09C8BA9C E5925BB9 C025C73E E5BEE057 DC089907
  FE81C2D2 1CB8AC61 87BA438D 94E3E8C4 DEC9E9BA
        quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
```

```
    C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
    DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
    06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
    4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
    03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
    604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
    D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
    467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
    7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
    5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
    80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
    418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
    D697DF7F 28
          quit
!
license udi pid ASR1002-HX sn JAE225206PR
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
license boot level adventerprise
license solution level appxk9
license solution level securityk9
memory free low-watermark processor 991004
!
spanning-tree extend system-id
diagnostic bootup level minimal
!
username cisco privilege 15 password 0 Cisco@123
username admin privilege 15 password 0 sentryo69!
!
redundancy
 mode none
!
bridge-domain 1
 member vni 6001
 member GigabitEthernet0/2/15 service-instance 1
!
bridge-domain 601
 no mac learning
!
bridge-domain 1000
crypto ikev2 authorization policy default_No_cert
 route set interface
 route set access-list FLEX_ACL
!
no crypto ikev2 authorization policy default
!
crypto ikev2 redirect gateway init
! (IKEv2 Cluster load-balancer is not enabled)
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_No_cert
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_No_cert
 proposal FlexVPN_IKEv2_Proposal_No_cert
!
crypto ikev2 keyring ANY
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key sentryo
 !
crypto ikev2 profile FLEX_SERVER_PROF_No_cert_1
 match identity remote address 0.0.0.0
 match identity remote fqdn domain isg.cisco.com
```

```
 identity local address 89.89.89.1
 authentication remote pre-share
 authentication local pre-share
 keyring local ANY
 aaa authorization group psk list FlexVPN_Author default_No_cert
 virtual-template 4
!
crypto ikev2 fragmentation
!
cdp run
!
lldp run
pseudowire-class L2TP_PW_TEST
 encapsulation l2tpv3
 sequencing both
 protocol l2tpv3 L2TP_TUNNEL_TEST
 ip local interface Loopback1
 ip pmtu
 ip dfbit set
 ip tos reflect
 ip ttl 100
!
class-map match-any TRANSACTIONAL
 match ip dscp cs2  af21  af22  af23  cs4  af41  af42
class-map match-all VOICE
 match ip dscp ef
class-map match-any MISSION-CRITICAL-DATA
 match access-group name MISSION-CRITICAL-DATA
class-map match-any MISSION-CRITICAL
 match ip dscp cs3  af31  af32  af33  cs6
class-map match-all CALL-SIGNALING
 match ip dscp cs3
!
policy-map HOST-INPUT-MARKING
 class VOICE
  set dscp ef
 class CALL-SIGNALING
  set dscp cs3
 class MISSION-CRITICAL-DATA
  set dscp af31
 class class-default
policy-map HOST-QUEUE-PACKETS
 class VOICE
  priority
 class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
 class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
 class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
policy-map UPLINK-QUEUE-PACKETS
 class VOICE
  priority
 class MISSION-CRITICAL
  bandwidth remaining percent 30
  queue-limit 96 packets
 class TRANSACTIONAL
  bandwidth remaining percent 20
  queue-limit 96 packets
 class class-default
  bandwidth remaining percent 25
  queue-limit 272 packets
```

```
!
crypto isakmp invalid-spi-recovery
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set_No_cert esp-aes esp-sha256-hmac
 mode transport
crypto ipsec fragmentation after-encryption
crypto ipsec df-bit clear
!
crypto ipsec profile default_No_cert_1
 set transform-set FlexVPN_IPsec_Transform_Set_No_cert
 set pfs group14
 set ikev2-profile FLEX_SERVER_PROF_No_cert_1
!
interface Loopback0
 ip address 192.168.201.6 255.255.255.255
!
interface Loopback1
 ip address 192.168.200.1 255.255.255.255
!
interface Loopback2
 description Segment Routing Loop
 ip address 3.3.3.3 255.255.255.255
!
interface Loopback12
 ip address 12.12.12.1 255.255.255.255
 ip ospf network point-to-point
 ip ospf 12 area 0
!
interface Loopback99
 ip address 192.168.13.1 255.255.255.255
!
interface Loopback100
 ip address 10.60.60.1 255.255.255.255
 bfd interval 50 min_rx 50 multiplier 3
!
interface Loopback101
 ip address 10.70.70.1 255.255.255.255
!
interface Loopback111
 ip address 192.168.220.4 255.255.255.255
!
interface Loopback200
 ip address 192.168.117.1 255.255.255.255
!
interface Tunnel100
 no ip address
!
interface GigabitEthernet0/0/0
 description connected to DMZ switch in RR06 on port G1/0/3
 ip address 173.39.13.85 255.255.255.192
 ip nat outside
 negotiation auto
!
interface GigabitEthernet0/0/1
 description connected to asr920-001
 ip dhcp relay information trusted
 ip dhcp relay information option-insert
 ip dhcp relay information check-reply
 ip address 192.168.69.1 255.255.255.0
 ip nat inside
 ip ospf network point-to-point
 ip ospf 1 area 0
```

```
 load-interval 30
 negotiation auto
 cdp enable
 mpls ip
 mpls ldp discovery transport-address 192.168.201.6
 mpls traffic-eng tunnels
 bfd interval 200 min_rx 200 multiplier 3
 service-policy output UPLINK-QUEUE-PACKETS
!
interface GigabitEthernet0/0/2
 description connected to ixia card 2 por 1
 mtu 9216
 no ip address
 load-interval 30
 negotiation auto
!
interface GigabitEthernet0/0/2.1201
 encapsulation dot1Q 1201
 vrf forwarding VRF_SCADA
 ip address 12.0.1.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1202
 encapsulation dot1Q 1202
 vrf forwarding VRF_TSCADA
 ip address 12.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1203
 encapsulation dot1Q 1203
 vrf forwarding VRF_PLANTLINK
 ip address 12.0.3.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1204
 encapsulation dot1Q 1204
 vrf forwarding VRF_MGMT
 ip address 12.0.4.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1205
 encapsulation dot1Q 1205
 vrf forwarding VRF_GRIDMON
 ip address 12.0.5.1 255.255.255.0
!
interface GigabitEthernet0/0/2.1206
 encapsulation dot1Q 1206
 vrf forwarding VRF_BUSINESS
 ip address 12.0.6.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3001
 encapsulation dot1Q 3001
 ip address 30.1.0.1 255.255.255.0
!
interface GigabitEthernet0/0/2.3002
 encapsulation dot1Q 3002
 ip address 30.2.0.1 255.255.255.0
!
interface GigabitEthernet0/0/3
 description connected to ixia card 2 port 2
 mtu 9216
 no ip address
 load-interval 30
 negotiation auto
 service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  bridge-domain 601
 !
```

```
 service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1000
 !
interface GigabitEthernet0/0/3.140
 encapsulation dot1Q 140
 ip address 140.140.140.1 255.255.255.0
!
interface GigabitEthernet0/0/3.799
 encapsulation dot1Q 799
 xconnect 192.168.199.1 799 encapsulation mpls
!
interface GigabitEthernet0/0/3.2001
 description For Windfarm Testbed
 encapsulation dot1Q 2001
 vrf forwarding Management_VRF
 ip address 201.201.201.1 255.255.255.0
!
interface GigabitEthernet0/0/4
 ip address 99.99.99.100 255.255.255.0
 negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/0/5
 description connected to 10.104.56.148 PC ethernet - asr G5
 ip address 192.168.228.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/6
 description Phy_Loop
 no ip address
 negotiation auto
 service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp  dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
   bridge-domain 601 split-horizon group 0
 !
 service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 998 ethernet
  encapsulation dot1q 998
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1001 ethernet
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1002 ethernet
  encapsulation dot1q 1002
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
```

```
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1052 ethernet
  encapsulation dot1q 1052
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1053 ethernet
  encapsulation dot1q 1053
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1054 ethernet
  encapsulation dot1q 1054
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1055 ethernet
  encapsulation dot1q 1055
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1056 ethernet
  encapsulation dot1q 1056
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1056
 !
 service instance 1057 ethernet
  encapsulation dot1q 1057
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 1058 ethernet
  encapsulation dot1q 1058
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
  bridge-domain 1000
 !
 service instance 2502 ethernet
  encapsulation dot1q 2502
  rewrite ingress tag pop 1 symmetric
   l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
   bridge-domain 601 split-horizon group 1
!
interface GigabitEthernet0/0/7
 description Phy_Loop
 no ip address
 load-interval 30
 negotiation auto
!
```

```
interface GigabitEthernet0/0/7.989
 encapsulation dot1Q 989
 xconnect 192.168.205.2 989 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.990
 encapsulation dot1Q 990
 xconnect 192.168.220.3 990 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.991
 encapsulation dot1Q 991
 xconnect 192.168.205.2 991 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.992
 encapsulation dot1Q 992
 xconnect 192.168.205.2 992 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.993
 encapsulation dot1Q 993
 xconnect 192.168.223.1 993 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.994
 encapsulation dot1Q 994
 xconnect 192.168.223.1 994 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.995
 encapsulation dot1Q 995
 xconnect 192.168.223.1 995 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.996
 encapsulation dot1Q 996
 xconnect 192.168.223.1 996 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.997
 encapsulation dot1Q 997
 xconnect 192.168.223.1 997 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.998
 encapsulation dot1Q 998
 xconnect 192.168.202.2 998 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.1001
 encapsulation dot1Q 1001
 xconnect 192.168.199.2 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2502
 encapsulation dot1Q 2502
 xconnect 192.168.199.2 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2503
 encapsulation dot1Q 2503
 xconnect 192.168.199.2 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2504
 encapsulation dot1Q 2504
 xconnect 192.168.199.2 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2505
 encapsulation dot1Q 2505
 xconnect 192.168.199.2 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2506
 encapsulation dot1Q 2506
 xconnect 192.168.199.2 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2507
```

```
 encapsulation dot1Q 2507
 xconnect 192.168.199.2 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2508
 encapsulation dot1Q 2508
 xconnect 192.168.199.2 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2509
 encapsulation dot1Q 2509
 xconnect 192.168.199.2 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2560
 encapsulation dot1Q 2560
 xconnect 192.168.199.2 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface TenGigabitEthernet0/1/0
 description connected to FPR4010 port 8
 ip address 192.168.70.2 255.255.255.0
 service-policy input HOST-INPUT-MARKING
!
interface TenGigabitEthernet0/1/0.106
 encapsulation dot1Q 106
 vrf forwarding Management_VRF
 ip address 106.106.0.2 255.255.255.0
 ip nat inside
 ip ospf network point-to-point
!
interface TenGigabitEthernet0/1/1
 no ip address
!
interface TenGigabitEthernet0/1/2
 ip address 192.168.84.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface TenGigabitEthernet0/1/2.2
 description connected to NCS-002-TenGigE0/0/0/6.2
 encapsulation dot1Q 2
 ip address 192.168.75.2 255.255.255.0
!
interface TenGigabitEthernet0/1/3
 no ip address
 shutdown
!
interface TenGigabitEthernet0/1/4
 no ip address
!
interface TenGigabitEthernet0/1/5
 no ip address
!
interface TenGigabitEthernet0/1/6
 no ip address
!
interface TenGigabitEthernet0/1/7
 no ip address
!
interface GigabitEthernet0/2/0
 description connected to ixia 10.64.66.36 card 1 port 14
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/0.143
 encapsulation dot1Q 143
 ip address 143.143.143.1 255.255.255.0
!
```

```
interface GigabitEthernet0/2/1
 description connected to Laptop SCADA FEP
 ip address 192.168.189.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/2/2
 description connected to ixia card 1 port 10
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/2.501
 encapsulation dot1Q 501
 ip address 171.171.171.1 255.255.255.0
!
interface GigabitEthernet0/2/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/4
 ip address 10.64.66.77 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/2/5
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/6
 description connected to sumatra-pp-2 on G0/0/0
 ip address 89.89.89.1 255.255.255.0
 negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/2/7
 no ip address
 speed 1000
 no negotiation auto
!
interface GigabitEthernet0/2/7.152
 encapsulation dot1Q 152
 ip address 152.152.152.1 255.255.255.0
!
interface GigabitEthernet0/2/8
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/9
 description connected to SA-1002HX-002 gi0/0/0
 ip address 192.168.60.1 255.255.255.0
 ip nat inside
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
interface GigabitEthernet0/2/10
 description connected to UCS 10.104.56.170 on VMNIC 8
 ip address 192.168.85.1 255.255.255.0
 ip nat inside
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/2/11
 no ip address
 shutdown
 negotiation auto
```

```
!
interface GigabitEthernet0/2/12
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/13
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/14
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/15
 description connected to IXIA card 2 port 13
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
 !
interface GigabitEthernet0/2/16
 description connected to IR1101
 ip address 69.69.69.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 12 area 0
 negotiation auto
!
interface GigabitEthernet0/2/17
 description connected to IR1101-cEDGE-002
 ip address 192.168.8.1 255.255.255.0
 ip nat inside
 negotiation auto
 cdp enable
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface Virtual-Template4 type tunnel
 bandwidth 1000000
 ip unnumbered Loopback100
 tunnel source GigabitEthernet0/2/6
 tunnel bandwidth transmit 1000000
 tunnel bandwidth receive 1000000
 tunnel protection ipsec profile default_No_cert_1
!
interface nve1
 no ip address
 source-interface Loopback12
 member vni 6001
  ingress-replication 12.12.12.2
 !
segment-routing mpls
 !
 set-attributes
  address-family ipv4
   sr-label-preferred
  exit-address-family
 !
 global-block 16000 24000
```

```
 !
 connected-prefix-sid-map
  address-family ipv4
   3.3.3.3/32 index 1 range 1
  exit-address-family
 !
router eigrp 99
 bfd interface GigabitEthernet0/0/4
 bfd interface GigabitEthernet0/2/6
 network 10.0.0.0
 network 89.89.89.0 0.0.0.255
 network 99.99.99.0 0.0.0.255
 network 140.140.140.0 0.0.0.255
 network 143.143.143.0 0.0.0.255
 network 152.152.0.0
 network 192.168.2.0
 network 192.168.4.0
 network 192.168.13.0
 network 192.168.89.0
 network 192.168.200.0
 network 192.168.201.0
 network 192.168.228.0
 redistribute bgp 200 metric 100 1 255 1 1500
 eigrp router-id 10.60.60.1
!
router ospf 1
 router-id 192.168.201.6
 segment-routing mpls
 network 3.3.3.3 0.0.0.0 area 0
 network 192.168.201.6 0.0.0.0 area 0
 bfd all-interfaces
 mpls ldp sync
!
router ospf 4 vrf Management_VRF
 redistribute static
 network 106.106.0.0 0.0.0.255 area 0
 default-information originate always metric 15
 default-metric 15
!
router ospf 12
 router-id 12.12.12.1
 network 12.12.12.1 0.0.0.0 area 0
 bfd all-interfaces
!
router bgp 200
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 192.168.60.2 remote-as 2001
 neighbor 192.168.60.2 shutdown
 neighbor 192.168.60.2 ebgp-multihop 255
 neighbor 192.168.70.1 remote-as 1001
 neighbor 192.168.70.1 update-source Loopback0
 neighbor 192.168.111.1 remote-as 200
 neighbor 192.168.111.1 ebgp-multihop 255
 neighbor 192.168.111.1 update-source Loopback0
 neighbor 192.168.113.1 remote-as 200
 neighbor 192.168.113.1 ebgp-multihop 255
 neighbor 192.168.113.1 update-source Loopback0
 neighbor 192.168.198.1 remote-as 200
 neighbor 192.168.198.1 shutdown
 neighbor 192.168.198.1 update-source Loopback0
 neighbor 192.168.198.1 fall-over
 neighbor 192.168.198.1 fall-over bfd
 neighbor 192.168.199.1 remote-as 200
 neighbor 192.168.199.1 shutdown
```

```
neighbor 192.168.199.1 update-source Loopback0
neighbor 192.168.199.1 fall-over
neighbor 192.168.199.1 fall-over bfd multi-hop
neighbor 192.168.201.4 remote-as 200
neighbor 192.168.201.4 update-source Loopback0
neighbor 192.168.201.10 remote-as 200
neighbor 192.168.201.10 update-source Loopback0
neighbor 192.168.202.1 remote-as 101
neighbor 192.168.202.1 ebgp-multihop 255
neighbor 192.168.202.1 update-source Loopback0
neighbor 192.168.203.1 remote-as 200
neighbor 192.168.203.1 update-source Loopback0
neighbor 192.168.220.2 remote-as 102
neighbor 192.168.220.2 ebgp-multihop 255
neighbor 192.168.220.2 update-source Loopback0
!
address-family ipv4
 bgp additional-paths install
 bgp nexthop trigger delay 1
 network 18.18.18.0 mask 255.255.255.0
 network 30.1.0.0 mask 255.255.255.0
 network 30.2.0.0 mask 255.255.255.0
 network 140.140.140.0 mask 255.255.255.0
 network 141.141.141.0 mask 255.255.255.0
 network 192.168.189.0
 network 192.168.200.1 mask 255.255.255.255
 network 192.168.201.7 mask 255.255.255.255
 network 192.168.201.8 mask 255.255.255.255
 network 192.168.205.2 mask 255.255.255.255
 network 192.168.205.4 mask 255.255.255.255
 network 192.168.220.2 mask 255.255.255.255
 network 192.168.223.1 mask 255.255.255.255
 redistribute connected
 redistribute eigrp 99
 neighbor 192.168.60.2 activate
 neighbor 192.168.60.2 next-hop-self
 neighbor 192.168.60.2 send-label
 neighbor 192.168.70.1 activate
 neighbor 192.168.70.1 next-hop-self
 neighbor 192.168.70.1 send-label
 neighbor 192.168.111.1 activate
 neighbor 192.168.111.1 send-community extended
 neighbor 192.168.111.1 next-hop-self
 neighbor 192.168.113.1 activate
 neighbor 192.168.113.1 send-community extended
 neighbor 192.168.113.1 next-hop-self
 neighbor 192.168.198.1 activate
 neighbor 192.168.198.1 next-hop-self
 neighbor 192.168.198.1 soft-reconfiguration inbound
 neighbor 192.168.198.1 send-label
 neighbor 192.168.199.1 activate
 neighbor 192.168.199.1 weight 40000
 neighbor 192.168.199.1 next-hop-self
 neighbor 192.168.199.1 soft-reconfiguration inbound
 neighbor 192.168.199.1 send-label
 neighbor 192.168.201.4 activate
 neighbor 192.168.201.4 weight 40000
 neighbor 192.168.201.4 next-hop-self
 neighbor 192.168.201.4 soft-reconfiguration inbound
 neighbor 192.168.201.4 send-label
 neighbor 192.168.201.10 activate
 neighbor 192.168.201.10 next-hop-self
 neighbor 192.168.201.10 soft-reconfiguration inbound
 neighbor 192.168.201.10 send-label
 neighbor 192.168.202.1 activate
```

```
  neighbor 192.168.202.1 next-hop-self
  neighbor 192.168.202.1 soft-reconfiguration inbound
  neighbor 192.168.202.1 send-label
  neighbor 192.168.203.1 activate
  neighbor 192.168.203.1 next-hop-self
  neighbor 192.168.203.1 soft-reconfiguration inbound
  neighbor 192.168.203.1 send-label
  neighbor 192.168.220.2 activate
  neighbor 192.168.220.2 next-hop-self
  neighbor 192.168.220.2 send-label
  distribute-list 1 out
 exit-address-family
 !
 address-family vpnv4
  neighbor 192.168.70.1 activate
  neighbor 192.168.70.1 send-community extended
  neighbor 192.168.70.1 next-hop-self
  neighbor 192.168.198.1 activate
  neighbor 192.168.198.1 send-community extended
  neighbor 192.168.198.1 next-hop-self
  neighbor 192.168.199.1 activate
  neighbor 192.168.199.1 send-community extended
  neighbor 192.168.199.1 next-hop-self
  neighbor 192.168.201.4 activate
  neighbor 192.168.201.4 send-community extended
  neighbor 192.168.201.4 next-hop-self
  neighbor 192.168.201.10 activate
  neighbor 192.168.201.10 send-community extended
  neighbor 192.168.201.10 next-hop-self
 exit-address-family
 !
 address-family l2vpn evpn
 exit-address-family
 !
 address-family ipv4 vrf Management_VRF
  redistribute ospf 4 match internal external 1 external 2
 exit-address-family
 !
 address-family ipv4 vrf VRF_BUSINESS
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_GRIDMON
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_MGMT
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_PLANTLINK
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_SCADA
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf VRF_TSCADA
  redistribute connected
 exit-address-family
!
ip tcp path-mtu-discovery
ip telnet source-interface GigabitEthernet0/0/0
ip http server
```

```
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip ftp source-interface Loopback1
ip ftp username splunk
ip ftp password Sdu@12345
ip tftp source-interface Loopback0
ip dns server
ip pim rp-address 12.12.12.1
ip nat inside source list NAT_INSIDE_POOL interface GigabitEthernet0/0/0 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
ip route 10.64.66.0 255.255.255.0 10.64.66.1
ip route 18.18.18.0 255.255.255.0 192.168.84.2
ip route 52.59.49.252 255.255.255.255 GigabitEthernet0/0/0
ip route 106.106.0.0 255.255.255.0 10.64.66.67
ip route 192.168.21.0 255.255.255.0 192.168.70.1
ip route 192.168.201.7 255.255.255.255 192.168.75.1
ip route 192.168.201.8 255.255.255.255 192.168.75.1
ip route 192.168.220.2 255.255.255.255 99.99.99.2 255
ip route vrf Management_VRF 0.0.0.0 0.0.0.0 10.64.66.1
ip ssh source-interface GigabitEthernet0/0/0
ip ssh version 2
!
ip access-list standard FLEX_ACL
 211 permit 10.1.1.10
 210 permit 10.2.2.20
 13 permit 89.89.89.0
 14 permit 99.99.99.0
 15 permit 192.168.169.1
 10 permit 10.60.60.0 0.0.0.255
 11 permit 192.168.220.0 0.0.0.255
 16 permit 140.140.140.0 0.0.0.255
 20 permit 192.168.2.0 0.0.0.255
 30 permit 192.168.4.0 0.0.0.255
 40 permit 192.168.5.0 0.0.0.255
 50 permit 192.168.199.0 0.0.0.255
 60 permit 192.168.200.0 0.0.0.255
 80 permit 192.168.202.0 0.0.0.255
 90 permit 192.168.203.0 0.0.0.255
 100 permit 192.168.204.0 0.0.0.255
 110 permit 192.168.210.0 0.0.0.255
ip access-list standard internet
 10 permit 192.168.6.0 0.0.0.255
!
ip access-list extended MISSION-CRITICAL-DATA
 10 permit tcp any eq 20000 any
 20 permit tcp any eq 20100 any
 30 permit tcp any eq 20101 any
 40 permit tcp any eq 20102 any
 50 permit udp any eq 1234 any
 60 permit udp any eq 1235 any
ip access-list extended NAT_INSIDE_POOL
 10 permit ip 192.168.60.0 0.0.0.255 any
 11 permit ip 192.168.85.0 0.0.0.255 any
 12 permit tcp 192.168.85.0 0.0.0.255 any
 13 permit udp 192.168.85.0 0.0.0.255 any
 14 permit icmp 192.168.85.0 0.0.0.255 any
 15 permit esp 192.168.85.0 0.0.0.255 any
 16 permit ahp 192.168.85.0 0.0.0.255 any
 20 permit tcp 192.168.60.0 0.0.0.255 any
 30 permit udp 192.168.60.0 0.0.0.255 any
 40 permit icmp 192.168.60.0 0.0.0.255 any
 50 permit esp 192.168.60.0 0.0.0.255 any
 60 permit ahp 192.168.60.0 0.0.0.255 any
```

```
 71 permit ip 192.168.66.0 0.0.0.255 any
 72 permit tcp 192.168.66.0 0.0.0.255 any
 73 permit udp 192.168.66.0 0.0.0.255 any
 74 permit icmp 192.168.66.0 0.0.0.255 any
 75 permit esp 192.168.66.0 0.0.0.255 any
 76 permit ahp 192.168.66.0 0.0.0.255 any
 77 permit ip any any
 78 permit gre any any
 81 permit ip 192.168.6.0 0.0.0.255 any
 82 permit tcp 192.168.6.0 0.0.0.255 any
 83 permit udp 192.168.6.0 0.0.0.255 any
 84 permit icmp 192.168.6.0 0.0.0.255 any
 85 permit esp 192.168.6.0 0.0.0.255 any
 86 permit ahp 192.168.6.0 0.0.0.255 any
 91 permit ip 192.168.7.0 0.0.0.255 any
 92 permit tcp 192.168.7.0 0.0.0.255 any
 93 permit udp 192.168.7.0 0.0.0.255 any
 94 permit icmp 192.168.7.0 0.0.0.255 any
 95 permit esp 192.168.7.0 0.0.0.255 any
 96 permit ahp 192.168.7.0 0.0.0.255 any
 101 permit ip 192.168.8.0 0.0.0.255 any
 102 permit tcp 192.168.8.0 0.0.0.255 any
 103 permit udp 192.168.8.0 0.0.0.255 any
 104 permit  icmp 192.168.8.0 0.0.0.255 any
 105 permit esp 192.168.8.0 0.0.0.255 any
 106 permit ahp 192.168.8.0 0.0.0.255 any
 107 permit ip 106.106.0.0 0.0.0.255 any
 108 permit tcp 106.106.0.0 0.0.0.255 any
 109 permit udp 106.106.0.0 0.0.0.255 any
 110 permit  icmp 106.106.0.0 0.0.0.255 any
 111 permit esp 106.106.0.0 0.0.0.255 any
 112 permit ahp 106.106.0.0 0.0.0.255 any
!
ip prefix-list GRT-VRF seq 5 permit 10.64.66.0/24
!
ip prefix-list VRF_GLO seq 2 permit 106.106.0.0/24
!
ip prefix-list iBGP_GLOBAL seq 5 permit 192.168.2.0/24
!
ip prefix-list lab-net seq 1 permit 10.64.66.0/24
!
route-map GLOBAL_TO_MAGAGEMENT_VRF permit 10
 match ip address prefix-list GLOBAL_TO_VRF_Management
!
route-map GRT-VRF-INTERNET permit 10
 match ip address prefix-list GRT-VRF
!
route-map GLOBAL-TO-VRF_PLANTLINK permit 10
 match ip address prefix-list iBGP_GLOBAL
!
route-map VRF-GLOBAL permit 10
 match ip address prefix-list VRF_GLO
!
snmp-server community public RO
snmp-server trap link ietf
snmp-server trap link switchover
snmp-server location SA-HER
snmp-server contact SCADA
snmp-server host 192.168.5.11 version 2c public
snmp ifmib ifindex persist
!
tftp-server bootflash:ASR1002-HX-JAE225206QL.cfg
tftp-server bootflash:ciscosdwan.cfg
tftp-server bootflash:asr1000-universalk9.17.03.04a.SPA.bin
!
```

```
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport input all
 transport output all
!
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
ntp master
ntp server 45.86.70.11
ntp server 10.104.56.158
!
end

9500
hostname WF-OSS-C9500
!
vrf definition Management_VRF
 rd 100:1
 !
 address-family ipv4
  route-target export 100:1
  route-target import 100:1
 exit-address-family
!
vrf definition Mgmt-vrf
 --More--          !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition OT_VRF
 rd 700:1
 !
 address-family ipv4
  route-target export 700:1
  route-target import 700:1
 exit-address-family
!
vrf definition VnV_VRF
 rd 500:1
 !
 address-family ipv4
  route-target export 500:1
  route-target import 500:1
 exit-address-family
!
 --More--          no aaa new-model
switch 1 provision c9500-16x
switch 2 provision c9500-16x
ip routing
!
```

```
ip multicast-routing vrf Management_VRF
ip domain name wf.com
ip dhcp excluded-address 10.10.101.1 10.10.101.50
!
login on-success log
!
--More--         !
!
stackwise-virtual
 domain 2
!
flow exporter 192.168.6.100
 destination 192.168.6.100
 transport udp 6007
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint TP-self-signed-3141569633
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3141569633
 revocation-check none
 rsakeypair TP-self-signed-3141569633
 hash sha256
crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
 source interface Vlan101
 hash sha256
!
license boot level network-advantage addon dna-advantage
memory free low-watermark processor 131093
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
enable secret 9 $9$rT5UEjrWOcqDA.$e2FNehaH33QAJmEoMFTYOslVMrUmX2wD5IymWpNaSDo
!
username dna password 0 Cisco@123
!
redundancy
 mode sso
crypto engine compliance shield disable
!
transceiver type all
 monitoring
!
vlan 2508
 remote-span
!
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 ot_traffic_o
 match ip dscp af21
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 ot_traffic
 match access-group name IXIA_TRAFFIC
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
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 video_o
 match ip dscp af41
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 network_control
 match ip dscp cs2
class-map match-any voice_o
 match ip dscp ef
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any scavenger_o
 match ip dscp cs1
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 bulk_data
 match ip dscp af11
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 bulk_data_o
match ip dscp af11
class-map match-any video
 match ip dscp af41
class-map match-any system-cpp-police-ios-routing
  description L2 control, Topology control, Routing control, Low Latency
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
class-map match-any voice
 match ip dscp ef
class-map match-any network_control_o
 match ip dscp cs2
class-map match-any system-cpp-police-ios-feature
  description
ICMPGEN,BROADCAST,ICMP,L2LVXCntrl,ProtoSnoop,PuntWebauth,MCASTData,Transit,DOT1XAuth,Swfwd,L
OGGING,L2LVXData,ForusTraffic,ForusARP,McastEndStn,Openflow,Exception,EGRExcption,NflSampled
,RpfFailed
class-map match-any scavenger
 match ip dscp cs1
!
policy-map system-cpp-policy
policy-map output
 class voice_o
```

```
  priority level 1
 class video_o
bandwidth remaining percent 10
 class ot_traffic_o
  bandwidth remaining percent 10
 class network_control_o
  bandwidth remaining percent 10
 class bulk_data_o
  bandwidth remaining percent 10
 class scavenger_o
  bandwidth remaining percent 10
 class class-default
  bandwidth remaining percent 15
policy-map input
 class voice
  set dscp ef
 class video
  set dscp af41
 class ot_traffic
  set dscp af21
 class network_control
  set dscp cs2
 class bulk_data
  set dscp af11
 class scavenger
set dscp cs1
 class class-default
  set dscp default
!
interface Loopback0
 ip address 192.168.5.2 255.255.255.255
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 101,500,700
switchport mode trunk
!
interface Port-channel11
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 negotiation auto
!
interface TenGigabitEthernet1/0/1
 description connectedToFPROldY015
 switchport access vlan 100
 switchport mode access
!
interface TenGigabitEthernet1/0/2
 switchport access vlan 101
 switchport mode access
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
 channel-group 1 mode active
 service-policy input input
 service-policy output output
!
interface TenGigabitEthernet1/0/4
!
interface TenGigabitEthernet1/0/5
 switchport access vlan 100
```

```
 switchport mode access
!
interface TenGigabitEthernet1/0/6
!
interface TenGigabitEthernet1/0/7
 switchport access vlan 100
 switchport mode access
!
interface TenGigabitEthernet1/0/8
!
interface TenGigabitEthernet1/0/9
 switchport access vlan 100
 switchport mode access
!
interface TenGigabitEthernet1/0/10
!
interface TenGigabitEthernet1/0/11
 switchport mode trunk
interface TenGigabitEthernet1/0/12
!
interface TenGigabitEthernet1/0/13
 switchport access vlan 214
 switchport mode access
!
interface TenGigabitEthernet1/0/14
!
interface TenGigabitEthernet1/0/15
 shutdown
!
interface TenGigabitEthernet1/0/16
!
interface TenGigabitEthernet1/1/1
 stackwise-virtual link 1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
 description Connected to Port TenGig1/1/1 on OSS-C9300-Access SW
 switchport mode trunk
 channel-group 11 mode desirable
 service-policy input input
 service-policy output output
!
interface TenGigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/5
 stackwise-virtual dual-active-detection
!
interface TenGigabitEthernet1/1/6
!
interface TenGigabitEthernet1/1/7
 switchport trunk allowed vlan 101,500,700
 switchport mode trunk
 channel-group 2 mode active
!
interface TenGigabitEthernet1/1/8
!
interface FortyGigabitEthernet1/1/1
!
interface FortyGigabitEthernet1/1/2
!
interface TenGigabitEthernet2/0/1
 description connectedToFPRNewX02B
switchport access vlan 100
 switchport mode access
```

```
!
interface TenGigabitEthernet2/0/2
!
interface TenGigabitEthernet2/0/3
!
interface TenGigabitEthernet2/0/4
 switchport access vlan 100
 switchport mode access
!
interface TenGigabitEthernet2/0/5
 switchport mode trunk
 channel-group 1 mode active
 service-policy input input
 service-policy output output
!
interface TenGigabitEthernet2/0/6
!
interface TenGigabitEthernet2/0/7
!
interface TenGigabitEthernet2/0/8
!
interface TenGigabitEthernet2/0/9
!
interface TenGigabitEthernet2/0/10
!
interface TenGigabitEthernet2/0/11
!
interface TenGigabitEthernet2/0/12
!
interface TenGigabitEthernet2/0/13
!
interface TenGigabitEthernet2/0/14
!
interface TenGigabitEthernet2/0/15
!
interface TenGigabitEthernet2/0/16
!
interface TenGigabitEthernet2/1/1
 stackwise-virtual link 1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
 description Connected to Port TenGig1/1/2 on OSS-C9300-Access SW
switchport mode trunk
 channel-group 11 mode desirable
 service-policy input input
 service-policy output output
!
interface TenGigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/5
 stackwise-virtual dual-active-detection
!
interface TenGigabitEthernet2/1/6
!
interface TenGigabitEthernet2/1/7
 switchport trunk allowed vlan 101,500,700
 switchport mode trunk
 channel-group 2 mode active
!
interface TenGigabitEthernet2/1/8
!
interface FortyGigabitEthernet2/1/1
!
```

```
interface FortyGigabitEthernet2/1/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 vrf forwarding Management_VRF
 ip address 10.10.100.1 255.255.255.0
 ip pim sparse-mode
!
interface Vlan101
 vrf forwarding Management_VRF
 ip address 10.10.101.1 255.255.255.0
 ip pim sparse-mode
 ip ospf network point-to-point
!
interface Vlan102
 vrf forwarding Management_VRF
 ip address 10.10.102.1 255.255.255.0
!
interface Vlan103
 vrf forwarding Management_VRF
 ip address 10.10.103.1 255.255.255.0
!
interface Vlan104
 vrf forwarding Management_VRF
 ip address 10.10.104.1 255.255.255.0
!
interface Vlan105
 vrf forwarding Management_VRF
 ip address 10.10.105.1 255.255.255.0
!
interface Vlan114
 vrf forwarding Management_VRF
 ip address 172.114.0.1 255.255.0.0
!
interface Vlan214
 ip address 172.214.0.2 255.255.0.0
!
interface Vlan500
 vrf forwarding VnV_VRF
 ip address 172.16.50.1 255.255.255.0
 ip ospf network point-to-point
!
interface Vlan600
 vrf forwarding VnV_VRF
 ip address 172.16.60.1 255.255.255.0
 --More--         !
interface Vlan700
 vrf forwarding OT_VRF
 ip address 172.16.70.1 255.255.255.0
 ip ospf network point-to-point
!
interface Vlan701
 vrf forwarding OT_VRF
 ip address 172.16.71.1 255.255.255.0
!
interface Vlan800
 ip address 172.16.80.1 255.255.255.0
!
interface Vlan2508
 ip address 169.254.1.3 255.255.255.0
!
router ospf 101 vrf Management_VRF
```

```
 router-id 1.1.1.1
 redistribute connected
 network 10.10.101.0 0.0.0.255 area 0.0.0.0
!
router ospf 500 vrf VnV_VRF
 router-id 1.1.1.1
 --More--         redistribute connected
 network 172.16.50.0 0.0.0.255 area 0.0.0.0
!
router ospf 700 vrf OT_VRF
 router-id 1.1.1.1
 redistribute connected
 network 172.16.70.0 0.0.0.255 area 0.0.0.0
!
iox
ip forward-protocol nd
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
no ip http server
ip http authentication local
no ip http secure-server
ip http client source-interface Vlan101
ip pim rp-address 10.10.100.1
ip pim vrf Management_VRF rp-address 10.10.100.1
ip route vrf Management_VRF 10.10.106.0 255.255.255.0 10.10.100.3
ip ssh bulk-mode 131072
ip ssh source-interface Vlan101
!
ip access-list extended IXIA_TRAFFIC
 10 permit ip 31.0.0.0 0.255.255.255 any
!
logging source-interface Vlan101 vrf Management_VRF
logging host 192.168.6.100 vrf Management_VRF
!
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 cisco123 RW
snmp-server trap-source Vlan101
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 bfd
snmp-server enable traps smart-license
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps rep
snmp-server enable traps memory bufferpeak
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
```

```
snmp-server enable traps energywise
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps udld link-fail-rpt
snmp-server enable traps udld status-change
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 envmon
snmp-server enable traps stackwise
snmp-server enable traps mvpn
snmp-server enable traps pw vc
snmp-server enable traps ipsla
snmp-server enable traps dhcp
snmp-server enable traps event-manager
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 ospfv3 state-change
snmp-server enable traps ospfv3 errors
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 bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps bgp cbgp2
snmp-server enable traps hsrp
snmp-server enable traps isis
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps lisp
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 entity-diag boot-up-fail hm-test-recover hm-thresh-reached
scheduled-test-fail
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 bulkstat collection transfer
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps transceiver all
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server enable traps rf
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfc vpn
```

```
snmp-server host 192.168.6.100 vrf Management_VRF version 3 priv cisco
!
control-plane
 service-policy input system-cpp-policy
!
line con 0
 stopbits 1
line vty 0 4
 login local
 transport preferred none
 transport input ssh
line vty 5 15
 login local
 transport preferred none
 transport input ssh
!
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
!
End
```

FAN Ring Switch Configuration (Non Edge Switch that is Not a Part of TAN Rings)

```
hostname FAN-BS4
!
no aaa new-model
rep ztp
rep autodisc
ptp mode e2etransparent
vtp mode transparent
vtp version 1
!

ip domain name wf.com
!

login on-success log
!
flow exporter 192.168.6.100
 destination 192.168.6.100
 transport udp 6007
!
device-tracking tracking
!
device-tracking policy IPDT_POLICY
 no protocol udp
 tracking enable
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
archive
 log config
  logging enable
  logging size 500
```

```
memory free low-watermark processor 63461
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause psp
errdisable recovery cause mrp-miscabling
errdisable recovery cause loopdetect
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
enable secret 9 $9$WvAxOEesAzfnN.$mRkA6cTyFxVetsh9504kUwfrc8RwL6bTpBCrpmk3iX.
!
username dna privilege 15 secret 9
$9$yDOgMvOokBX0RE$GNMGJxJjEFqdauVf/VUwO./tvTz5TSeuKyWXarTFw4c
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
vlan 101
lldp run
!
interface GigabitEthernet1/1
 description PNP STARTUP VLAN
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 rep segment 12
 rep ztp-enable
!
interface GigabitEthernet1/2
 switchport trunk allowed vlan 1-2507,2509-4094
 switchport mode trunk
 device-tracking attach-policy IPDT_POLICY
 rep segment 12
 rep ztp-enable
!
interface GigabitEthernet1/3
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/4
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/5
 device-tracking attach-policy IPDT_POLICY
```

```
!
interface GigabitEthernet1/6
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/7
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/8
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/9
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/10
 device-tracking attach-policy IPDT_POLICY
!
interface AppGigabitEthernet1/1
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan101
 ip dhcp client client-id ascii cisco-0029.c23c.598b-Vl101
 ip address dhcp
!
no ip http server
ip http authentication local
no ip http secure-server
ip http client source-interface Vlan101
ip forward-protocol nd
!
ip ssh bulk-mode 131072
ip ssh source-interface Vlan101
ip scp server enable
!
logging source-interface Vlan101
logging host 192.168.6.100
!
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
snmp-server view DNAC-ACCESS iso included
snmp-server trap-source Vlan101
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
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 power-ethernet police
snmp-server enable traps rep
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
```

```
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps port-security
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps smart-license
snmp-server enable traps event-manager
snmp-server enable traps ipsla
snmp-server enable traps transceiver all
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 bfd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
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 bgp cbgp2
snmp-server enable traps dhcp
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached
scheduled-test-fail
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune rp-
mapping-change interface-election
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps alarms informational
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps rf
snmp-server host 192.168.6.100 version 3 priv cisco
!
control-plane
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login local
 transport preferred none
 transport input ssh
line vty 5 15
 login local
 transport preferred none
 transport input ssh
```

```
!
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
!
pnp profile pnp-zero-touch
 transport https ipv4 192.168.6.100 port 443
pnp startup-vlan 101
End
```

QoS on IE-3400

```
!
Extended IP access list OT_TRAFFIC
10 permit ip 172.10.0.0 0.255.255.255 any
!

!
class-map match-any ot_traffic
 match access-group name OT_TRAFFIC

class-map match-any network_control
 match ip dscp cs2

class-map match-any bulk_data
 match ip dscp af11

class-map match-any video
 match ip dscp af41

class-map match-any voice
 match ip dscp ef

class-map match-any scavenger
 match ip dscp cs1
!

policy-map input
 class voice
  set dscp ef
 class video
  set dscp af41
 class ot_traffic
  set dscp af21
 class network_control
  set dscp cs2
 class bulk_data
  set dscp af11
 class scavenger
  set dscp cs1
 class class-default
  set dscp default
!
policy-map output
 class voice_o
  priority
 class video_o
  bandwidth remaining percent 10
 class ot_traffic_o
  bandwidth remaining percent 10
```

```
 class network_control_o
  bandwidth remaining percent 20
 class bulk_data_o
  bandwidth remaining percent 15
 class scavenger_o
  bandwidth remaining percent 15
 class class-default
  bandwidth remaining percent 10
!

interface TenGigabitEthernet 1/1
service-policy input input
service-policy output output
```

QoS on FAN Aggregation and on the OSS and ONSS (C-9300/C-9500)

```
!
Extended IP access list OT_TRAFFIC
10 permit ip 172.10.0.0 0.255.255.255 any
!

!
class-map match-any ot_traffic
 match access-group name OT_TRAFFIC

class-map match-any network_control
 match ip dscp cs2

class-map match-any bulk_data
 match ip dscp af11

class-map match-any video
 match ip dscp af41

class-map match-any voice
 match ip dscp ef

class-map match-any scavenger
 match ip dscp cs1
!
policy-map input
 class voice
  set dscp ef
 class video
  set dscp af41
 class ot_traffic
  set dscp af21
 class network_control
  set dscp cs2
 class bulk_data
  set dscp af11
 class scavenger
  set dscp cs1
 class class-default
  set dscp default
!

!
policy-map output
 class voice_o
  priority level 1
 class video_o
  bandwidth remaining percent 10
 class ot_traffic_o
  bandwidth remaining percent 10
```

```
 class network_control_o
  bandwidth remaining percent 20
 class bulk_data_o
  bandwidth remaining percent 15
 class scavenger_o
  bandwidth remaining percent 15
 class class-default
  bandwidth remaining percent 10

!

interface TenGigabitEthernet 1/1
service-policy input input
service-policy output output
!
```

Appendix B: Cisco Catalyst Center Day N Templates

Cisco Catalyst Center templates can be used to apply configurations to multiple switches at a time. The following are various templates that can be created on Cisco Catalyst Center for easy configuration changes on wind farm devices.

VLAN Creation

```
vlan $vlan_id
name $vlan_name
```

Vrf Creation

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

VLAN Interface Creation and Addition of a VRF

```
interface Vlan$vlan_id
 vrf forwarding $VRF_name
 ip address 10.10.$vlan_id.1 255.255.255.0
!
```

Port-channel Creation

```
interface $int_one
channel-group $PCNo mode desirable
no shut
interface $int_two
channel-group $PCNo mode desirable
no shut
```

Shut/Unshut an Interface

```
#if ($shut == 1)
interface $int_name
shutdown

#else
interface $int_name
no shut
#end
```

Appendix C: Turbine Operator Network Configuration

C9300 Switch:

```
hostname SCADA-C9300-1
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
!
aaa authentication dot1x default group radius local
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization exec default local
aaa authorization network default group radius local
aaa authorization network MACSEC-UPLINK local
aaa authorization auth-proxy default group radius
aaa authorization credential-download default local
aaa authorization credential-download MACSEC-UPLINK local
aaa accounting identity default start-stop group radius
!
!
aaa attribute list MUST-SECURE
 attribute type linksec-policy must-secure
!
aaa session-id common
clock timezone UTC 5 30
boot system switch all flash:cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20231115_063559_V17_14_0_13.SSA.bin
switch 1 provision c9300-24ux
eap profile EAP-PROFILE
 method tls
 pki-trustpoint CA
!
!
!
!
!
ip routing
!
!
!
!
!
ip multicast-routing
ip domain name wf.com
!
!
!
login on-success log
vtp mode transparent
!
!
```

```
!
!
!
!
!
!
access-session mac-move deny
!
key chain MAC-SEC macsec
 key 4000000000000000000000000000000000000000000000000000000000000000
  cryptographic-algorithm aes-128-cmac
  key-string CAFECAFECAFECAFE0CAFE0CAFE0CAFE0
  lifetime local 00:00:00 Jan 1 1993 infinite
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint TP-self-signed-1953829722
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1953829722
 revocation-check none
 rsakeypair TP-self-signed-1953829722
 hash sha256
!
crypto pki trustpoint my-trustpoint
 enrollment terminal pem
 serial-number none
 ip-address 10.10.101.25
 subject-name C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN= SCADA-C9300-1-Y819.wf.com
 subject-alt-name SCADA-C9300-1-Y819.wf.com
 revocation-check none
 rsakeypair my-4096rsa-key
 hash sha256
!
crypto pki trustpoint CA
 enrollment url http://10.20.200.1:80
 serial-number
 ip-address none
 subject-name CN=Y819
 revocation-check none
 rsakeypair my-4096rsa-key
 hash sha512
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
```

```
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain TP-self-signed-1953829722
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31393533 38323937 3232301E 170D3233 30393130 31343230
  31365A17 0D333330 39303931 34323031 365A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39353338
  32393732 32308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 0100D294 2D74E554 D2C51BB8 0ACA158C 4F501283 28D76C6E F9E92941
  B1892FE7 3D3B6A8D 8ED577B6 F3904883 0B0E82ED 572EB121 5760527A 49560B0A
  53ED1714 AF004717 09413FC9 EA864694 53BD97C6 624E767C AF2EFDB0 BE51FBDA
  8B66AD78 CA1BD6AF 9C6508FB 8507701B 67CEFAD9 1F9DBC96 D1AA5609 99A1FE32
  1BBDACF4 C034D861 6FD9A6CC F598A52F 06FADEA3 B6AD8CD6 E6D59760 AC9C59D2
  AF6A3E3B 38F8C847 4000697B C59FDD21 D4398617 48EF3791 7038C44E D92729F9
  BD88D8EC 262F5A60 77F9C033 EB300981 F7F61A04 25824B96 D83DA37D EF645079
  5DD8D4A5 86C2A603 C7102E54 BE29DE18 CF96E010 7AA06298 4E712F53 34ECF102
  A0C6AB7D 616B0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 149AD8C8 B507AEE7 B4230FFF 5CA8E098 4C899939
  04301D06 03551D0E 04160414 9AD8C8B5 07AEE7B4 230FFF5C A8E0984C 89993904
  300D0609 2A864886 F70D0101 05050003 82010100 2C228C2C 05BE9ACA 9B2B60AC
  1DA22230 7800F903 FCE40A0C 0E008520 D4F1D7B6 A5E465F4 708D8ECC 0EFAE2A3
  62FFD115 7241F686 99D4658C 70BD7BF5 CEE86844 63A6FC3B 9F999E5B BCF1F558
  78F6E593 F436165D 94C522FB 33B8FE55 98D0DE0F AF1EAE82 E449B4F2 02B7273B
  6098AB82 2E74937E EDE1B3CB 1CF943A4 9B3FD21F D429B5B8 F0883CEE D7027576
  F7E949CB 1908D833 5FD07E34 F15C961A 6DFA5AA0 16849D4D E498336A 12F798F7
  68037219 8C64280A 3F77509D 33FC1EF0 01552480 2D5FFC4D E50D7533 A49B8552
  70B3653E 7120FACC 4CE4FAEA 38FE81DF FAC4A7CC 68896E8F 9D1F70AA FDEB075B
  C1EA1BC9 85129630 7324C06C F2402E14 3CF7C0F8
        quit
crypto pki certificate chain my-trustpoint
 certificate 5D0000000834C9B4516C9B5106000100000008
  30820557 3082043F A0030201 0202135D 00000008 34C9B451 6C9B5106 00010000
  0008300D 06092A86 4886F70D 01010B05 00301D31 1B301906 03550403 13125749
  4E2D504E 3137554A 54334856 4F2D4341 301E170D 32333130 31373037 32393435
  5A170D32 34313031 37303733 3934355A 306B310B 30090603 55040613 02494E31
  0C300A06 03550408 13034B41 52310C30 0A060355 04071303 424C5231 0E300C06
  0355040A 13056369 73636F31 0C300A06 0355040B 1303494F 54312230 20060355
  04031319 53434144 412D4339 3330302D 312D5938 31392E77 662E636F 6D308202
  22300D06 092A8648 86F70D01 01010500 0382020F 00308202 0A028202 0100C111
  F959BE09 70AF0EB5 EC03303E 208BC446 2ED3DDB8 CDBD9999 5C288A8D D0FC1BD9
  2D57D51B D1982A85 5138057D F42EFEDC 724A2D99 9B32F7E9 F38D6952 44E09CB7
  704F916E 7C28EBC0 8CE99372 7F3A74F4 243BC6DE BF520D5D 95F0AB01 89A464F5
  316BBDA2 0FC3CF4C 170277BA 958D82DC BB7538C8 12ADB3FD E942EA72 1A37357E
  9C5785E5 5B0B7F4D ED2A9364 E34BE545 4E233C58 F01D9398 577565D2 0BFB26F6
  1F5A0980 DB276F4B B9E167E3 279841B2 CD3AC307 828A8874 5DE23A36 6E71DB49
  3B084036 36B454E3 8EE509FF BE4545C2 6A49F535 777BBB86 7A7AD0B8 2F173F87
  92CE8947 B56AE037 CF6DE834 14CCBBDC 848493FD FC8E6BD8 B82B7B50 16507BEB
  92AD4866 A6F957B4 3D323793 89704661 A730CC80 874765D2 A3FC0CE9 55C3EDB6
  C1FFD219 CEEA25BC 2A37FD92 97BE765A 39969A9E 4366BA1A 17545C23 402BC449
  A1F8C82D 989248A8 16ACC6B6 2E6BFB6F 349AD372 C46D3E70 88C628AC 29F2F282
  E294571E 30532138 C74BA5CA 95DACDB4 0F7EBC80 23106216 4FC30798 8BE752F3
  B59BE661 BA3D67A0 03975084 963D1A1B E9462B96 44BD25BD 4CE94410 DE68A4B4
  622EB9EE A195BB18 E190A3EC 41458CF4 C8CB517F 55751976 3C8608E5 94DC820D
  62774746 789DC676 FF46CDB0 862F378B 07EEC0AF 6FB327EA 2C8978E8 BEAF6ADE
  E92B0AA2 A0C98E9B 80067B5A 0D30B3FA 1DD62ACB 65AC7E12 19804EE8 278D0203
  010001A3 82014030 82013C30 0B060355 1D0F0404 030205A0 30240603 551D1104
  1D301B82 19534341 44412D43 39333030 2D312D59 3831392E 77662E63 6F6D301D
  0603551D 0E041604 148707B2 FA3A3D1E 0B80517A DBF6B2C2 60532F77 BB301F06
  03551D23 04183016 8014423B 8A8E6F52 4DF00C73 041B9CBC 2F5FE804 E4D1304E
  0603551D 1F044730 453043A0 41A03F86 3D66696C 653A2F2F 2F2F5749 4E2D504E
  3137554A 54334856 4F2F4365 7274456E 726F6C6C 2F57494E 2D504E31 37554A54
  3348564F 2D434128 31292E63 726C3069 06082B06 01050507 0101045D 305B3059
```

```
  06082B06 01050507 3002864D 66696C65 3A2F2F2F 2F57494E 2D504E31 37554A54
  3348564F 2F436572 74456E72 6F6C6C2F 57494E2D 504E3137 554A5433 48564F5F
  57494E2D 504E3137 554A5433 48564F2D 43412831 292E6372 74300C06 03551D13
  0101FF04 02300030 0D06092A 864886F7 0D01010B 05000382 01010060 985C7255
  A34D9F1A 4F185EA7 1D6A9788 1EB3DD17 5F77FD03 6FF7F384 92EF37A0 8BF7DBBF
  50B37939 02D53E07 C20F7AB7 3DCFDF4F C9DF6006 75776435 7D6516B4 B2DB7B88
  F5A9010A 70787C97 516EF1CA 73719002 6263B7CA 1A06E2B0 59A3A089 53F16486
  4DE9A88E F7524FCF 6A9E40AE 81F72CA3 5E357A67 448D6522 18CB2C5E 4F2DCAEF
  A50AF024 BDA19225 D8B8BD3E C0CBD982 08B6303C 5A6A1897 D53C013B 00CDB8F9
  CC40935F 7AAEA00F B725776B 1042D81E 537BBC3A 172765BD 1697A0E3 E51DEC8A
  0698E537 BDA94E0F 87005150 FF623F50 D9F90845 EF70BE8B E0383F8E 8EE66C0F
  D78C25C9 86418D3D 33B27AC9 CFC9D968 484DA38A 6609533D BA8759
        quit
 certificate ca 5E67662095B742BD41CA0F583A64E1E6
  3082033C 30820224 A0030201 0202105E 67662095 B742BD41 CA0F583A 64E1E630
  0D06092A 864886F7 0D01010B 0500301D 311B3019 06035504 03131257 494E2D50
  4E313755 4A543348 564F2D43 41301E17 0D323331 30303930 39313030 395A170D
  32383130 30393135 31333530 5A301D31 1B301906 03550403 13125749 4E2D504E
  3137554A 54334856 4F2D4341 30820122 300D0609 2A864886 F70D0101 01050003
  82010F00 3082010A 02820101 00BD39BA 8D15127C 5A4E3239 A91B657C EB737C6C
  1183ABF1 EABEFF63 C4093F0E 5178777A A58AB0A7 4FC537A2 FC844FE0 DA345F8C
  28ABCB0E CA6E8837 95921E49 B9A04591 5E3C2C2B 1EEB3C86 7A389A57 5A3C147D
  6C7BC494 626FF74A 2A41C6EE 3EF37587 E58F8945 84EB6854 C3B30689 77AA7A74
  09C2C325 D77B051E 9434AE78 315B022B 63C14E37 E0602A68 2FC91A11 B9083FD9
  EF6CF25F 1952D54C 4C720DB4 C38B9AE5 41DA0D76 CBDD67A5 39D01535 E27BF364
  560DF96A 45F3737E 38629125 5FADB62D 2DADE789 0F2997B8 338E0C14 503BE66A
  2D63AB74 3D882156 E9AE67A3 552308EC 4D0E0E21 DEEAB596 B9DF78CB D7F4B3BA
  E9C62CFC 35C4FEA8 CF6BDED0 DF020301 0001A378 3076300B 0603551D 0F040403
  02018630 0F060355 1D130101 FF040530 030101FF 301D0603 551D0E04 16041442
  3B8A8E6F 524DF00C 73041B9C BC2F5FE8 04E4D130 1206092B 06010401 82371501
  04050203 01000130 2306092B 06010401 82371502 04160414 92052E45 E2E20D2B
  B85013E2 EEA63F49 EE18DCDC 300D0609 2A864886 F70D0101 0B050003 82010100
  2DA1A14F 53FB976A 659254D9 D8109290 7CFAE352 F1AD8BF4 752D9791 6114E46F
  5BDCD3DD 1FF865B9 BE150462 48434289 D907BE07 221DD566 AE368E55 6A0B7DEF
  D0E8756F 5753C899 EC42E405 B10580B9 7224E8D0 4D43A675 08E421E8 8667A4E6
  B9AA45BF 0393E97D 75A9F6B6 231D5B2E 1463A83C BA539DC8 C0C703A0 3B149D72
  DD63063D FD74CC5B CB67FF92 7158C26B A5B6D8AF 7DBC8CB4 3DD33EA4 F9A44706
  8D80F6EA 588711E5 84A32459 3B6EBBB2 22A814C1 C333F34B CC373875 77B9089D
  A03D7D95 41385914 B84084CD 3E8A21BC 7197CCF7 A44CB1FB 26F0E7F2 B1E77562
  8864BCC3 4D535DA7 ECD51219 CC6BB7C9 9DC99B2C B86B4A55 2BA25D48 2128307D
        quit
crypto pki certificate chain CA
 certificate 08
  30820525 3082030D A0030201 02020108 300D0609 2A864886 F70D0101 0D050030
  0E310C30 0A060355 04031303 49535230 1E170D32 34303132 31313335 3734375A
  170D3235 30313230 31333537 34375A30 4D310D30 0B060355 04031304 59383139
  313C3012 06035504 05130B46 4F433237 31325938 31393026 06092A86 4886F70D
  01090216 19534341 44412D43 39333030 2D312D59 3831392E 77662E63 6F6D3082
  0222300D 06092A86 4886F70D 01010105 00038202 0F003082 020A0282 020100C1
  11F959BE 0970AF0E B5EC0330 3E208BC4 462ED3DD B8CDBD99 995C288A 8DD0FC1B
  D92D57D5 1BD1982A 85513805 7DF42EFE DC724A2D 999B32F7 E9F38D69 5244E09C
  B7704F91 6E7C28EB C08CE993 727F3A74 F4243BC6 DEBF520D 5D95F0AB 0189A464
  F5316BBD A20FC3CF 4C170277 BA958D82 DCBB7538 C812ADB3 FDE942EA 721A3735
  7E9C5785 E55B0B7F 4DED2A93 64E34BE5 454E233C 58F01D93 98577565 D20BFB26
  F61F5A09 80DB276F 4BB9E167 E3279841 B2CD3AC3 07828A88 745DE23A 366E71DB
  493B0840 3636B454 E38EE509 FFBE4545 C26A49F5 35777BBB 867A7AD0 B82F173F
  8792CE89 47B56AE0 37CF6DE8 3414CCBB DC848493 FDFC8E6B D8B82B7B 5016507B
  EB92AD48 66A6F957 B43D3237 93897046 61A730CC 80874765 D2A3FC0C E955C3ED
  B6C1FFD2 19CEEA25 BC2A37FD 9297BE76 5A39969A 9E4366BA 1A17545C 23402BC4
  49A1F8C8 2D989248 A816ACC6 B62E6BFB 6F349AD3 72C46D3E 7088C628 AC29F2F2
  82E29457 1E305321 38C74BA5 CA95DACD B40F7EBC 80231062 164FC307 988BE752
  F3B59BE6 61BA3D67 A0039750 84963D1A 1BE9462B 9644BD25 BD4CE944 10DE68A4
  B4622EB9 EEA195BB 18E190A3 EC41458C F4C8CB51 7F557519 763C8608 E594DC82
  0D627747 46789DC6 76FF46CD B0862F37 8B07EEC0 AF6FB327 EA2C8978 E8BEAF6A
  DEE92B0A A2A0C98E 9B80067B 5A0D30B3 FA1DD62A CB65AC7E 1219804E E8278D02
  03010001 A34F304D 300B0603 551D0F04 04030205 A0301F06 03551D23 04183016
  80141307 525E8608 9D1968D8 F1F23140 CD3DA76E D144301D 0603551D 0E041604
  148707B2 FA3A3D1E 0B80517A DBF6B2C2 60532F77 BB300D06 092A8648 86F70D01
```

```
  010D0500 03820201 009868EC 4441CD5E D02B96AF B94FAFE3 DB096EB1 FAF7FD9D
  AEF0EFEB 5138163C 21C4680C 93A26F1A 1BFC886A 9E3E3579 2B06DF9E DD84CC9C
  54400113 197B6B15 165908FC 7731C2B5 FCDA715F 461185F7 D7AB645E 3BB80E4E
  FA14483B 3E238447 4C1C1D18 DB6FB924 268F9A5F FA7505F2 B964B47A 05B48C89
  19AC6C00 D99AAD1D D0DDC15E 0EA3C320 6EA9B07E E5A07616 0DC33612 50F5261A
  D50A52F8 AEBBE7B7 1C73E9E6 24EB218B 4E102D2D F9BD3EB9 6E4FE67B 779ED34C
  71FB2861 06C7E640 4EF3912C 0AE53391 929AC6CB 4E1D52EC B21928D4 0D06A483
  D10E05A1 6E761E94 9A1AC722 5ADCD1BB 3F1D1066 5915D68B 7DC844FD ECC1EAE9
  B1205388 E343FE64 404F06EC 920A9547 F603C3C5 99645A41 E74C1883 D4FADD8F
  EE111723 B688A6CE D1934BC4 FE8808C3 740BBFE5 E6B0D297 5F762F38 C42941F6
  6E1FA2D4 3BEC97B3 80D6B144 A4E55A67 BAAB5E1D 792BF7E6 E9483963 6217F0C9
  A6100C93 3CE41AC1 ED1A8B82 ED02B33A E790648D A0A6F97E 8C345279 6E43C903
  C1FD37F9 3AA573CB 98BDCF69 546FC2A3 04F1CC30 65F70606 308549CF 2D51FD03
  D53DFD16 9A89C955 FF461104 EF578A6F FB19CE99 3B74F9CC 11E66795 15631337
  12EC2607 73F234FE E135B13C B5409A5F E298D96D BEB5A35C 35B59F57 83DA8084
  2E2D6EFE 0B2CC57E 42BAFA7E A6E2FA40 AE7CF359 DAF08F7B B9421015 C14E469C
  8D7251C2 74755EC3 71
        quit
 certificate ca 01
  308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  0E310C30 0A060355 04031303 49535230 1E170D32 33313232 32303631 3131355A
  170D3236 31323231 30363131 31355A30 0E310C30 0A060355 04031303 49535230
  82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02 82020100
  C93FCBD8 F9044D93 7FD17F8C F7A466CE 86303FB7 961EF078 32735D8B B55E6105
  D0F10B77 DC368C25 31C4018E AB3AABD1 A2A33AA0 2D0F8606 C34DF26F E877546A
  4EEEB656 D4374570 A2923C21 788364DD ABAA7F51 F3E4099E 5EB4CAA5 29E0FE0A
  075D2689 BCC92916 0BF88269 1509DE8C 10537C63 8A03D129 30792797 3EDA3630
  362067CD 072D3285 3A4046D7 0AA2CBDF 23F5A28C 3B5B8551 CB46C313 F23430BC
  60BBF346 F1957919 CF6787D9 0032295F D2796DAF E508294F F49664B9 D7031865
  092C3546 C94E0E19 352E5815 289419BA B2C840FD 0AFCA295 3FA7B91D 4E06CEEF
  5B2E2AD8 7C3CFBED 760D92E9 FE5C4382 85E73DE8 8559B059 A2F9D88C 00F942C6
  3D83213B 5ADBCBD5 B6ED1E44 424F2372 B670FF9F CD87DC38 A4EB3D65 D8DE59F1
  61385435 F20B03C6 D8FF9047 95F14E8E C0F2545E A632418F 9C79141B 6C352661
  B4E228EF AE5764BA 85094A44 3BEEC94E A6779A0D B3239873 40B77AD9 FAA25B81
  7E606F4B 68ACDE7B 5F55AEE4 7084FA8D C6C44B9A 06445DB7 CD32D8C7 EE37393C
  9E3575FD DF3ACCF6 04E8C549 0A76486C E6D5F6C3 CE7C75F1 0486FC0E 16BF7DB6
  0C13A497 D8C1FEFF 34AA67EE 42922309 9D7E876F F3985091 4A9024C2 E62151F1
  B7231AD3 5CA1C579 D79FD49D 30E24DEF DD93905D 8CD1FEB7 56F1111F BE1D1E74
  D6E2F32C C864A2ED 327FA8F5 6A3DB351 A254182B D4ACC070 DEABFE4C 915FBCB9
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 16801413 07525E86 089D1968
  D8F1F231 40CD3DA7 6ED14430 1D060355 1D0E0416 04141307 525E8608 9D1968D8
  F1F23140 CD3DA76E D144300D 06092A86 4886F70D 01010D05 00038202 0100C5ED
  B8AD3E39 A6B19533 3D029858 35FC67B7 CEF78131 AD879855 B2C70CBD 4E9D7D4A
  AE86430A E5F6399B 8B95AA07 C2C1ADC8 AD90ECB5 F5B42F69 028EFE47 D551E18B
  237357F6 0525D0E1 4B2CAEE1 9C331260 491421E0 A00AAE96 FE196B18 A43E9D54
  A754FCE5 B8758B34 082A4B0F 8015A7C6 09DD11CE 5CE1A7BE 26447759 FAFC73A6
  07F2270F 1768CA0F 90AEB12A 35AF668A 945721B5 ABBB2641 B31B8D88 CE098C19
  F6BBABE8 91046FC9 E37558EE 433BA7FD 19F16F4E 1C4FA14A 8E06217B 5A3469D0
  0419B1EF 711A2C8E BC25E628 F2738D58 F9547857 22C6CBDF D79C27B0 52E36EC5
  D8F0A1E9 33D4E7C6 D90429BD BAE9545F EAE8F78E D48662B8 2B6FD7B4 8405B1A7
  D0790E88 31482F89 410D7A31 3CC376CA 5375D649 ABF76307 C5A6E5E9 59827A8E
  6C705E59 32985A51 F0B10A18 96252952 80DFBBFA BE7A9605 4B8060A6 98790B17
  02D1143D 7A8121D2 21EFDE23 9C934085 42835E29 CE11C60B 8A1452FE 160BCF0D
  78BFC763 6E909872 7AC5939C B593A376 F0031BE3 B428A015 C07941FF A1EF4C63
  FDAE7A33 DEE55B66 FB52B3AE 01818D63 5FE54C28 95706297 5D448562 3A380D9C
  8B1A9D5F 2ACA1518 CF24DC21 8182A63A 97166FF5 7555D85F 84BCF8F9 CF60DBBA
  FF88F098 6638D179 62F1FA7E 026FA05E A5633F16 4FB6B514 EBF135F5 441CE34C
  A9700577 591F02AF FD3DB02F D8390514 F3A812D7 9E76BF4B 2C2CBDA3 DA
  92
        quit
!
!
license boot level network-advantage addon dna-advantage
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 webauth-global-inactive
 inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
 username usr-macsec
 pki-trustpoint CA
!
memory free low-watermark processor 131696
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
mka policy MKA-POLICY
 key-server priority 150
 sak-rekey interval 65535
!
!
!
username usr-macsec aaa attribute list MUST-SECURE
!
redundancy
 mode sso
!
!
!
!
!
transceiver type all
 monitoring
!
vlan 5
 name Multicast_VLAN
!
vlan 10
 name PrivateVLANvlan
  private-vlan primary
  private-vlan association 101,102
!
vlan 20
 name IXIA_TrafficTestVLAN
!
!
           vlan 101
  name isolated_VLAN
  private-vlan isolated
!
!
vlan 111
 name Management_VLAN
!
!
!
lldp run
!
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
 event authentication-failure match-all
```

```
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
policy-map system-cpp-policy
!
!
!
!
!
!
!
!
!
!
!
service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface Port-channel1
 switchport mode trunk
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 negotiation auto
!
interface TenGigabitEthernet1/0/1
 switchport mode trunk
!
interface TenGigabitEthernet1/0/2
!
interface TenGigabitEthernet1/0/3
 switchport mode trunk
!
interface TenGigabitEthernet1/0/4
!
interface TenGigabitEthernet1/0/5
 switchport access vlan 20
 switchport mode access
 device-tracking
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface TenGigabitEthernet1/0/6
 description Connected to WF-NUC-PC2 Windows 11 Host
 switchport private-vlan mapping 10 101
 switchport mode private-vlan promiscuous
 speed 1000
 duplex full
 spanning-tree portfast
!
interface TenGigabitEthernet1/0/7
 switchport access vlan 100
 switchport mode access
!
interface TenGigabitEthernet1/0/8
!
interface TenGigabitEthernet1/0/9
!
interface TenGigabitEthernet1/0/10
 switchport mode private-vlan promiscuous
!
interface TenGigabitEthernet1/0/11
!
```

```
interface TenGigabitEthernet1/0/12
!
interface TenGigabitEthernet1/0/13
!
interface TenGigabitEthernet1/0/14
!
interface TenGigabitEthernet1/0/15
!
interface TenGigabitEthernet1/0/16
!
interface TenGigabitEthernet1/0/17
!
interface TenGigabitEthernet1/0/18
!
interface TenGigabitEthernet1/0/19
!
interface TenGigabitEthernet1/0/20
!
interface TenGigabitEthernet1/0/21
!
interface TenGigabitEthernet1/0/22
 switchport mode trunk
 macsec network-link
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 channel-group 1 mode active
 service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface TenGigabitEthernet1/0/23
 switchport private-vlan mapping 10 101
 switchport mode private-vlan promiscuous
!
interface TenGigabitEthernet1/0/24
 switchport mode trunk
 macsec network-link
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 channel-group 1 mode active
 service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface GigabitEthernet1/1/1
 switchport mode private-vlan promiscuous
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
 switchport mode trunk
 rep segment 1 edge
 macsec network-link
 mka policy MKA-POLICY
 mka pre-shared-key key-chain MAC-SEC
 service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface TenGigabitEthernet1/1/2
 switchport mode trunk
 mka policy MKA-POLICY
 mka pre-shared-key key-chain MAC-SEC
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
```

```
interface TenGigabitEthernet1/1/5
!
interface TenGigabitEthernet1/1/6
!
interface TenGigabitEthernet1/1/7
!
interface TenGigabitEthernet1/1/8
!
interface FortyGigabitEthernet1/1/1
!
interface FortyGigabitEthernet1/1/2
!
interface TwentyFiveGigE1/1/1
!
interface TwentyFiveGigE1/1/2
!
interface AppGigabitEthernet1/0/1
!
interface Vlan1
 no ip address
!
interface Vlan5
 ip address 10.5.1.2 255.255.0.0
 ip pim sparse-mode
 standby 5 ip 10.5.1.1
 private-vlan mapping 501,502
!
interface Vlan10
 ip address 10.10.1.2 255.255.255.0
 standby 1 ip 10.10.1.1
 standby 1 priority 105
 private-vlan mapping 101,102
!
interface Vlan20
 ip address 10.20.1.2 255.255.0.0
 standby 20 ip 10.20.1.1
!
interface Vlan100
 ip address 10.10.100.2 255.255.255.0
!
interface Vlan111
 ip address 10.111.1.2 255.255.255.0
 ip helper-address 10.10.1.10
 standby 111 ip 10.111.1.1
!
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 10.1.0.0 0.0.255.255 area 0
 network 10.10.102.0 0.0.0.255 area 0
 network 10.10.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip pim rp-address 10.5.1.1
ip ssh bulk-mode 131072
!
!
!
!
!
!
control-plane
 service-policy input system-cpp-policy
!
!
!
```

```
line con 0
 stopbits 1
line vty 0 4
 transport input ssh
line vty 5 31
 transport input ssh
!
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
ntp server 10.10.1.10
!
!
!
!
!
!
end
```

IE9320 Switch:

```
hostname WF-SCADA-IE9320-1
!
!
no logging console
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
!
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization network MACSEC-UPLINK local
aaa authorization credential-download MACSEC-UPLINK local
!
!
aaa attribute list MUST-SECURE
 attribute type linksec-policy must-secure
!
aaa session-id common
!
!
!
clock timezone UTC 5 30
boot system switch all flash:ie9k_iosxe.BLD_POLARIS_DEV_LATEST_20240313_033241_V17_15_0_18.SSA.bin
switch 1 provision ie-9320-22s2c4x
eap profile EAP-PROFILE
 method tls
 pki-trustpoint CA
!
rep ztp
!
!
!
!
ip routing
!
!
!
!
login on-success log
```

```
vtp mode transparent
!
!
!
!
!
access-session mac-move deny
!
key chain MAC-SEC macsec
 key 4000000000000000000000000000000000000000000000000000000000000000
  cryptographic-algorithm aes-128-cmac
  key-string CAFECAFECAFECAFE0CAFE0CAFE0CAFE0
  lifetime local 00:00:00 Jan 1 1993 infinite
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint TP-self-signed-2076045765
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2076045765
 revocation-check none
 rsakeypair TP-self-signed-2076045765
 hash sha256
!
crypto pki trustpoint my-trustpoint
 enrollment terminal pem
 serial-number none
 ip-address none
 subject-name C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN= WF-SCADA-IE9320-1.wf.com
 subject-alt-name WF-SCADA-IE9320-1.wf.com
 revocation-check none
 rsakeypair my-4096rsa-key
 hash sha256
!
crypto pki trustpoint CA
 enrollment url http://10.20.200.1:80
 serial-number
 fqdn IE9320-1.wf.com
 ip-address none
 subject-name CN=IE9320-1
 subject-alt-name IE9320-1.wf.com
 revocation-check none
 rsakeypair myrsakeys
 auto-enroll regenerate
 hash sha512
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
```

```
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain TP-self-signed-2076045765
crypto pki certificate chain my-trustpoint
 certificate 2300000004D96A262BD2A32F8A000000000004
  30820552 3082043A A0030201 02021323 00000004 D96A262B D2A32F8A 00000000
  0004300D 06092A86 4886F70D 01010B05 00301031 0E300C06 03550403 13055746
  2D434130 1E170D32 33313231 31303835 3531375A 170D3234 31323131 30393035
  31375A30 81933127 30250609 2A864886 F70D0109 02131857 462D5343 4144412D
  49453933 32302D31 2E77662E 636F6D31 0B300906 03550406 1302494E 310C300A
  06035504 0813034B 4152310C 300A0603 55040713 03424C52 310E300C 06035504
  0A130563 6973636F 310C300A 06035504 0B130349 4F543121 301F0603 55040313
  1857462D 53434144 412D4945 39333230 2D312E77 662E636F 6D308202 22300D06
  092A8648 86F70D01 01010500 0382020F 00308202 0A028202 010096D2 404EC7D3
  95616E3A 122CD0CA A213443C 94F812E6 8CFC8062 B054B032 C0CDA806 9E08ED7A
  1BCE3305 35D83634 B8B1F752 3AA87A9B DF4BE684 BDD872BA 3882302D 4F2CF08C
  867B0588 C26F7494 D790BB72 644DC661 CC63271A 26D73F9A 42E3EA4C 564AD9A3
  2158AC9B 3B5A642A D370A6CA 572DAF21 EA24CE32 DEA36965 BBC1B53F F488432A
  227BDCD5 106DFE54 D9BFC1E5 CD4704EF 81F97C87 9843C7F9 4766712A 722C3EB6
  CF5C266F 3451050E FC4F298B 35C4C683 9106E90A 955EC349 49F2F1B7 2885296C
  DB97EE74 A54F9115 61C33EC0 10928CEA A3021031 4A2AA4C8 754ADD86 419B936F
  EAA7ED00 19A8A2DF DDC09530 E02075E8 9AEEE6B2 4325BC89 842DBE66 A424043D
  DAA2DE6C F011BB46 F5FAD4EA 9451A154 C29B9BC2 945AFBF1 E97EA8FE 42DC792D
  08EE323F 8FCEFBA4 AABE2C9E ABF95DF2 22582502 8D008E92 5CD6325B 270988C7
  F5250C3C AEE09316 FB6B5347 69331BB3 9FEE38AC DE344DFC D0174310 3305DDDA
  F08B387B C9E14D86 098D7522 EF6D9CB0 E5ECBD67 4EFB2283 25210BA1 354EBA7F
  451D364C 303B1D86 665E99EF 6F48EE0A 21E5EEAA A11AFC92 8EA0C89F 79423D62
  22E698ED D15152B3 8C9ED207 F2F2B99E DB665785 A8240A05 383296B1 4B3FE90B
  7D04B354 360010B2 0625495E 04A2F3E4 AC5CD7A4 316EDC56 1B1730C4 7D40B04C
  4F375F86 2B235DC9 7E44C8B4 58887525 A5A098B7 51BD7AA9 B7410203 010001A3
  82011F30 82011B30 0B060355 1D0F0404 030205A0 30230603 551D1104 1C301A82
  1857462D 53434144 412D4945 39333230 2D312E77 662E636F 6D301D06 03551D0E
  04160414 0853300A C3D98AEB 9BFA6356 830519F8 3FEB7A50 301F0603 551D2304
  18301680 1414C04B 830396F5 BCFEE923 357FBED5 2541B87C 93303E06 03551D1F
  04373035 3033A031 A02F862D 66696C65 3A2F2F2F 2F57494E 2D383231 55524E41
  314C3444 2F436572 74456E72 6F6C6C2F 57462D43 412E6372 6C305906 082B0601
  05050701 01044D30 4B304906 082B0601 05050730 02863D66 696C653A 2F2F2F2F
  57494E2D 38323155 524E4131 4C34442F 43657274 456E726F 6C6C2F57 494E2D38
  32315552 4E41314C 34445F57 462D4341 2E637274 300C0603 551D1301 01FF0402
  3000300D 06092A86 4886F70D 01010B05 00038201 0100B643 3FE988CB F49E5571
  4D79B79C 5D59004F 265B455F E7F2E1B2 730F135E E64E77C1 E93A40FF 395E600E
  484D395D 9AD98891 9A9BCEFE 5C3BB116 6A825611 0B8AD7E4 D6A64FFB 4ECF8D58
  6211FD42 CB18CE32 EEE9BB42 CA01A5DD EFF316AA 7C5354A4 D1265509 6B6D83ED
  3ABF3816 E4CF4DCF 5CCEAFC8 8630C28B 71792D6E 18B08F1F 2D3F1706 355B95AA
  DAC71AEB A053AA71 DD06054F B7C67E1F 4D56A8C7 EA3C03A9 8C8C6325 11EC0EE5
  895BF0BC 88C1ADC9 393106B4 3097AD17 AD97BFE4 E984A455 9E46C52D 41BC0A51
  DBB578EC D5738D9C 22B1A19A 7F0F6DA2 57629DE2 93A04B7E 41CE1178 A6BE1D3B
  9CA647B5 17E33F58 CB354E59 9E030AE2 BFC228AC 9EB2
        quit
 certificate ca 3557E375F43B3AA14CC7023E5EF23AD1
  308202FB 308201E3 A0030201 02021035 57E375F4 3B3AA14C C7023E5E F23AD130
  0D06092A 864886F7 0D01010B 05003010 310E300C 06035504 03130557 462D4341
  301E170D 32333132 31313038 31333337 5A170D32 38313231 31303832 3333375A
  3010310E 300C0603 55040313 0557462D 43413082 0122300D 06092A86 4886F70D
  01010105 00038201 0F003082 010A0282 010100C9 4E2F650A 919384C8 2053EDC0
  9AC7E33B 9D04D1AB 35BA43F2 C948238D 5F4AFB2A 6A9DCF57 2F8F59EE DEC9360D
  E7ADFBFF 51A22D11 8F5B644B 834BF712 7DF5404C DA023189 83427288 E760D257
  072B7A82 E3937236 8B7978FF 26EFEA9D 92121113 650EF3B3 7655FA00 FB8DFFC7
  C003DCC8 2E92DFC2 25990E48 453FA17A 497506B9 12333B62 AF6DD71C 8A3F75DA
  E9EA44AB 9C811DD2 351B07C3 1328A54C 96B09759 5FCA65FC 3F6BF2E5 7014EE88
```

```
  5558D298 B46D5233 F9779641 D67CE011 42655411 1E239E3C E73EC9F5 0CBCFC09
  B2794AD9 5435B73F 0FE12D44 424BBA0A CAD97B96 91F9DE11 84A53082 16895BA4
  2789F268 10BF857C D18042FD 9A926891 7B28FF02 03010001 A351304F 300B0603
  551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
  0E041604 1414C04B 830396F5 BCFEE923 357FBED5 2541B87C 93301006 092B0601
  04018237 15010403 02010030 0D06092A 864886F7 0D01010B 05000382 01010018
  F2167B6C 00889A0C 9FB8D3EE 9BA6B019 13D70061 43E94DA0 07543FBB 2E45FCDE
  2A62740C 802CB61D AB8B1931 48C63425 7AA89FDA 555C9734 D2E7C6FA 7785072E
  D481E2A3 07A65D6C 42703D03 39A95694 4BCC7B5A 549EE2C1 6CB20516 F86E711A
  54FB9AE3 0CC242F1 D8D0F314 8E33E6F9 99BE3FA8 74F19CF8 5108A4B0 D5B008A3
  1F591830 2F11756E 963E0A40 7681CB71 2A801C74 316E66D8 4237C923 A3AF7B69
  03AFA6D8 E6446BA8 03BA7410 D8433A0B A31CA430 FA1FB1DA 9FA48616 66882E2F
  8B24BD77 34C65D6F 4E007CBF BCA264AE 650CC2A4 5D383FC2 2F55D395 6B026B3F
  29262E20 76A077F5 B10976DF 4DBB4FF1 9C3BADC3 4B243445 359E5B14 65168A
        quit
crypto pki certificate chain CA
 certificate 09
  3082043B 30820223 A0030201 02020109 300D0609 2A864886 F70D0101 0D050030
  0E310C30 0A060355 04031303 49535230 1E170D32 34303132 31313431 3635305A
  170D3235 30313230 31343136 35305A30 47311130 0F060355 04031308 49453933
  32302D31 31323012 06035504 05130B46 444F3237 31334A4A 5A32301C 06092A86
  4886F70D 01090216 0F494539 3332302D 312E7766 2E636F6D 30820122 300D0609
  2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C1D474 716BDC22
  B26DD240 FC87FB4B 73671D75 96F0C592 32FEA394 BA6D045A B0CE1086 B6189747
  96A86413 2AC664F4 794AF846 F6EC11F8 9CB39C06 859F0F8D B8B1D945 C9A819F8
  49D6A6EA A834F008 34A95096 87C3ACEE C99916B6 E1E01D6F 64982959 1EECC3CE
  6F0AB09D 6E395F74 B39FC126 E065A68C 1755B107 F266100E 05130ED9 38AA1BDD
  0CC99691 51BC6EB7 0AB8AFE9 43444509 D403A761 8F1D36B7 75900DFD 75705205
  A689C397 8E8B0651 7A8DF3A1 55E96AA8 479F6C5A D8F73284 545378F2 855363C1
  6D021043 CC5137C4 6F31F45C A420C26C A06E112D 23F05622 07EEFAB7 5A9AE07C
  4D1087B2 05B82AE4 51A176D1 680F893A 9DF2EB52 2B42BEF2 3D020301 0001A36B
  3069300B 0603551D 0F040403 0205A030 1A060355 1D110413 3011820F 49453933
  32302D31 2E77662E 636F6D30 1F060355 1D230418 30168014 1307525E 86089D19
  68D8F1F2 3140CD3D A76ED144 301D0603 551D0E04 1604142F C8D84E19 ED10DE20
  7C085E89 A5DA680D 41583C30 0D06092A 864886F7 0D01010D 05000382 02010043
  9C166BE1 6D6A2AC1 B3812387 F036AF2C 0CD0C323 1C9255A3 1DD85EEC BCA859DD
  69833DD0 D7B6FD67 A55BCA17 1782608A 66804FBE D6BA3F80 5462EBCB 265B526C
  84D77EF7 0034BDE5 D311415D EF093064 6F39909E 57D59943 CB57EF29 54EB8432
  4D95E59A 66CD9A02 4DFA7847 37239A49 6F02870E 26AC1FD6 62E76396 BDCC615F
  7AD9493F 1DD04D33 98B3D54C 8E2869A1 2269973C 626F58F7 BBBC24AA DACB7A42
  ABD5E0F6 2BD1A8FD 0ED16FE8 290D2C85 2101B06A 6DCF07DB 3241A6F5 D8092618
  776E6A70 E0922C6D 467ADD81 48A1676F C90CBA5A 2BF3DD2B 29A009A5 7D01D0EF
  0AF5D0F1 F42E50B7 D189AB88 99E58074 62D7236B F4984888 20BF5EE1 9BF530AC
  D98D4820 8E0D873A 6BC184EC C128262F 7D014CB4 F527B6BE F0D30187 963618D3
  ECE5034C 356CF71D 564C6788 D940C3CE 201D802B 84A738AC CD2064A5 BE1A3BAA
  E71C8D9B A3BB1D6B 8C11FBFE E9DAF4A8 6DE93120 39F70CC0 FE4F9C71 456998F9
  012E9769 5810E7BA 3F0F7B15 772122BD 4BEBE2C4 65BE3775 2A26B602 F4D5290D
  090249BE 9ADD250E E73DFDB4 F1522CBF ED92F372 CE2342D1 DF42B27A 16900D9D
  178E0D18 E1CD3DF9 068EF56D D3D3605A 9BC160A8 C07190E0 53FF3A97 F6061D5A
  2D4E0FDF BDCD2127 A31E3A77 8BB13E8D 408EEB46 7BA6CB0F E27E2347 F09CB727
  98563284 F677D415 06001A5B 43411B20 3E288B38 B1478055 F703C539 28185E
        quit
 certificate ca 01
  308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
  0E310C30 0A060355 04031303 49535230 1E170D32 33313232 32303631 3131355A
  170D3236 31323231 30363131 31355A30 0E310C30 0A060355 04031303 49535230
  82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02 82020100
  C93FCBD8 F9044D93 7FD17F8C F7A466CE 86303FB7 961EF078 32735D8B B55E6105
  D0F10B77 DC368C25 31C4018E AB3AABD1 A2A33AA0 2D0F8606 C34DF26F E877546A
  4EEEB656 D4374570 A2923C21 788364DD ABAA7F51 F3E4099E 5EB4CAA5 29E0FE0A
  075D2689 BCC92916 0BF88269 1509DE8C 10537C63 8A03D129 30792797 3EDA3630
  362067CD 072D3285 3A4046D7 0AA2CBDF 23F5A28C 3B5B8551 CB46C313 F23430BC
  60BBF346 F1957919 CF6787D9 0032295F D2796DAF E508294F F49664B9 D7031865
  092C3546 C94E0E19 352E5815 289419BA B2C840FD 0AFCA295 3FA7B91D 4E06CEEF
  5B2E2AD8 7C3CFBED 760D92E9 FE5C4382 85E73DE8 8559B059 A2F9D88C 00F942C6
  3D83213B 5ADBCBD5 B6ED1E44 424F2372 B670FF9F CD87DC38 A4EB3D65 D8DE59F1
  61385435 F20B03C6 D8FF9047 95F14E8E C0F2545E A632418F 9C79141B 6C352661
  B4E228EF AE5764BA 85094A44 3BEEC94E A6779A0D B3239873 40B77AD9 FAA25B81
```

```
  7E606F4B 68ACDE7B 5F55AEE4 7084FA8D C6C44B9A 06445DB7 CD32D8C7 EE37393C
  9E3575FD DF3ACCF6 04E8C549 0A76486C E6D5F6C3 CE7C75F1 0486FC0E 16BF7DB6
  0C13A497 D8C1FEFF 34AA67EE 42922309 9D7E876F F3985091 4A9024C2 E62151F1
  B7231AD3 5CA1C579 D79FD49D 30E24DEF DD93905D 8CD1FEB7 56F1111F BE1D1E74
  D6E2F32C C864A2ED 327FA8F5 6A3DB351 A254182B D4ACC070 DEABFE4C 915FBCB9
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 16801413 07525E86 089D1968
  D8F1F231 40CD3DA7 6ED14430 1D060355 1D0E0416 04141307 525E8608 9D1968D8
  F1F23140 CD3DA76E D144300D 06092A86 4886F70D 01010D05 00038202 0100C5ED
  B8AD3E39 A6B19533 3D029858 35FC67B7 CEF78131 AD879855 B2C70CBD 4E9D7D4A
  AE86430A E5F6399B 8B95AA07 C2C1ADC8 AD90ECB5 F5B42F69 028EFE47 D551E18B
  237357F6 0525D0E1 4B2CAEE1 9C331260 491421E0 A00AAE96 FE196B18 A43E9D54
  A754FCE5 B8758B34 082A4B0F 8015A7C6 09DD11CE 5CE1A7BE 26447759 FAFC73A6
  07F2270F 1768CA0F 90AEB12A 35AF668A 945721B5 ABBB2641 B31B8D88 CE098C19
  F6BBABE8 91046FC9 E37558EE 433BA7FD 19F16F4E 1C4FA14A 8E06217B 5A3469D0
  0419B1EF 711A2C8E BC25E628 F2738D58 F9547857 22C6CBDF D79C27B0 52E36EC5
  D8F0A1E9 33D4E7C6 D90429BD BAE9545F EAE8F78E D48662B8 2B6FD7B4 8405B1A7
  D0790E88 31482F89 410D7A31 3CC376CA 5375D649 ABF76307 C5A6E5E9 59827A8E
  6C705E59 32985A51 F0B10A18 96252952 80DFBBFA BE7A9605 4B8060A6 98790B17
  02D1143D 7A8121D2 21EFDE23 9C934085 42835E29 CE11C60B 8A1452FE 160BCF0D
  78BFC763 6E909872 7AC5939C B593A376 F0031BE3 B428A015 C07941FF A1EF4C63
  FDAE7A33 DEE55B66 FB52B3AE 01818D63 5FE54C28 95706297 5D448562 3A380D9C
  8B1A9D5F 2ACA1518 CF24DC21 8182A63A 97166FF5 7555D85F 84BCF8F9 CF60DBBA
  FF88F098 6638D179 62F1FA7E 026FA05E A5633F16 4FB6B514 EBF135F5 441CE34C
  A9700577 591F02AF FD3DB02F D8390514 F3A812D7 9E76BF4B 2C2CBDA3 DA
  92
        quit
!
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 webauth-global-inactive
 inactivity-timer 3600
dot1x system-auth-control
memory free low-watermark processor 59462
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
mka policy MKA-POLICY
 key-server priority 150
 sak-rekey interval 65535
mka policy MKAPolicy
 macsec-cipher-suite gcm-aes-128 gcm-aes-256
!
!
!
username dna aaa attribute list MUST-SECURE
username usr-macsec aaa attribute list MUST-SECURE
!
redundancy
 mode sso

!
```

```
!
!
!
!
!
vlan 5
 name Multicast_VLAN
!
vlan 10
 name PrivateVLANvlan
  private-vlan primary
  private-vlan association 101,102
!
vlan 20
 name IXIA_TrafficTestVLAN
!
!
           vlan 101
  name isolated_VLAN
  private-vlan isolated
!
!
vlan 111
 name Management_VLAN
!
!
!
lldp timer 5
lldp holdtime 20
lldp run
!
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 LevelHPD
 match dscp cs3  af31  af32  af33  cs4  af41  af42  af43
class-map match-any system-cpp-default
 description EWLC data, Inter FED Traffic
class-map match-any LevelLPD
 match dscp default  cs1
class-map match-any LevelMPD
 match dscp cs2  af21  af22  af23
class-map match-any system-cpp-police-sys-data
 description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any LevelMCD
 match dscp cs5  ef  cs6  cs7
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
 event authentication-failure match-all
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
policy-map system-cpp-policy
!
!
!
!
```

```
!
!
!
!
!
!
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
 switchport access vlan 5
 switchport mode access
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
 switchport voice vlan dot1p
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/24
!
interface TenGigabitEthernet1/0/25
 switchport mode trunk
 rep segment 100 edge
 macsec network-link
```

```
 service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface TenGigabitEthernet1/0/26
 switchport private-vlan host-association 10 101

 switchport mode trunk
!
interface TenGigabitEthernet1/0/27
 switchport mode trunk
 rep segment 1
 macsec network-link
 mka policy MKA-POLICY
 mka pre-shared-key key-chain MAC-SEC
!
interface TenGigabitEthernet1/0/28
 switchport mode trunk
 rep segment 1
 macsec network-link
!
interface AppGigabitEthernet1/0/1
 switchport voice vlan dot1p
!
interface Vlan1
 no ip address
!
interface Vlan111
 ip address 10.111.1.4 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ssh bulk-mode 131072
!
snmp-server community private RW
snmp-server community public RO
!
!
!
control-plane
 service-policy input system-cpp-policy
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
ntp server 10.10.1.10
!
ptp clock transparent domain 0  profile default
!
!
!
!
!
!
!
!
!
end
```

FSN Switch:

```
hostname WF-SCADA-FSN-Switch
!
!
no logging console
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
!
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization network MACSEC-UPLINK local
aaa authorization credential-download MACSEC-UPLINK local
!
!
aaa attribute list MUST-SECURE
 attribute type linksec-policy must-secure
!
aaa session-id common
clock timezone UTC 5 30
rep ztp
rep autodisc
iedt refresh-interval 21600
eap profile EAP-PROFILE
 method tls
 pki-trustpoint CA
!
ptp mode e2etransparent
vtp mode transparent
!
!
!
!
!
!
!
!
!
login on-success log
!
!


access-session mac-move deny
!
key chain MAC-SEC macsec
 key 4000000000000000000000000000000000000000000000000000000000000000
  cryptographic-algorithm aes-128-cmac
  key-string CAFECAFECAFECAFE0CAFE0CAFE0CAFE0
  lifetime local 00:00:00 Jan 1 1993 infinite
!
crypto pki trustpoint CA
 enrollment url http://10.20.200.1:80
 serial-number
 fqdn V0SZ.wf.com
 ip-address none
 subject-name CN=V0SZ
 subject-alt-name V0SZ.wf.com
 revocation-check none
 rsakeypair myrsakeys
 hash sha512
!
!
crypto pki certificate chain CA
 certificate 02
  3082052F 30820317 A0030201 02020102 300D0609 2A864886 F70D0101 0D050030
```

```
 0E310C30 0A060355 04031303 49535230 1E170D32 33313232 32303631 3730325A
 170D3234 31323231 30363137 30325A30 3F310D30 0B060355 04031304 5630535A
 312E3012 06035504 05130B46 4F433234 32395630 535A3018 06092A86 4886F70D
 01090216 0B563053 5A2E7766 2E636F6D 30820222 300D0609 2A864886 F70D0101
 01050003 82020F00 3082020A 02820201 009D8A08 D8135238 F0B4617A D655DA6A
 FCE973F9 1E3668D2 610BAFEF 16102218 A8A18EA3 EB19878C 1A53AA0A 5ED7058A
 16557BB6 0C3D5CBE BDD58BAE D1F6F6DF E39C38BB 779F5A6E 891EF289 6CFF9FCF
 36C0712E 8CF5F544 992F39D0 F19F4BD8 51669C1D 1D14E15B 715DA3B7 B57D423A
 3C570A4B EBC364E8 012B1D0E D4EA5D39 E0CFF04D 1CD42A0B B3197CE7 6E4C5E4C
 B409D3B8 2A9D3DAC 7FD67232 BC131D24 19AA1F7D 3E075E31 3939397B D91FF459
 D1A36E04 891B6CA1 538E7BE9 6DEEDB49 79545B07 5081EE3D E92CE7CF 83CF0CE5
 5750C05A 869AC9D8 F1F05DF9 4F6013C1 D2F53288 C415A4D8 5631D452 25CFB343
 86AD3E35 843F1BA0 E4818BEC 495D7667 094EF970 807DE2C2 6FEE5732 C6E4B05A
 048FFD8E 725BF6A8 45262C82 5AE64E9A 30FF46D9 8ED803CB 474FB7E1 69B8B955
 D66B3E08 10F2EF89 6BEEAFA4 BFC28758 49DA4F9C 9AD91CE4 ECBEB354 965EA3B2
 62E9B7E9 7EC90762 98A323C3 DE39CBA7 59C405D0 9A75FBF4 B94A9F2C 61D75DED
 70602EE5 9F82105D D5215B15 6DBF41F9 C283FB86 DED95AC3 BB75AE6C 904ACA6A
 C41A88CB 196CF5FC 9DFCD646 FCC32E1D 07B75229 2852BC4E 73025AF6 E02EF586
 9BD56019 CECB4A0B A05A800B 2C2FE791 0B64B1A6 6C2F73FD 0EB8C29C DBE5FFCB
 6CC1D45E B7A78C44 E1C33387 A1686674 55BE4F37 B20BB755 9555B898 51E3A013
 16A0D1A7 5D85D0DC C5AE8BB5 74D9E488 23020301 0001A367 3065300B 0603551D
 0F040403 0205A030 16060355 1D11040F 300D820B 5630535A 2E77662E 636F6D30
 1F060355 1D230418 30168014 1307525E 86089D19 68D8F1F2 3140CD3D A76ED144
 301D0603 551D0E04 16041450 BB0C8D2A E604593F 3C2C26D6 ADA838D2 2130E930
 0D06092A 864886F7 0D01010D 05000382 02010027 00B7A7C3 C709947F 41CCCF90
 93FA4C65 9935FA1E 76BC3B49 61AC9397 B4E2EF7D 4EC79CA1 02F2A489 252796F8
 446A6995 ADC8B019 01831BAC B8ABBD44 B27AE379 A71E6A69 ABF5C979 3DFB4944
 5AD4B871 3A09D248 8A8CFAE4 AAA87425 59AE7278 B98C6C04 7391EBD9 E1511E31
 F6F64C48 4DDC34AB AF0B39AB 32E3AA7F E0FC6E38 D31CC1F4 978362F1 9F6A7E5B
 21C07169 6DDABB53 6A69F6D8 C53E8DC5 BF95F34B B9295EAB 01110C25 62A4FE3C
 599C46CE CC3B0D3A 23203DC4 11623BC1 A73E4EC7 DED46CD9 A81921BE 3F5F7799
 09F309E5 09EE1A57 81C97750 C1A41D50 AF4E084A C06935AC 657799E9 98130AC1
 BAF3370B 7F8096BC 69C1D63D A1ACF647 20B3FEDE 295622E2 72C699B5 63BAECB9
 074EE053 1D397E99 7E8A5F29 1379E5E7 2999A6A8 1D868950 4132892B 84340907
 2F8A1CDF F71209CD 0FAB8BBB C3CB9746 EA0DF60D 195FD41B A1278797 0DB2DA97
 527FE4B9 19E4F97F 7EB07032 071C6205 916801C1 2BF5E9E8 35349618 B57E4835
 78729483 13B4E424 7457097F 107BA060 D01A0327 D71AAA43 82770C1C 5878A59F
 3EA37FA6 8292309B 930A3024 8AF06842 36559B53 607F0D75 9CE331FF B8E46047
 9D7A18AA FC935DF9 6D317D6C 12F68EAE 201CAF47 92392E71 30D722AB CA267E19
 2C575753 32FCD959 13D8F22A 64E17C10 0106A00B F1E249A0 FEBD1DDC 3C979FA3
 F2528F92 0BCF67A4 04FACD8F C948F69E 2763D2
       quit
certificate ca 01
 308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 0D050030
 0E310C30 0A060355 04031303 49535230 1E170D32 33313232 32303631 3131355A
 170D3236 31323231 30363131 31355A30 0E310C30 0A060355 04031303 49535230
 82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02 82020100
 C93FCBD8 F9044D93 7FD17F8C F7A466CE 86303FB7 961EF078 32735D8B B55E6105
 D0F10B77 DC368C25 31C4018E AB3AABD1 A2A33AA0 2D0F8606 C34DF26F E877546A
 4EEEB656 D4374570 A2923C21 788364DD ABAA7F51 F3E4099E 5EB4CAA5 29E0FE0A
 075D2689 BCC92916 0BF88269 1509DE8C 10537C63 8A03D129 30792797 3EDA3630
 362067CD 072D3285 3A4046D7 0AA2CBDF 23F5A28C 3B5B8551 CB46C313 F23430BC
 60BBF346 F1957919 CF6787D9 0032295F D2796DAF E508294F F49664B9 D7031865
 092C3546 C94E0E19 352E5815 289419BA B2C840FD 0AFCA295 3FA7B91D 4E06CEEF
 5B2E2AD8 7C3CFBED 760D92E9 FE5C4382 85E73DE8 8559B059 A2F9D88C 00F942C6
 3D83213B 5ADBCBD5 B6ED1E44 424F2372 B670FF9F CD87DC38 A4EB3D65 D8DE59F1
 61385435 F20B03C6 D8FF9047 95F14E8E C0F2545E A632418F 9C79141B 6C352661
 B4E228EF AE5764BA 85094A44 3BEEC94E A6779A0D B3239873 40B77AD9 FAA25B81
 7E606F4B 68ACDE7B 5F55AEE4 7084FA8D C6C44B9A 06445DB7 CD32D8C7 EE37393C
 9E3575FD DF3ACCF6 04E8C549 0A76486C E6D5F6C3 CE7C75F1 0486FC0E 16BF7DB6
 0C13A497 D8C1FEFF 34AA67EE 42922309 9D7E876F F3985091 4A9024C2 E62151F1
 B7231AD3 5CA1C579 D79FD49D 30E24DEF DD93905D 8CD1FEB7 56F1111F BE1D1E74
 D6E2F32C C864A2ED 327FA8F5 6A3DB351 A254182B D4ACC070 DEABFE4C 915FBCB9
 02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
 0F0101FF 04040302 0186301F 0603551D 23041830 16801413 07525E86 089D1968
 D8F1F231 40CD3DA7 6ED14430 1D060355 1D0E0416 04141307 525E8608 9D1968D8
 F1F23140 CD3DA76E D144300D 06092A86 4886F70D 01010D05 00038202 0100C5ED
 B8AD3E39 A6B19533 3D029858 35FC67B7 CEF78131 AD879855 B2C70CBD 4E9D7D4A
```

```
  AE86430A E5F6399B 8B95AA07 C2C1ADC8 AD90ECB5 F5B42F69 028EFE47 D551E18B
  237357F6 0525D0E1 4B2CAEE1 9C331260 491421E0 A00AAE96 FE196B18 A43E9D54
  A754FCE5 B8758B34 082A4B0F 8015A7C6 09DD11CE 5CE1A7BE 26447759 FAFC73A6
  07F2270F 1768CA0F 90AEB12A 35AF668A 945721B5 ABBB2641 B31B8D88 CE098C19
  F6BBABE8 91046FC9 E37558EE 433BA7FD 19F16F4E 1C4FA14A 8E06217B 5A3469D0
  0419B1EF 711A2C8E BC25E628 F2738D58 F9547857 22C6CBDF D79C27B0 52E36EC5
  D8F0A1E9 33D4E7C6 D90429BD BAE9545F EAE8F78E D48662B8 2B6FD7B4 8405B1A7
  D0790E88 31482F89 410D7A31 3CC376CA 5375D649 ABF76307 C5A6E5E9 59827A8E
  6C705E59 32985A51 F0B10A18 96252952 80DFBBFA BE7A9605 4B8060A6 98790B17
  02D1143D 7A8121D2 21EFDE23 9C934085 42835E29 CE11C60B 8A1452FE 160BCF0D
  78BFC763 6E909872 7AC5939C B593A376 F0031BE3 B428A015 C07941FF A1EF4C63
  FDAE7A33 DEE55B66 FB52B3AE 01818D63 5FE54C28 95706297 5D448562 3A380D9C
  8B1A9D5F 2ACA1518 CF24DC21 8182A63A 97166FF5 7555D85F 84BCF8F9 CF60DBBA
  FF88F098 6638D179 62F1FA7E 026FA05E A5633F16 4FB6B514 EBF135F5 441CE34C
  A9700577 591F02AF FD3DB02F D8390514 F3A812D7 9E76BF4B 2C2CBDA3 DA
  92
```


```
        quit
!
!
diagnostic bootup level minimal
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 webauth-global-inactive
 inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
 username usr-macsec
 pki-trustpoint CA
!
license boot level network-advantage
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 64978
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
mka policy MKA-POLICY
 key-server priority 150
 sak-rekey interval 65535
!
!
username usr-macsec aaa attribute list MUST-SECURE

crypto engine compliance shield disable
!
!
transceiver type all
 monitoring
!
!
vlan 5
 name Multicast_VLAN
!
vlan 10
 name PrivateVLANvlan
```

```
  private-vlan primary
  private-vlan association 101,102
!
vlan 20
 name IXIA_TrafficTestVLAN
!
!
           vlan 101
  name isolated_VLAN
  private-vlan isolated
!
!
vlan 111
 name Management_VLAN
!
!
lldp timer 5
lldp holdtime 20
lldp run
!
!
class-map match-any MCD
 match dscp cs5  ef  cs6  cs7
class-map match-any LPD
 match dscp default  cs1
class-map match-any MPD
 match dscp cs2  af21  af22  af23
class-map match-any HPD
 match dscp cs3  af31  af32  af33  cs4  af41  af42  af43
 match access-group name QoS_ACL
           !
class-map match-all HPD_Output
 match dscp cs4
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
 event authentication-failure match-all
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
policy-map WF_SCADA_Ingress_Policy
 class MCD
  set ip dscp ef
 class HPD
  set ip dscp cs4
 class MPD
  set ip dscp cs2
 class LPD
  set ip dscp cs1
policy-map WF_SCADA_Egress_Policy
 class MCD
  priority
  queue-limit 48 packets
 class MPD
  bandwidth remaining percent 30
  queue-limit 48 packets
 class LPD
  bandwidth remaining percent 30
  queue-limit 272 packets
 class HPD_Output
  bandwidth remaining percent 40
```

```
  queue-limit 48 packets
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1/1
 switchport mode trunk
           rep segment 100
service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!

!
interface GigabitEthernet1/2
 switchport mode trunk
           rep segment 100
service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!

!
interface GigabitEthernet1/3
 description PNP STARTUP VLAN
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/4
 switchport access vlan 9
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/5
 switchport access vlan 59
 switchport mode access
 ip access-group DAUNU_ACL out
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/6
 description ##ConnectedToWindowsCA##
 switchport mode private-vlan host
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/7
 switchport private-vlan mapping 10 101-102
 switchport mode private-vlan promiscuous
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/8
```

```
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/9
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/10
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface AppGigabitEthernet1/1
!
interface Vlan1
 no ip address
 shutdown
!
!
!
interface Vlan111
 ip address dhcp
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip ssh bulk-mode 131072
!
ip access-list extended QoS_ACL
 10 permit ip 10.1.10.0 0.0.0.255 any
!
snmp-server community private RW
snmp-server community public RO
snmp-server contact Switch
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
ntp server 10.10.1.10
!
!
!
!
!
!
!
!
!
!
!
!
!
           End
```

TSN Switch :

```
hostname WF-SCADA-TSN
!
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
!
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization network MACSEC-UPLINK local
aaa authorization credential-download MACSEC-UPLINK local
!
!
aaa attribute list MUST-SECURE
 attribute type linksec-policy must-secure
!
aaa session-id common
clock timezone UTC 5 30
rep ztp
rep autodisc
iedt refresh-interval 21600
eap profile EAP-PROFILE
 method tls
 pki-trustpoint CA
!
ptp mode e2etransparent
vtp mode transparent
!
!
!
!
!
!
!
!
login on-success log


access-session mac-move deny
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
 hash sha256
!
crypto pki trustpoint TP-self-signed-4060431784
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4060431784
 revocation-check none
 rsakeypair TP-self-signed-4060431784
 hash sha256
!
!
crypto pki trustpoint CA
 enrollment url http://10.20.200.1:80
 serial-number
 fqdn Y1SL
 ip-address none
 subject-name CN=Y1SL
 revocation-check none
 rsakeypair my-4096rsa-key
 hash sha512
!
!
crypto pki certificate chain SLA-TrustPoint
```

```
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain TP-self-signed-4060431784
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34303630 34333137 3834301E 170D3233 31323035 30393535
  33325A17 0D333331 32303430 39353533 325A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 30363034
  33313738 34308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 01009E6A 0139E090 34B3DBCA 7982322A A310D739 085EAA72 9B50CE67
  34987E43 103AB7FA A1E91DA5 11BB805E E6033BB1 3679F080 80801DC5 375D006A
  6C3F9902 05D0D411 14DA5951 2F081138 C7FC27AE 6D835C1B CCD8A611 F0A6FBCE
  4BE56C8F 246A7F25 D50C6663 0D1F1773 5F195F92 24CF8BBA 17120193 576E87A1
  55F00020 3FB35F3C 168F8687 6F71B280 9B1C1ACA CAD08DAE 94B328C3 230FBE52
  9631815E FA56D503 20B294D7 CB7B0E9C 35E0B5A2 B799CCCC 8E0845FA C524C327
  517E5796 93BA0671 5AF1A7D2 E0F35507 DA340CF0 E047C7F6 77A8F096 C7A7378D
  73C6D1DD 0054C002 4224F47F 3A0EDB46 800784E5 0503239B 93E1A87C 61D7B2C6
  CAA1DE79 46E10203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 146F8C76 890A5019 4F6522EE 15F7BBE4 978569E8
  DC301D06 03551D0E 04160414 6F8C7689 0A50194F 6522EE15 F7BBE497 8569E8DC
  300D0609 2A864886 F70D0101 05050003 82010100 19DC4593 92033710 80CEA7A5
  B3173FAB 6A434C91 B44B9D54 3E6D84CA CEA8B9A2 423EB597 9C74EC51 36E0C472
  759A5BBA 055AEB22 0888815A 3202861E 21C61CD5 318C07D0 7422EF86 EC74B4D3
  9EC53168 BFD1AE5B 76376422 39852FA9 993F422A 27C3894B 272251CE CF50BBA6
  3BB1783D 1E440857 BB703128 D38BD9C5 45B0BA5A 557F3A49 DEABB46C 9A16549E
  B7F907FB AE91CBAA 1BF49B7C E32BA7BC 4AB210D6 643BF417 147BDE71 ABA998D6
  0D22A1C6 86398E26 1AB51E19 C076BAB4 68BE1CFE 97A629F7 1029035F 00E80514
  604841B3 6C7EB94C FE913E04 F56A0C9C A0FDD762 72C6EE9E A3C7BF2D 22D5A17E
  5EC534B8 E45FD0A4 BC621619 76F6130F B2D11423
        quit
crypto pki certificate chain Win-CA
crypto pki certificate chain CA
!
diagnostic bootup level minimal
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 webauth-global-inactive
 inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
 username usr-macsec
 pki-trustpoint CA
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88360
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
!
username usr-macsec aaa attribute list MUST-SECURE

crypto engine compliance shield disable
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
vlan 5
 name Multicast_VLAN
!
vlan 10
 name PrivateVLANvlan
  private-vlan primary
  private-vlan association 101,102
!
vlan 20
 name IXIA_TrafficTestVLAN
!
!

           vlan 101
  name isolated_VLAN
  private-vlan isolated
!
!
vlan 111
 name Management_VLAN
!
!
!
lldp timer 5
lldp holdtime 20
lldp run
!
!
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
 event authentication-failure match-all
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 10
```

```
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1/1
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/2
 switchport mode trunk
 rep segment 101
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/3
 switchport mode trunk
 rep segment 101
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/4
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/5
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/6
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/7
 description Connected to WF-SCADA-UCS 10_64_66_115 vmnic7
 switchport private-vlan host-association 10 101
 switchport mode private-vlan host
 speed 1000
 duplex full
 spanning-tree portfast
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/8
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/9
 service-policy input WF_SCADA_Ingress_Policy
 service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/10
 service-policy input WF_SCADA_Ingress_Policy
```

```
 service-policy output WF_SCADA_Egress_Policy
           !
interface AppGigabitEthernet1/1
!
interface Vlan1
 no ip address
!
!
interface Vlan111
 ip address dhcp
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip ssh bulk-mode 131072
           !
ip access-list extended QoS_ACL
 10 permit ip 10.1.10.0 0.0.0.255 any
!
!
!
snmp-server community private RW
snmp-server community public RO
snmp-server contact Switch
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
ntp server 10.10.1.10
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
!
!
!
!
!
!
!
!
!
!
!
!
!
end
```

CA server sample configuration for auto-enrollment:

```
crypto pki server CA
no database archive
issuer-name CN=ISR
grant auto
hash sha512
!

crypto pki trustpoint CA
 revocation-check crl
 rsakeypair CArsaKeys
!
```

Acronyms and Initialisms

The following table summarizes the acronyms and initialisms that apply to a wind farm solution.

Term	Definition
4G LTE	Fourth generation long-term evolution
AAA	Authentication, authorization, and accounting
ACL	Access control list
AD	Active Directory
ADM	Axis device manager
AIS	Automatic identification system
AMP	Advanced malware protection
AP	Access point
ARP	Address resolution protocol
AVC	Application visibility and control
BGP	Border gateway protocol
BS	(Turbine) Base switch
BW	Bandwidth
CA	Certificate authority
CBWFQ	Class-based weighted fair queuing
CC	Control venter
CCTV	Closed circuit television
CDN	Cisco Developer Network
CE	Carrier Ethernet
Cisco Catalyst Center	Cisco Digital Network Architecture Center
CLI	Command line interface
CoS	Class of service
CTS	Cisco Trustsec
URWB	Cisco Ultra Reliable Wireless Backhaul
CV	(Cisco) Cyber Vision
CVC	Cisco Cyber Vision Center
CVD	Cisco Validated Design
DAD	Dual active detection
DC	Data center

DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DNS	Domain names system
DODAG	Destination oriented directed acrylic graph
DoS	Denial of service
DSCP	Differentiated services code point
DSRC	Dedicated short-range communications
EB	Enhanced beacon; 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
EP	Endpoint
ETS	European teletoll services
ETSI	European Telecommunications Standards Institute
EVA	Emergency vehicle alert
FAN	Farm area network
FAR	Field area router
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
FM	FluidMesh
FMC	Firepower Management Center
FND	(Cisco) Field Network Director
FNF	Flexible NetFlow
FP	Firepower

FW	Firewall
HA	High availability
HER	Headend router
HMI	Human machine interface
HQ	Headquarter
HQoS	Hierarchical quality of service
HSRP	Hot standby touter protocol
HTDB	Host Tracking Database
I/O	Input and output
IA	Industrial automation
IB	Internal border
ICA	Intersection collision avoidance
IE	(Cisco) Industrial Ethernet
IEC	International Electrotechnical Commission
IED	Intelligent end device
IKE	Internet key exchange
IMA	Intersection movement assist
IOT	Internet of things
IP	Internet protocol
IPAM	IP address management
IPsec	Internet protocol security
IR	Cisco Industrial Router
iSCSI	Internet small computer systems interface
ISE	(Cisco) Identity Services Engine
IT	Information technology
L2TP	Layer 2 tunneling protocol
L3VPN	Layer 3 virtual private network
LAN	Local area network
LER	Label edge router
LG	Cimcon LightingGale
LLG	Least loaded gateway
LoRa	Long range
LoRaWAN	Long range WAN

LSP	Label switched Path
LSR	Label switched router
MAC	Media access control
MAN	Metropolitan area network
ME	Mesh end
MIC	Message integrity code
MMS	Manufacturing message specification
MNT	Monitoring node
MP	Mesh point
MPLS	Multi-protocol label switching
MQC	Modular QoS CLI
MRP	Media redundancy protocol
MTU	Maximum transmission unit
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
NMS	Network management system
NOC	Network operations center
NS	(Turbine) nacelle switch
NSF/SSO	Non-stop forwarding with stateful switchover
NTP	Network time protocol
OAM	Operations, administration, and management
OBU	On-board unit
OEM	Original equipment manufacturer
OFTO	Offshore transmission owner
ONSS	Onshore substation
OPC UA	Open platform communications unified architecture
OSPF	Open shortest path first
OSS	Offshore substation
OT	Operational technology

OTAA	Over the air activation
PAgP	Port aggregated protocol
PAN	Policy administration node; personal area network
PCA	Pedestrian crossing assist
PEN	Policy extended node
PEP	Policy enforcement point
PHB	Per hop behavior
PIM-ASM	Protocol independent multicast - any source multicast
PKI	Public key infrastructure
PLC	Power line communication
PnP	Plug and Play
PoE	Power over Ethernet
PoP	Point of presence
PQ	Priority queuing
PQ	Priority Queuing
PRP	Parallel redundancy protocol
PSM	Personal safety message
PSN	Policy services node
PVD	Probe vehicle data
PVM	Probe vehicle management
PXG	Platform exchange grid node
pxGrid	Platform exchange grid
QoS	Quality of service
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

RTU	Remote terminal unit
SA	Substation automation
SCADA	Supervisory control and data acquisition
SCMS	Security credential management system
SD-Access	Software-defined Access
SD-WAN	Software defined wide area network
SFC	Secure network analytics flow collector
SFC	Secure Network Analytics Flow Collector
SGACL	Security group-based access control list
SGT	Security group tag
SLC	Street light controller
SOV	Service operations vessel
SPAT	Signal phase and timing message
SRM	Signal request message
SSID	Service set identifier
SSM	Software security module
STP	Spanning tree protocol
SVI	Switched virtual interface
SVL	StackWise virtual link
SXP	SGT exchange protocol
TAN	Turbine area network
TBN	Turbine base network
TC	Transit control
TCP	Transmission control protocol
TFTP	Trivial file transfer protocol
TIM	Traveler information message
TLS	Transport layer security
TLV	Type length value
TMC	Traffic monitoring center
TPE	ThingPark Enterprise
UCS	Cisco Unified Computing System
UDP	User datagram protocol
UHF	Ultra high frequency

UPS	Uninterrupted power supply
V2I	Vehicle to infrastructure
V2P	Vehicle to pedestrian
V2V	Vehicle to vehicle
V2X	Vehicle to infrastructure
VHF	Very high frequency
VLAN	Virtual local area network
VN	Virtual network
VNI	VXLAN network identifier
VoD	Video on demand
VoIP	Voice over internet protocol
VPN	Virtual private network
VRF	Virtual routing and forwarding
VSM	Video Surveillance Manager
VXLAN	Virtual extensible LAN
WAN	Wide area network
WAVE	Wireless access in vehicular networking
WF	Wind farm
Wi-Fi	Wireless fidelity
WLAN	Wireless local area network
WLC	Wireless LAN controller
WPAN	Wireless personal area network
WRED	Weighted random early detect
WSMP	WAVE short message protocol
WTG	Wind turbine generator
ZTD	Zero touch deployment
ZTP	Zero touch provisioning