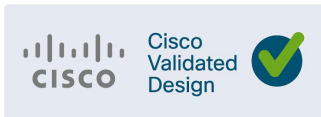




Cisco Solution for Renewable Energy: Offshore Wind Farm 1.0

Implementation Guide

June 2023



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

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

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

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

©2023 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Contents

Preface	3
Document Objective and Scope	3
Audience	3
Chapter 1: Introduction	4
Implementation Flow	4
Chapter 2: Solution Network Topology and Addressing	6
Solution Validation Topologies	6
Network VRFs and VLANs	8
IP Addressing	9
Solution Components	10
Chapter 3: Offshore Substation Network Implementation	12
Offshore Substation Core Network Implementation	12
Bringing Up Catalyst 9500 StackWise Virtual	12
Configuring FAN Ring Aggregation Switch Stack	14
Catalyst 9300 Switch Stack for FAN Aggregation	14
Configuring OSS Infrastructure Network Access	15
OSS Network DMZ with Firewall	16
Cisco Firepower Next Generation Firewall (NGFW) Implementation	16
Firepower Installation and High Availability Configuration	16
Configuring Firepower for Wind Farm Solution Use Cases	17
Chapter 4: Farm Area Network Implementation	22
Configuring a Farm Area Network Ring	22
FAN Ring Topology and REP Ring Configuration	22
Configuring a Turbine Area Network	23
Configuring Turbine Area Network without High Availability	23
Configuring TAN with High Availability and REP Subtended Ring	23
Chapter 5: Implementing OSS Infrastructure Applications and Services	25
Cisco Cyber Vision Center Local Installation and Configuration	25
Cisco Cyber Vision Center Installation	25
Configuring Cyber Vision Center Data Synchronization	25
Cisco Stealthwatch Flow Collector Installation and Configuration	25
SCADA OPC-UA Server Installation and Configuration	26
OPC-UA message types and Flow	27
Cisco Cyber Vision Sensor installation on a 9300 Switch to Detect OPC-UA Traffic	29
Step 1: Mount the USB SSD on a 9300 Switch and Install the Cyber Vision Sensor Application on the Mounted Drive	29
Step 2: Configure the Cyber Vision Sensor Application on the 9300 Switch	30
Step 3: Install the Cyber Vision Sensor on the 9300 Switch from the Cyber Vision Center	31
Step 4: Edit the yaml File on the 9300 Switch and Add OPC-UA Ports	32
Step 5: Verify the OPC-UA Flow in Cyber Vision Center	33
Chapter 6: Implementing the Onshore Substation Network	35
Onshore Substation (ONSS) Core Network Implementation	35
Catalyst 9500 StackWise Virtual	35
Configuring ONSS Infrastructure Network Access	36
OSS Network DMZ with Firewall	36

Cisco Next Generation Firewall (NGFW) Implementation.....	36
Turbine Vendor OPC-UA client.....	36
Chapter 7: Implementing Wireless Access Networks.....	37
Offshore Wind Farm Wi-Fi Implementation.....	38
Configuring C9800 WLC High Availability from Cisco DNA Center	38
Configuring Wi-Fi APs using Cisco DNA Center	41
Upgrading C9800 WLC and AP Images Using Cisco DNA Center	44
Wi-Fi Guest User Access.....	49
Operating the Wireless Network	51
Cisco DNA Center Wireless Assurance	51
Defective AP Replacement (RMA) using Cisco DNA Center	53
Troubleshooting Wireless Client Authentication	54
Offshore Wind Farm CURWB Implementation for SOV to OSS Connectivity	55
OSS Wired Network.....	56
CURWB Network Configuration	59
Service Operations Vessel Network	62
SOV Wired Network	63
CURWB Configuration	66
Chapter 8: Implementing WAN Backhaul and Control Center.....	71
Implementing WAN Backhaul	71
Configuring WAN Substation using Cisco SD-WAN	72
Deploying WAN Edge Routers (IR8340) using Cisco SD-WAN	72
Configuring WAN Edge Routing for High Availability	72
Implementing Network Control Center and Application Services.....	73
Configuring a DHCP Server	73
Domain Name Server	73
Cisco DNA Center Installation and Configuration.....	73
Cisco ISE Installation and Configuration and Integration with Cisco DNA Center	74
ISE Installation and Initial Configuration	74
Cisco Firepower Management Center installation and Configuration	74
Cisco Cyber Vision Center Global Center.....	74
Cisco Stealthwatch Management Console installation and Configuration	75
Chapter 9: Implementing Network Management and Automation	76
Preparing Cisco DNA Center and Switches for Device Onboarding.....	76
FAN and TAN Ring Devices Onboarding (Day-0 Provisioning).....	78
Create Day 0 Templates for 3400 Onboarding.....	79
Onboard the FAN Ring	79
Configure the FAN REP Ring Using the REP Workflow	82
Onboard TAN Switches	82
TAN REP Ring Configuration.....	83
Day N Configurations using Cisco DNA Center Templates	86
Adding a New Switch to a FAN REP Ring	86
Network Assurance	87
Chapter 10 Implementing Network Security and QoS	88
Implementing Network Security	88
Configuring Firepower Zones and Policies for OPC-UA	88
Configuring Cisco Cyber Vision Sensors on TAN and FAN Ring	88
OT Flow detection using Cyber Vision Sensors.....	91
Configuring Stealthwatch (SNA) NetFlow.....	92
Integrating Stealthwatch with Identity Services Engine.....	93
Implementing QoS	93
OSS QoS Configuration for OSS C9300 and C9500 Switches	93
OSS QoS Configuration for the OSS C3400 Switches.....	94

Implementing Multicast Traffic Support in an Offshore Substation	94
Appendix A: Configuration Examples	97
WAN PE Configuration	97
WAN HER Configuration.....	104
FAN Ring Switch Configuration (Non Edge Switch that is Not a Part of TAN Rings)	131
QoS on IE-3400.....	135
QoS on FAN Aggregation and on the OSS and ONSS (C-9300/C-9500)	136
Appendix B: Cisco DNA Center Day N Templates.....	138
Acronyms and Initialisms.....	139



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 (CURWB) 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 DNA Center), Cisco C9800 WLC and APs, and CURWB.

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 Renewable 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 1.0 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.

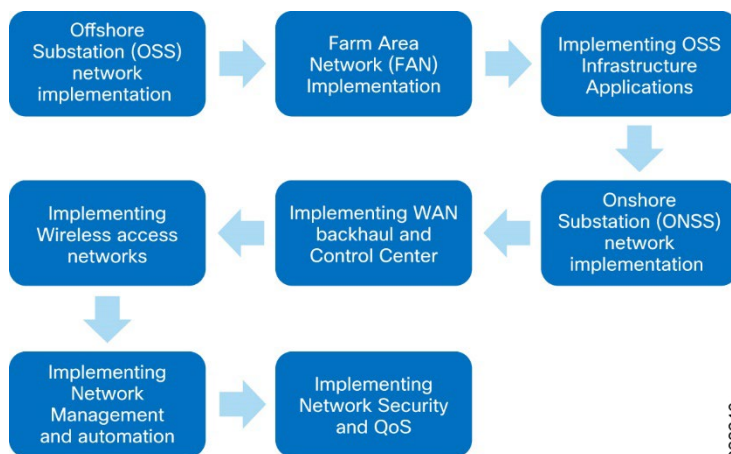
The offshore wind farm solution architecture includes ruggedized access network devices, such as Cisco Industrial Ethernet (IE) switches and Cisco Industrial Routers (IR). It also includes Cisco Catalyst 9300 and 9500 Series switches, Cisco Next Generation Firewalls (NGFW) and the Cisco Unified Computing Systems (UCS) servers, C9800 Wireless LAN Controllers (WLCs), CURWB, 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 1.0 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.

Introduction

- 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 DNA Center, Cisco ISE, Cyber Vision Global Center, SNA Manager, and so on.
- Deployment of wireless network components, such as WLC, access points, CURWB radios, and so on for wind farm wireless network access.
- Implementation of network management services using Cisco DNA Center, and automated provisioning of wind farm network components using Cisco DNA 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 CURWB network that provides wireless connectivity for SOVs back to the OSS. See Figure 2-2.

Figure 2-1: Wind Farm 1.0 Wired Network Topology

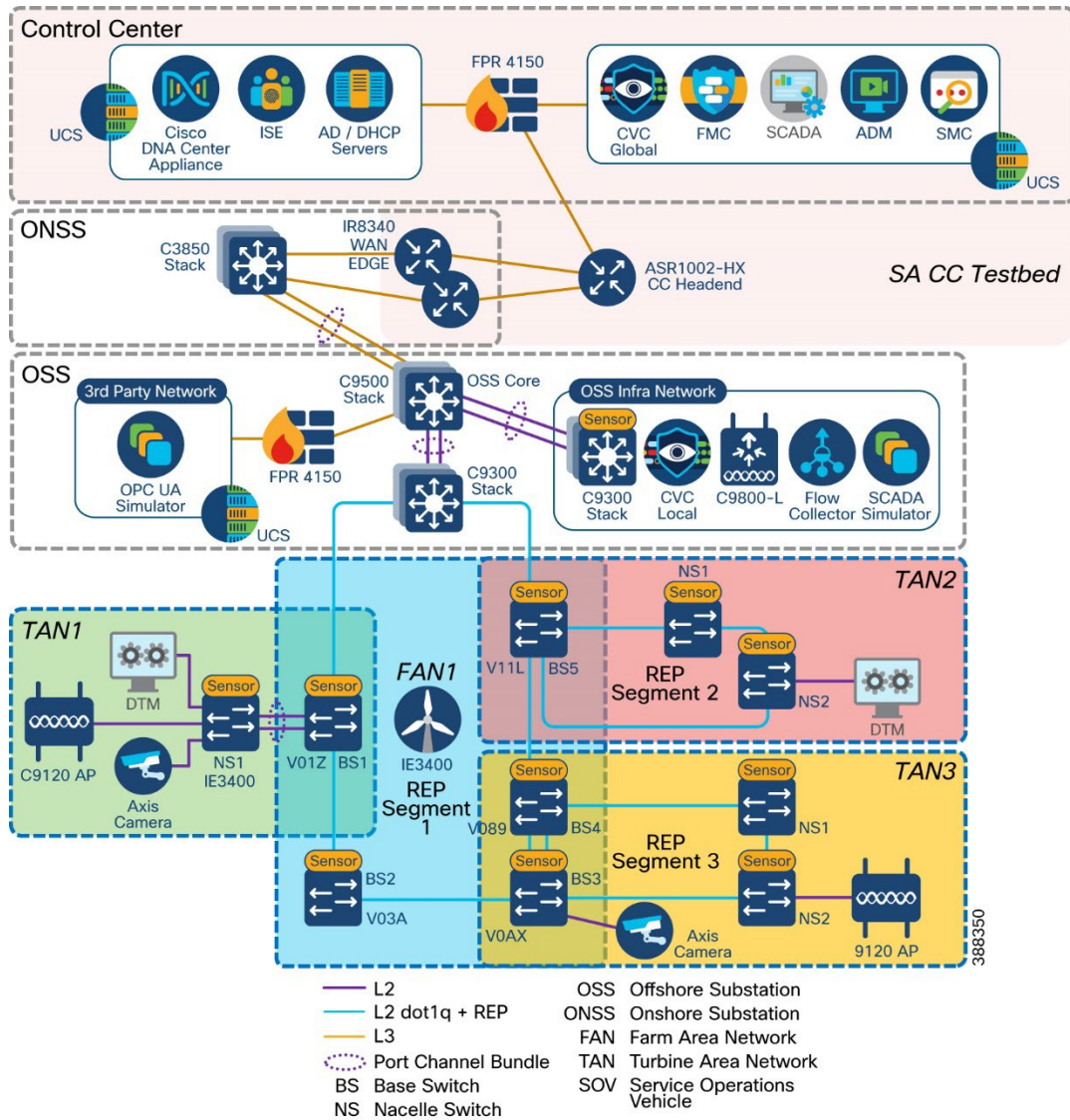
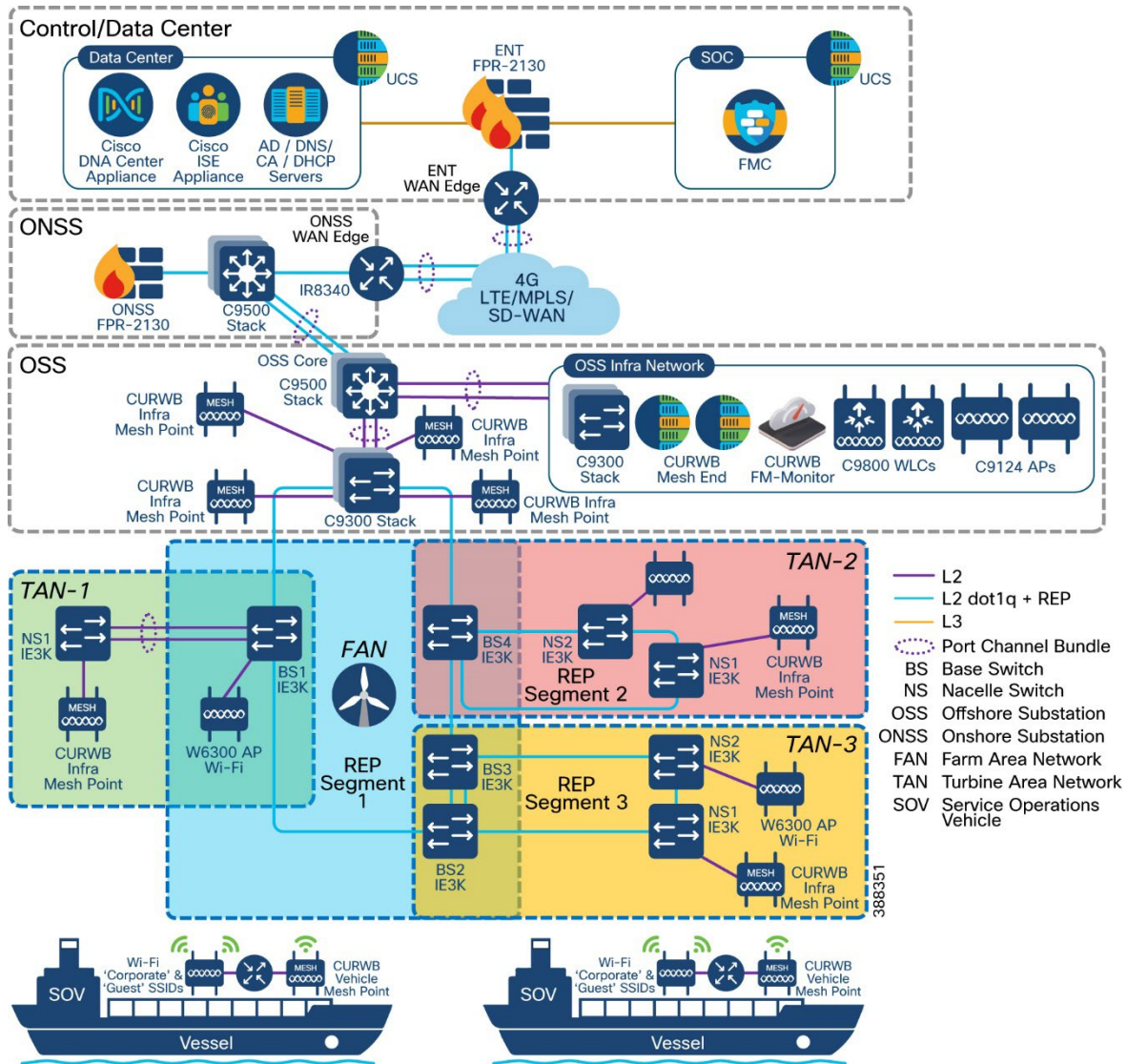


Figure 2-2: Wind Farm 1.0 Wireless Network Topology



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)	<ul style="list-style-type: none"> ▪ 100 ▪ 101 ▪ 102 ▪ 103 ▪ 104 ▪ 105 ▪ 106 	<ul style="list-style-type: none"> ▪ 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 ▪ CURWB management VLAN
VnV_VRF (voice and video VRF)	<ul style="list-style-type: none"> ▪ 500 ▪ 600 	<ul style="list-style-type: none"> ▪ VLANs for CCTV cameras in FAN and TAN ▪ IP telephony devices voice VLAN
Wi-Fi access	<ul style="list-style-type: none"> ▪ 900 ▪ 901 	<ul style="list-style-type: none"> ▪ Employee and contractor Wi-Fi access ▪ Guest Wi-Fi access
CURWB	<ul style="list-style-type: none"> ▪ 1000 	<ul style="list-style-type: none"> ▪ CURWB traffic
OT_VRF (SCADA and other OT traffic)	<ul style="list-style-type: none"> ▪ 700 	<ul style="list-style-type: none"> ▪ SCADA OT traffic VLAN in TAN and turbine base network (TBN) Example: turbine controller VLAN, SCADA clients
Global routing table (GRT)	<ul style="list-style-type: none"> ▪ 800 ▪ 801 	<ul style="list-style-type: none"> ▪ OSS local VLAN in OSS network only (not to be routed) ▪ ONSS local VLAN in ONSS network only (not to be routed)

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	CURWB 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
CURWB access	1000	172.18.100.0/24	172.18.100.1	VLAN for CURWB 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 DNA 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
CURWB FM3500 and FM4500	CURWB mesh point	9.4
CURWB FM1000 Gateway	CURWB mesh gateway	1.6.0
CURWB FM-Monitor VM	CURWB 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

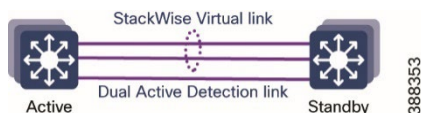
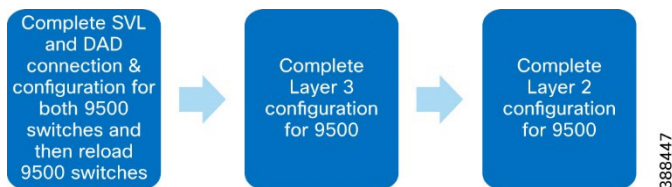


Figure 3-2 shows the workflow for the initial bring-up of the Catalyst 9500 Series switches.

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:

Offshore Substation Network Implementation

```
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
interface Loopback0
 ip address 192.168.5.2 255.255.255.255
 !
vlan 101
 name OSS_NET_MGMT
 !
interface Vlan101
 vrf forwarding Management_VRF
 ip address 10.10.101.1 255.255.255.0
 ip ospf network point-to-point
 !
vrf definition Management_VRF
 rd 100:1
 !
 address-family ipv4
  route-target export 100:1
  route-target import 100:1
 exit-address-family
 !
```

- b. Configure OSPF routing for control center reachability:

```
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
 !
```


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-channell1
 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
```

Offshore Substation Network Implementation

```

description ##ConnectionTo9500##
channel-group 1 mode desirable
!
interface Port-channell
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 1.0 Design Guide](#). 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

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration FMC Access

Name: OPC_Client_Int

Enabled
 Management Only

Description: Going to OPC Client

Mode: None

Security Zone: inside_zone

Interface ID: Ethernet1/3

MTU: 1500
(64 - 9198)

Propagate Security Group Tag:

Cancel OK

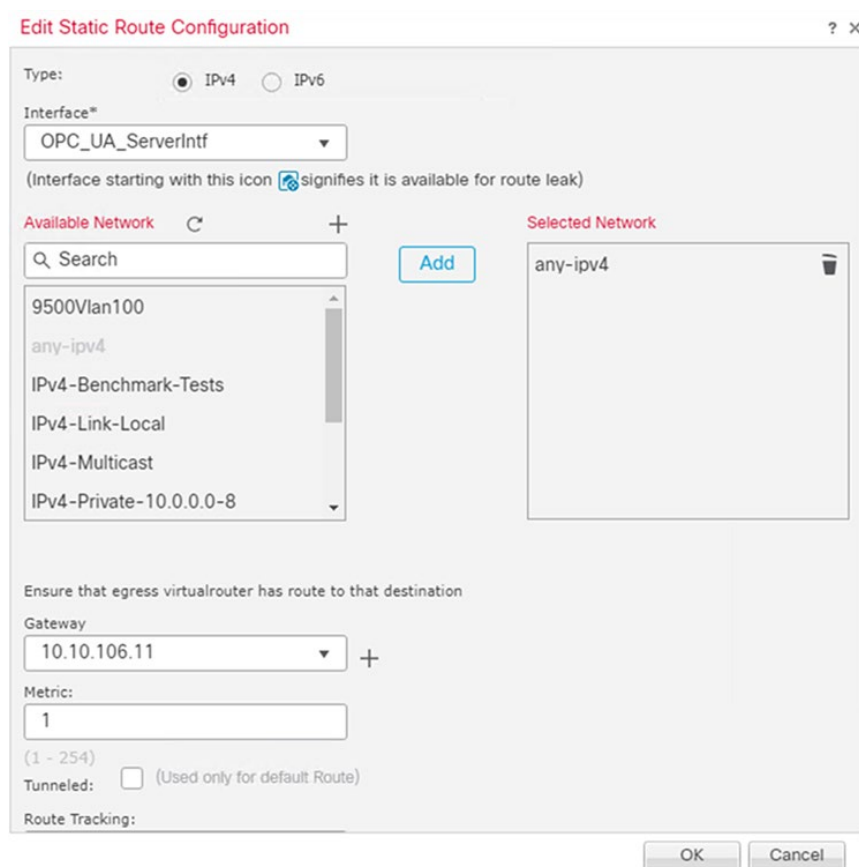
Repeat Steps 2a and 2b as needed to bring up the other Firepower interfaces and assign IP addresses and names to them.

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

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
+ Add Route						
▼ 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*:

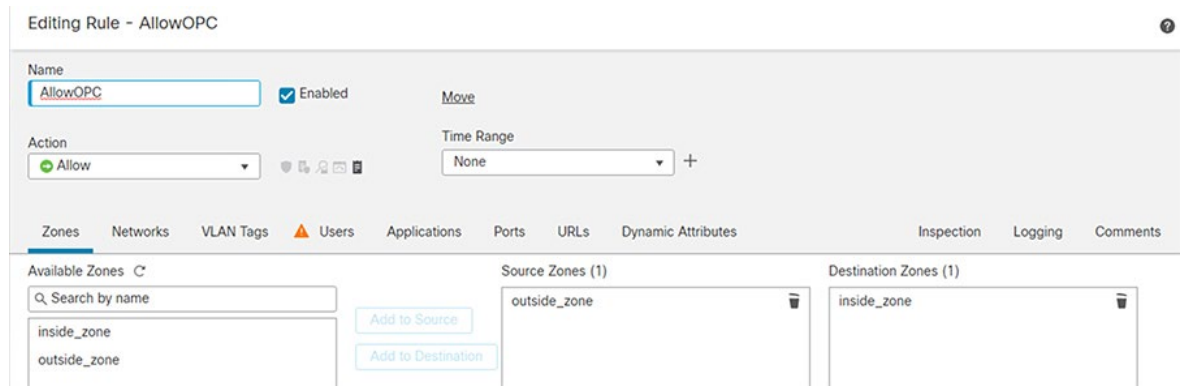
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/static_and_default_routes_for_firepower_threat_defense.html

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

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

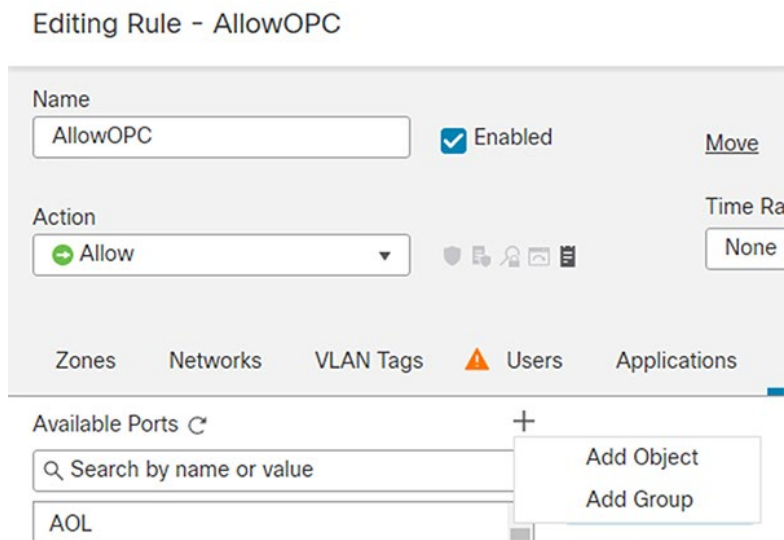
 - a. Choose **Policies > Access Control > New Policy** from the Main menu.
 - b. Click **Add Rule** and configure the policy. See Figure 3-9 for an example.

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

#	Name	Source Zones	Dest Zones	Source Networ...	Dest Networ...	VLAN Tags	Users	Appl...	Source Ports	Dest Ports	URLs	Source Dynamic Attribu...	Destin... Dynamic Attribu...	Action
1	AllowOPC	outside_zon	inside_zonx	Any	Any	Any	Any	Any	Any	OPC62620 OPCport49 OPCPort53 OPCport62 OPCPorts4	Any	Any	Any	Allow

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 DNA Center REP provisioning workflow, which simplifies the configuration and management of devices (see [Onboard TAN Switches](#)).

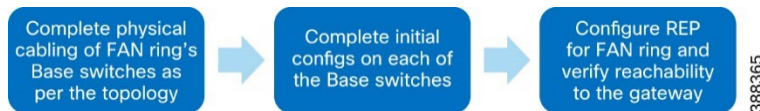
This chapter includes the following topics:

- [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 **show 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 edge2 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
```

Farm Area Network Implementation

```
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 recommend 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 1.0 Design Guide* 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 1.0 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 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.

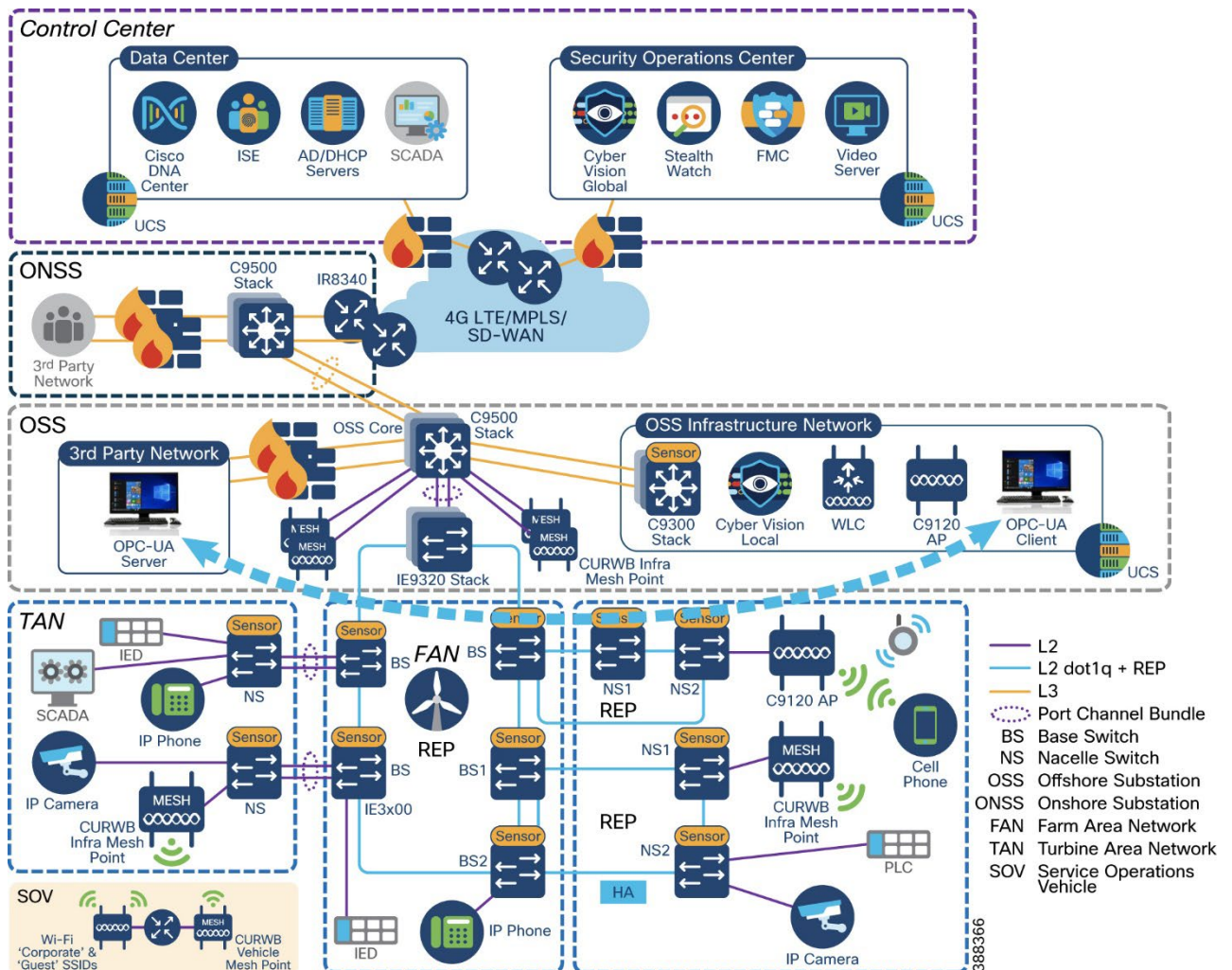
Note: Make sure to activate Cisco Smart Software Licensing for the SNA appliances (SMC and SFC) after the installation and configuration. For information about SNA licensing, see *Cisco Secure Network Analytics Smart Software Licensing Guide 7.4.2*:

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.

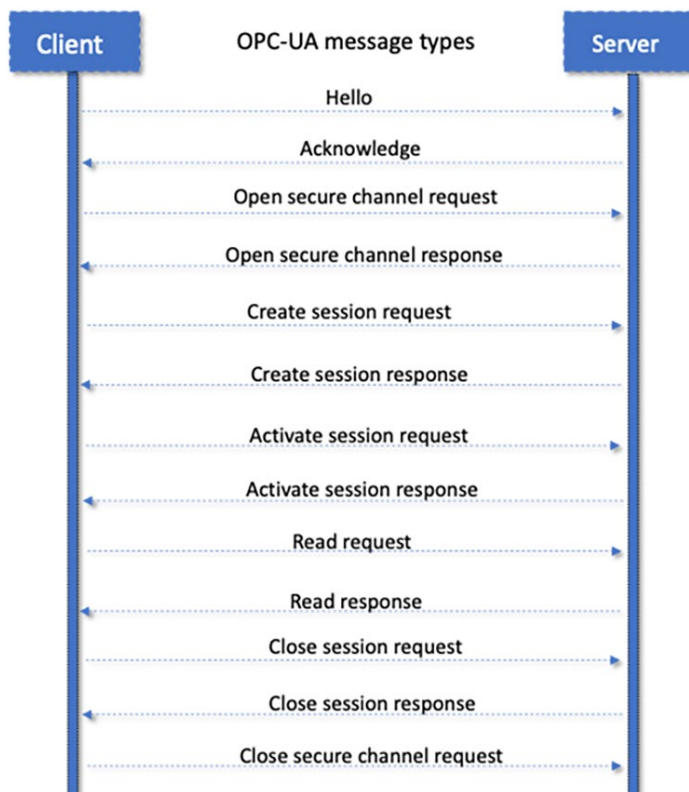
Figure 5-2: OPC-UA Wireshark Capture

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

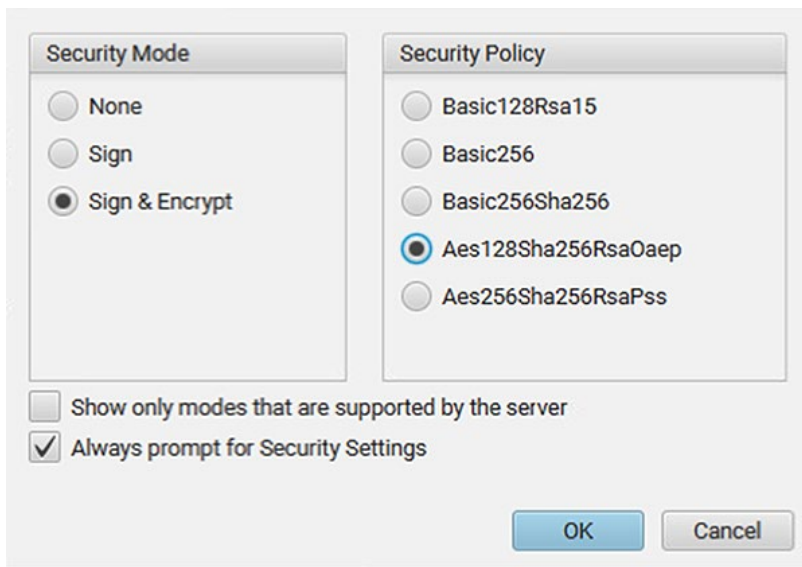


Figure 5-5 shows the OPC-UA client application fetching parameters from an OPC-UA server application over TCP.

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

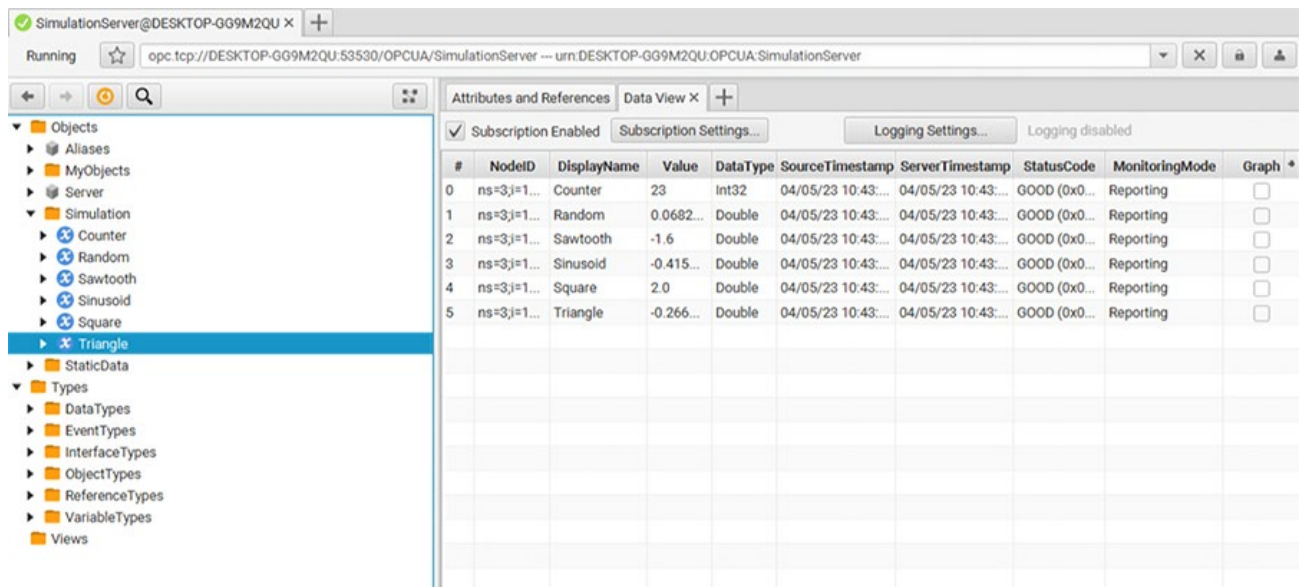


Figure 5-6 shows the Prosys OPC-UA server application provisioned to establish a connection to a server over TCP or HTTP.

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




Server Status:	✓ Running
PubSub Status:	✓ Running
Connection Address (UA TCP):	opc.tcp://DESKTOP-GG9M2QU:53530/OPCUA/SimulationServer 
Connection Address (UA HTTPS):	opc.https://DESKTOP-GG9M2QU:53443/OPCUA/SimulationServer 
PubSub Connection Address:	opc.udp://224.0.5.1:4840 
Current Server Time:	2023-04-05 10:47:29+0530
Server Starting Time:	2023-04-05 10:38:44+0530
Edition:	Free

Figure Shows

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

- 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
- 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

Get Cisco device configuration

The current configuration of your Cisco device enables you to:

- Reconfigure the Cyber Vision IOx sensor app on this device;
- Reconfigure your Cisco device for Cyber Vision (i.e modify the IP address);
- Deploy the Cyber Vision IOx sensor app on a new device using this configuration.

Device IP:	Device port:
10.10.100.4	443
Capture IP address:	Capture prefix length:
169.254.1.2	30
Capture VLAN number:	Collection IP address:
2508	10.10.101.5
Collection prefix length:	Collection VLAN number:
24	101
Collection gateway:	Use global credentials:
10.10.101.1	No
Disk size:	
Use up to 15GB	

- 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

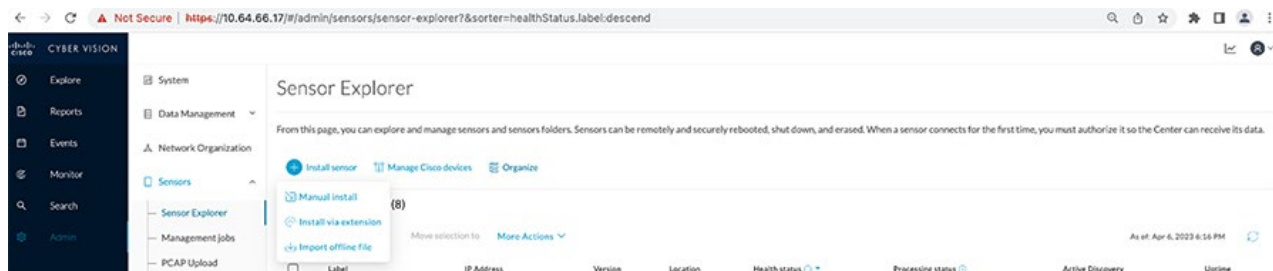
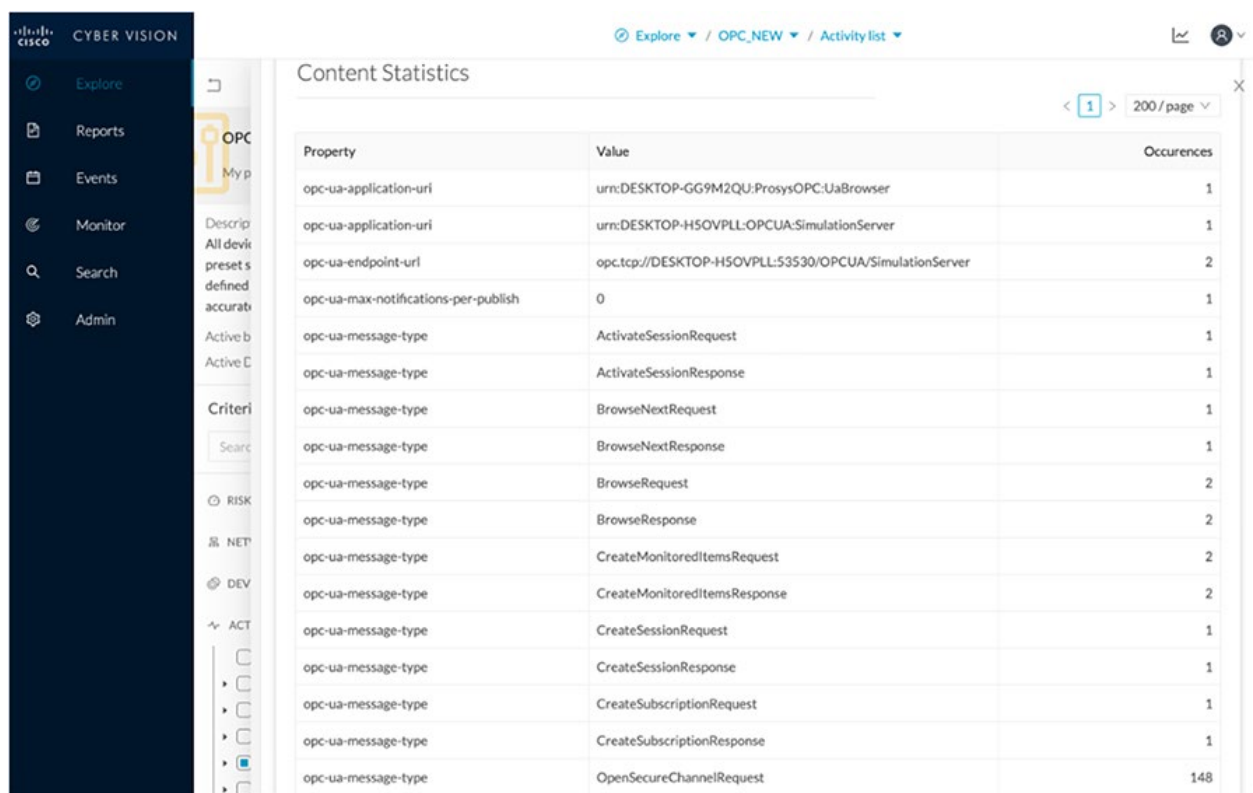


Figure 11 shows the status of the sensor deployment on the CVC Dashboard after completing the installation.

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

OPC-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:
```

```

opcu:
  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.

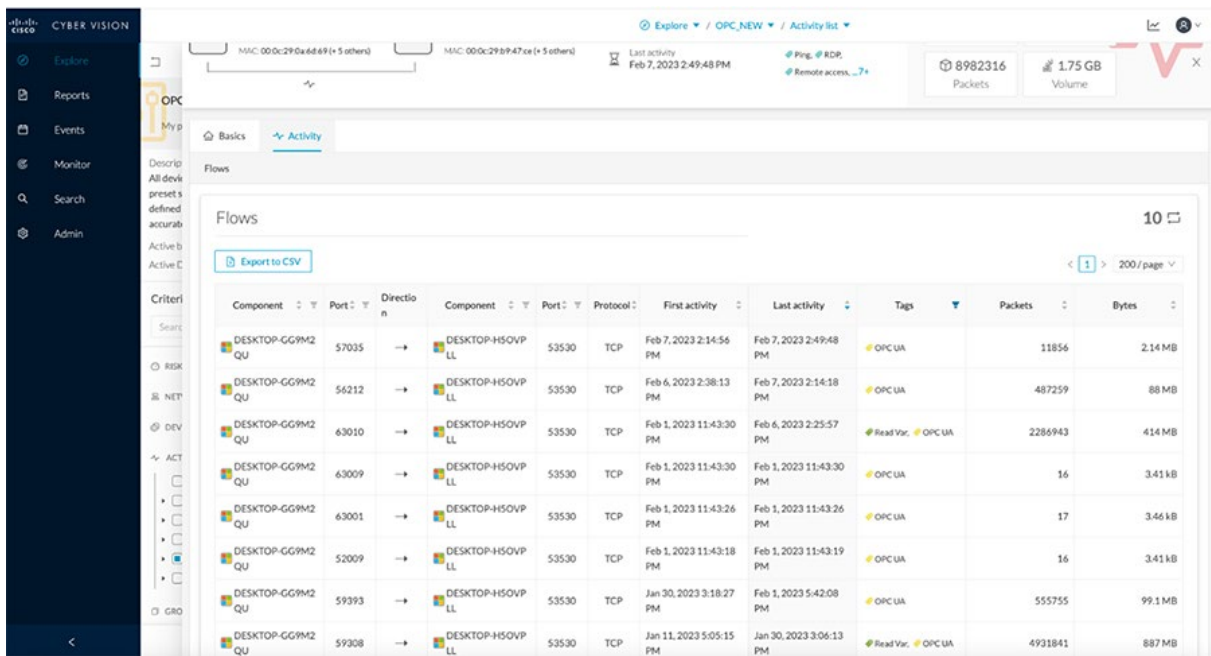
Figure 5-12: OPC-UA Frame Types in CVC Dashboard

The screenshot shows the 'Content Statistics' section of the Cyber Vision Center dashboard. A table lists various OPC-UA message types and their corresponding values and occurrence counts. The table has three columns: Property, Value, and Occurrences. The 'Occurrences' column is sorted in descending order.

Property	Value	Occurrences
opc-ua-application-uri	urn:DESKTOP-GG9M2QU:ProsysOPC:UaBrowser	1
opc-ua-application-uri	urn:DESKTOP-HSOVPLL:OPCUA:SimulationServer	1
opc-ua-endpoint-url	opc.tcp://DESKTOP-HSOVPLL:53530/OPCUA/SimulationServer	2
opc-ua-max-notifications-per-publis	0	1
opc-ua-message-type	ActivateSessionRequest	1
opc-ua-message-type	ActivateSessionResponse	1
opc-ua-message-type	BrowseNextRequest	1
opc-ua-message-type	BrowseNextResponse	1
opc-ua-message-type	BrowseRequest	2
opc-ua-message-type	BrowseResponse	2
opc-ua-message-type	CreateMonitoredItemsRequest	2
opc-ua-message-type	CreateMonitoredItemsResponse	2
opc-ua-message-type	CreateSessionRequest	1
opc-ua-message-type	CreateSessionResponse	1
opc-ua-message-type	CreateSubscriptionRequest	1
opc-ua-message-type	CreateSubscriptionResponse	1
opc-ua-message-type	OpenSecureChannelRequest	148

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 configuring 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:

```
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 ospf 101 metric 1 1 1 1 1
  network 10.10.101.0 0.0.0.255
  network 10.201.201.0 0.0.0.255
 autonomous-system 900
 exit-address-family
```

In addition, update the OSPF configuration on the 9500 switch in the ONSS as follows:

```
router ospf 101 vrf Management_VRF
 router-id 2.2.2.2
 redistribute connected
 redistribute eigrp 900
 network 10.10.101.0 0.0.0.255 area 0.0.0.0
 network 10.201.201.0 0.0.0.255 area 0.0.0.0
```

Here is an example of a completed routing 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 ospf 101 metric 1 1 1 1 1
  network 10.10.101.0 0.0.0.255
  network 10.201.201.0 0.0.0.255
```

Implementing the Onshore Substation Network

```
    autonomous-system 900
    exit-address-family
!
router ospf 101 vrf Management_VRF
  router-id 2.2.2.2
  redistribute connected
  redistribute eigrp 900
  network 10.10.101.0 0.0.0.255 area 0.0.0.0
  network 10.201.201.0 0.0.0.255 area 0.0.0.0
```

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.

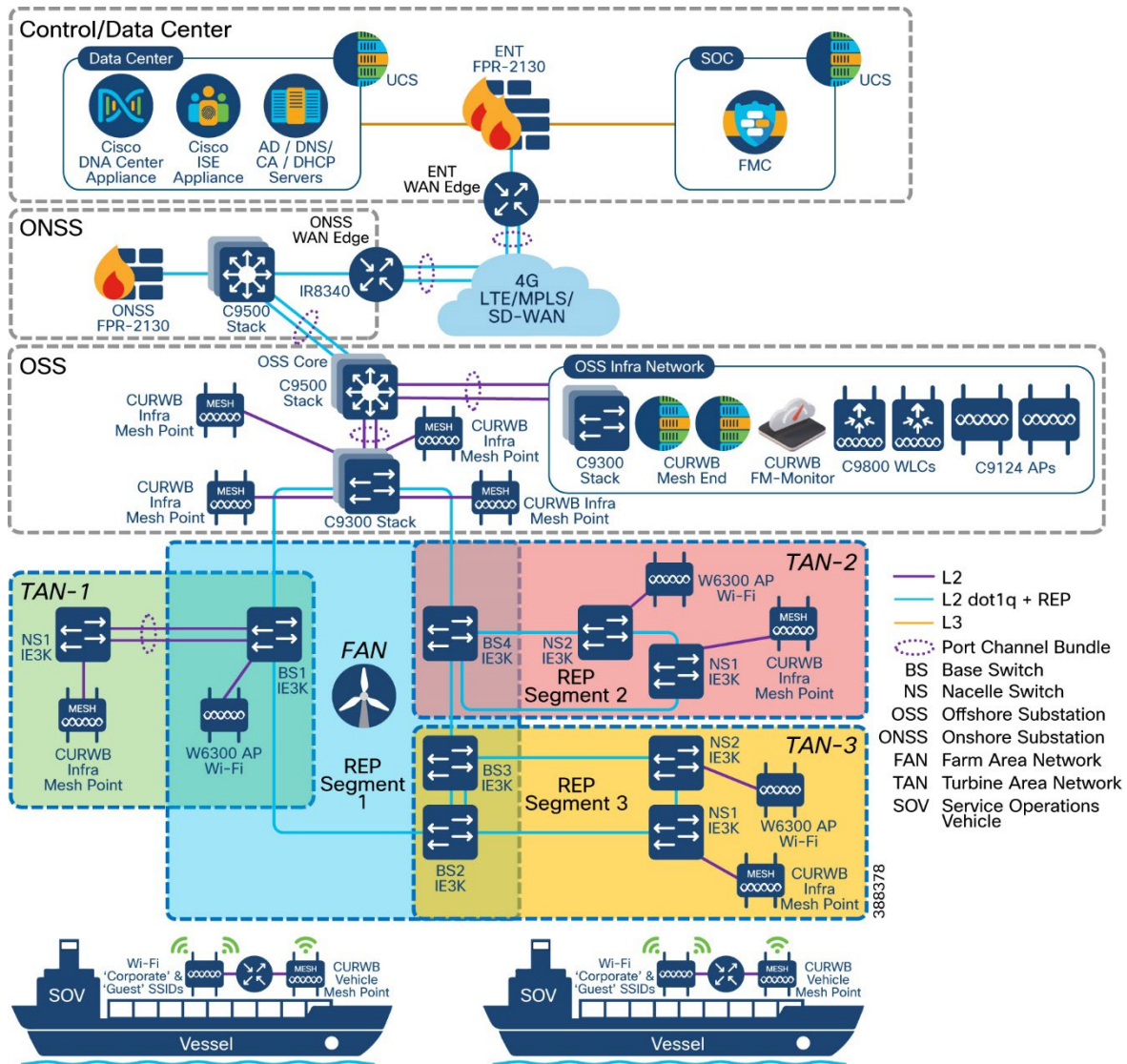
Chapter 7: Implementing Wireless Access Networks

This chapter includes the following topics:

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

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

Figure 7-1: Offshore Wind Farm Wireless Architecture



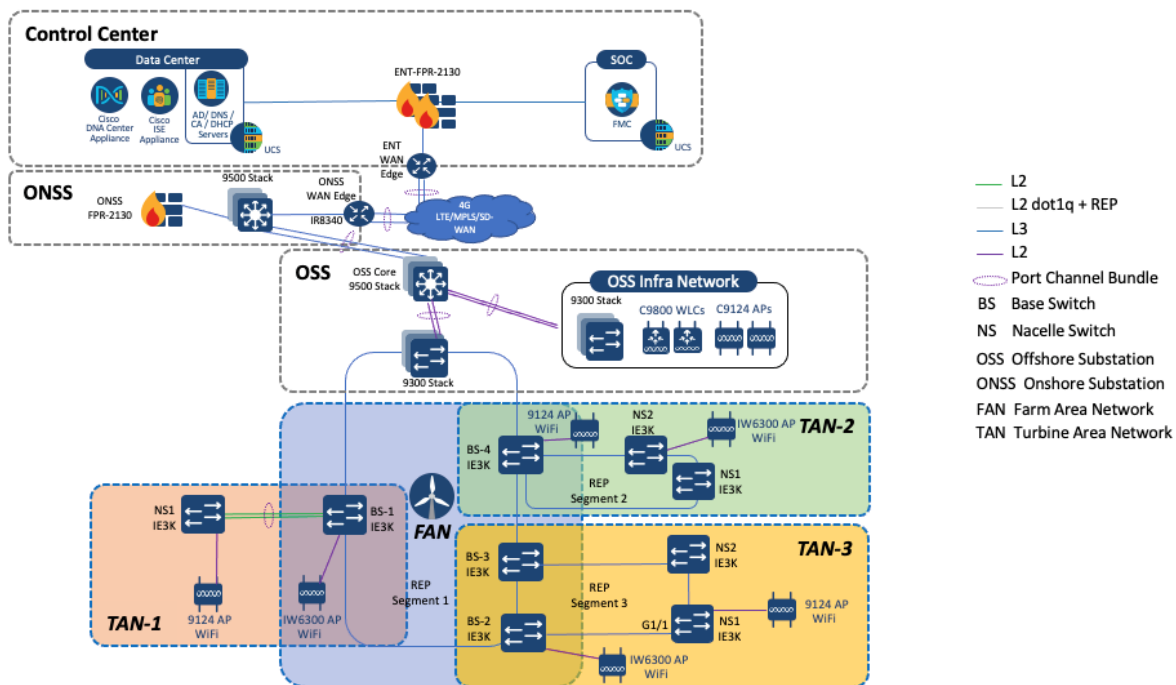
Offshore Wind Farm Wi-Fi Implementation

This section provides implementation details for offshore wind farm Wi-Fi access.

Wi-Fi implementation includes the following components:

- Cisco DNA 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 DNA Center non-fabric wireless deployment, see *Catalyst 9800 Non-Fabric Deployment using Cisco DNA 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 DNA Center

Catalyst 9800 Series WLCs can be configured in an active/standby high availability (HA) stateful switch-over (SSO) pair. Cisco DNA 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 DNA 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 DNA Center

High Availability

Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure.

Primary C9800 WF-WLC-9800.windfarm.com	Redundancy Management IP* 192.168.11.5
Select Secondary C9800 WLC.windfarm.com	Peer Redundancy Management IP* 192.168.11.6
Netmask* 24	

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 DNA 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 DNA 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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller Administration UI. The breadcrumb navigation is 'Administration > Device'. The left sidebar contains menu items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Redundancy' and includes the following configuration details:

- Redundancy Configuration: **ENABLED**
- Redundancy Pairing Type: **RMI+RP** (selected), RP
- RMI IP for Chassis 1*: 192.168.11.5
- RMI IP for Chassis 2*: 192.168.11.6
- Management Gateway Failover: **ENABLED**
- Gateway Failure Interval (seconds): 8
- Local IP: 169.254.11.6
- Remote IP: 169.254.11.5
- Keep Alive Timer: 1 x 100 (milliseconds)
- Keep Alive Retries: 5
- Chassis Renumber: 2
- Active Chassis Priority*: 1
- Standby Chassis Priority*: 2

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller Monitoring UI. The breadcrumb navigation is 'Monitoring > General > System'. The 'Redundancy' tab is selected. The 'General' section shows the following status:

- My State: ACTIVE
- Peer State: STANDBY HOT
- Unit: Primary
- Unit ID: 1
- Redundant Mode (Operational): sso
- Redundancy Mode (Configured): sso
- Redundancy State: sso
- Manual Swact: enabled
- Communications: Up
- Standby Failures: 0
- Switchovers System Experienced: 0

The 'Chassis Details' table is as follows:

Chassis	Role	MAC Address	Priority	H/W Version	Current State	IP Address	RMI IP Address	Mobility MAC Address	Image Version	Device Uptime
*1	Active	f4bd.9e56.d540	2	V02	Ready	169.254.11.5	192.168.11.5	f4bd.9e56.d54b	17.9.2	1 week, 3 hours, 15 minutes
2	Standby	f01d.2d36.3ce0	1	V02	Ready	169.254.11.6	192.168.11.6	0000.0000.0000	17.9.2	1 week, 3 hours, 11 minutes

The 'Switchover Details' section shows 0 items to display.

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 DNA Center

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

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





Figure 7-7: Select APs to Provision

The screenshot shows the Cisco DNA Center Inventory page. At the top, it says 'DEVICES (4)' and 'FOCUS: Inventory'. Below this is a table with columns for 'Device Name', 'IP', 'Actions', 'Reachability', 'EoX Status', and 'Manageability'. Four devices are listed, each with a blue checkmark in the 'Actions' column. A context menu is open over the 'Provision' action for the second device, showing options like 'Assign Device to Site', 'Provision Device', 'LAN Automation', and 'LAN Automation Status'. The 'Provision Device' option is highlighted.

Device Name	IP	Actions	Reachability	EoX Status	Manageability
AP3C57.31C5.7EF4	19	Inventory	Reachable	Not Scanned	Managed
AP3C57.31C5.ADA8	19	Provision	Reachable	Not Scanned	Managed
AP2416.9DDE.DB58	19	Telemetry	Reachable	Not Scanned	Managed
APA0B4.3965.BEA0	19	Device Replacement	Reachable	Not Scanned	Managed

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 DNA Center.

Figure7-8: Assign Each AP to a Site

Serial Number	Devices	
FOC243919K1	AP3C57.31C5.7EF4	 Global/RTP/RTP-06/Floor-1 ✕
		<input checked="" type="checkbox"/> Apply to All ⓘ
FJC25251V6Q	AP3C57.31C5.ADA8	 Global/RTP/RTP-06/Floor-1 ✕
FCW2415P0ET	AP2416.9DDE.DB58	 Global/RTP/RTP-06/Floor-1 ✕
FCW2350PKCW	APA0B4.3965.BEA0	 Global/RTP/RTP-06/Floor-1 ✕

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

Network Devices / Provision Devices

1 Assign Site 2 Configuration 3 Summary

Serial Number	Device Name	AP Zone Name	RF Profile	SSIDs
FOC243919K1	AP3C57.31C5.7EF4	Not Applicable	LOW	2
			Apply to All ⓘ	
FJC25251V6Q	AP3C57.31C5.ADA8	Not Applicable	LOW	2
FCW2415P0ET	AP2416.9DDE.DB58	Not Applicable	LOW	2
FCW2350PKCW	APA0B4.3965.BEA0	Not Applicable	LOW	2

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

The screenshot displays the 'Provision Devices' interface. On the left, a list of devices is shown with their IDs: AP3C57.31C5.7EF4, AP3C57.31C5.ADA8, AP2416.9DDE.DB58, and APA0B4.3965.BEA0. The main area shows the configuration summary for a selected device, categorized into three sections:

- Device Details:**
 - Device Name: AP3C57.31C5.ADA8
 - Serial Number: FJC25251V6Q
 - Mac Address: 4c:a6:4d:23:ba:c0
 - Device Location: Global/RTP/RTP-06/Floor-1
- AP Zone Details:**
 - AP Zone Name: default-zone
- RF Profile Details:**
 - RF Profile: LOW
 - Radio Type: 2.4GHz/5GHz/6GHz
 - 5GHz Channel Width: 20 MHz
 - 6GHz Channel Width: Best
 - 2.4GHz Data Rate(In Mbps): 1,2,5,5,6,9,11,12,18,24,36,48,54
 - 5GHz Data Rate(In Mbps): 6,9,12,18,24,36,48,54
 - 6GHz Data Rate(In Mbps): 6,9,12,18,24,36,48,54
 - Zero Wait DFS: Disabled

On the right, the 'Provision Device' dialog box is open. It has three radio buttons: 'Now' (selected), 'Later', and 'Generate configuration preview'. Below these is a 'Task Name*' field containing 'Provision APs'. At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

- 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

Warning

All the Unified AP(s), which are already part of the configured floor(s) for the selected RF profile and Zone will be processed and rebooted along with selected ones.

Do you want to continue?

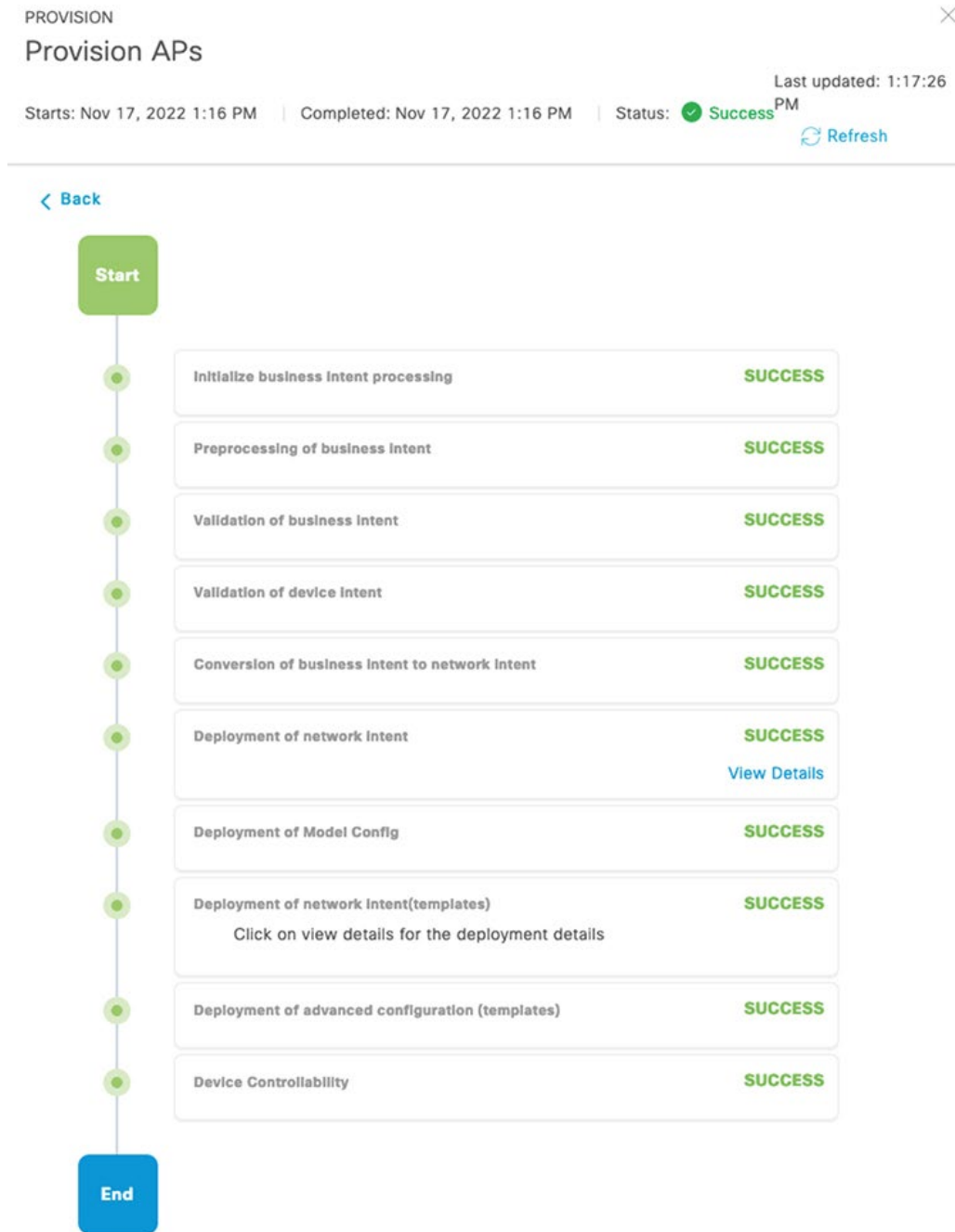
No **Yes**

- Click **Yes**.

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

- Navigate to the Cisco DNA 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 DNA Center

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

1. Upload and tag the desired C9800 WLC image as the golden image in the Cisco DNA 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 DNA Center Image Repository

Image Name	Version	Devices	Advisories	Golden Image	Device Roles & Tags
C9800-L-universalk9_wlc.17.10.01.SPA.bin Verified	17.10.01.0.1444 (Latest) Add On (N/A)	0	0 Criti... 0 High	★	Role: All

2. Choose **Provision > Inventory**.

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

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

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	MAC Address	Device Role	Image Version
AP3C57.31C5.7EF4	192.168.11.11	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../RTP-06/Floor-1	4c:a6:4d:22:45:40	ACCESS	17.9.2.52
AP3C57.31C5.ADA8	192.168.11.12	Unified AP	Reachable	Not Scanned	Managed	N/A	6	.../RTP-06/Floor-1	4c:a6:4d:23:ba:c0	ACCESS	17.9.2.52
AP2416.90DE.D858	192.168.11.14	Unified AP	Reachable	Not Scanned	Managed	N/A	6	.../RTP-06/Floor-1	5c:a6:2d:ff:df:a0	ACCESS	17.9.2.52
APA084.3965.BEA0	192.168.11.13	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../RTP-06/Floor-1	a0:b4:39:c3:63:20	ACCESS	17.9.2.52
WF-WLC-9800.windfarm.com	192.168.11.10	Wireless Controller	Reachable	0 alerts	Managed	Non-Compliant	10	.../RTP/RTP-06	f0:1d:2d:36:3c:eb	ACCESS	17.9.2

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

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

✖ **Software Image** i

Non-Compliant since Dec 6th, 2022, 02:56:01 PM
Compliance last run on: Dec 6th, 2022, 02:56:01 PM

17.10.01

Golden Image Version

Running Version: 17.9.2

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

Figure 7-16: Choose the C9800 WLC to Upgrade

DEVICES (5)
FOCUS: **Inventory** ▾

Filter | Add Device Tag Actions ^ ⓘ | 1 Selected

Device Name	Inventory	Device Family	Reachability ⓘ
<input type="checkbox"/> AP3C57.31C5.7EF4	Software Image >	Image Update	
<input type="checkbox"/> AP3C57.31C5.ADA8	Provision >	Image Update Status	
<input type="checkbox"/> AP2416.9DDE.DB58	Telemetry >	Download Update Readiness Report	
<input type="checkbox"/> APA0B4.3965.BEA0	Device Replacement >	Check Image Update Readiness	
<input checked="" type="checkbox"/> WF-WLC-9800.windfarm	Compliance >	Wireless Controller	Reachable
	More >		

- 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

Image Update ×

1 Analyze Selection 2 Distribute 3 Activate 4 Schedule and Clean Up 5 Summary

Analyze Selection
Before you proceed for the Update, analyze your selection.

Devices to Update: 1 | Device Family: 1 | Sites: 1

Search Table ▾

1 Selected Update ▾ ISSU ▾

Device	From Image	To Image ⓘ	Comment
WF-WLC-9800.windfarm.com (192.168.11.10)	C9800-L-universalk9_wlc.17. 09.02.SPA.bin	C9800-L-universalk9_wlc.17. 10.01.SPA.bin	Update Readiness Report

[Take a Tour](#) [Back](#) [Next](#)

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

Figure 7-18: Software Distribution Checks

Image Update

1 Analyze Selection 2 Distribute 3 Activate 4 Schedule and Clean Up 5 Summary

Software Distribution Checks
You can set an order on Pre and Post checks for your Software Distribution. If you don't see the check you can add a new custom check.

1 Pre and Post checks

Flash check SYSTEM PRE

Not able to see the check you would like to run? You can [add a new check](#).

Back Next

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

Figure 7-19: Image Activation Configuration

Image Update

1 Analyze Selection 2 Distribute 3 Activate 4 Schedule and Clean Up 5 Summary

Software Activation Checks
You can enable and set an order on Pre and Post checks for your Software Activation. If you don't see the check you can add a new custom check.

Skip Activation

2 Pre and Post checks

Config register check SYSTEM PRE

Startup config check SYSTEM PRE POST

Not able to see the check you would like to run? You can [add a new check](#).

Back Next

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

Figure 7-20: Schedule Update and Clean Up

Image Update ×

Analyze Selection Distribute Activate **4** Schedule and Clean Up 5 Summary

Schedule
Schedule when you want the software distribution and activation tasks to occur.

ⓘ Your time zone will be used as the default site time zone.

Software Distribution
⚠ If the ITSM ServiceNow application is enabled, choose Later.

Software Activation
After Distribution

Now Later

Task Name*
Distribution of C9800-L-universalk9_wlc.17.1C

Flash Cleanup
Flash cleanup will store only the running image and remove all previous images saved on the device.

Initiate Flash Cleanup after Activation

Back Next

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

Figure 7-21: C9800 WLC Image Upgrade Summary

Image Update

Analyze Selection Distribute Activate Schedule and Clean Up **5 Summary**

Summary
Review your entry and make changes if you wish to do

Devices to Update: 1 | Device Family: 1 | Sites: 1

Device	From Image	To Image	Update Support
WF-WLC-9800.windfarm.com (192.168.11.10)	C9800-L-universalk9_wlc.17.09.0 2.SPA.bin	C9800-L-universalk9_wlc.17.10.0 1.SPA.bin	

Software Distribution Checks

Scheduled On
Now

Pre And Post Checks
1. Flash check SYSTEM PRE

Software Activation Checks

Scheduled On
Activation will take place right after Distribution is done.

Flash Cleanup : Enabled

Pre And Post Checks
1. Config register check SYSTEM PRE
2. Startup config check SYSTEM PRE POST

[Back](#) [Submit](#)

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

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

PROVISION

WLC-Update

Starts: Nov 16, 2022 3:49 PM | Completed: Nov 16, 2022 3:51 PM | Status: Success | Last updated: 3:51:14 PM [Refresh](#)

Hostname: WF-WLC-9800.windfarm.com
IP Address: 192.168.10.11

App Name	Device Provisioning, Device Controllability and Telemetry	Success ●
Configured At	Nov 16, 2022 3:51 PM	
Description	WLC-Update	

[See Details](#)

Wi-Fi Guest User Access

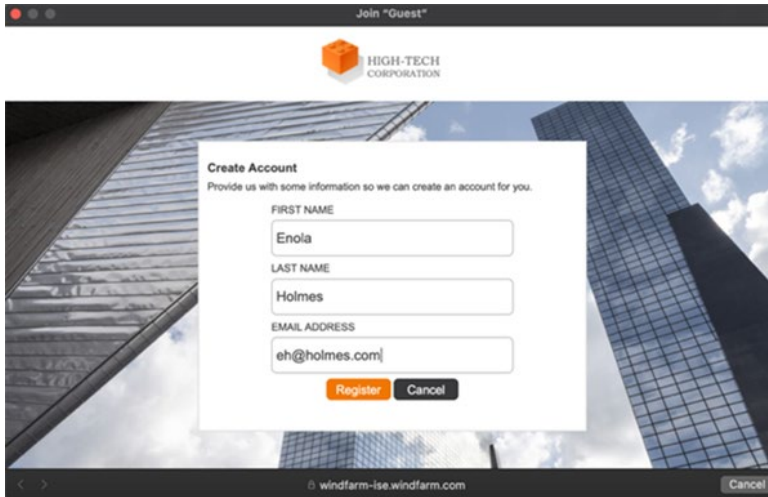
This section describes the steps that a guest user needs to perform to connect to the Guest SSID for internet access.

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 not appear automatically, open a browser and navigate to the internet.

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



Join "Guest"

HIGH-TECH CORPORATION

Create Account
Provide us with some information so we can create an account for you.

FIRST NAME
Enola

LAST NAME
Holmes

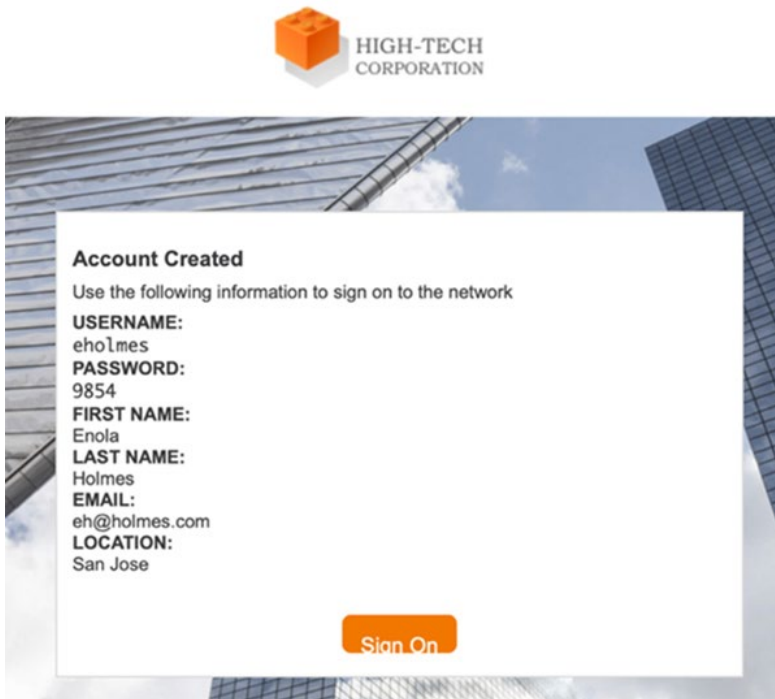
EMAIL ADDRESS
eh@holmes.com

Register Cancel

windfarm-ise.windfarm.com Cancel

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



HIGH-TECH CORPORATION

Account Created
Use the following information to sign on to the network

USERNAME:
eholmes

PASSWORD:
9854

FIRST NAME:
Enola

LAST NAME:
Holmes

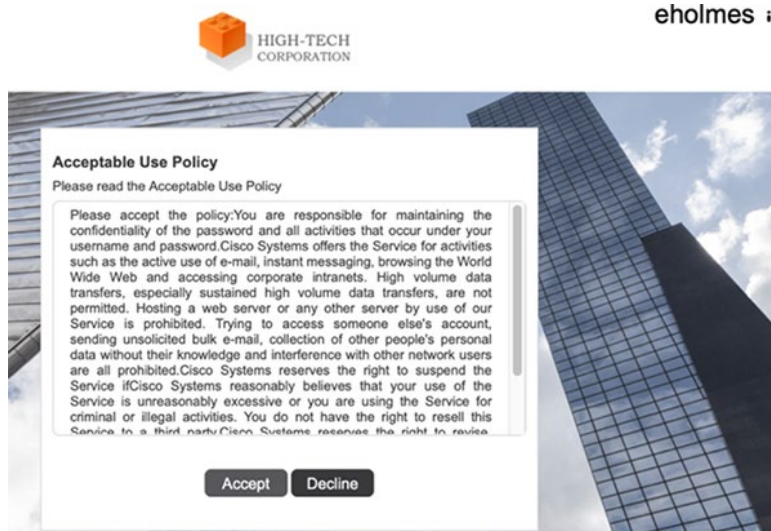
EMAIL:
eh@holmes.com

LOCATION:
San Jose

Sign On

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

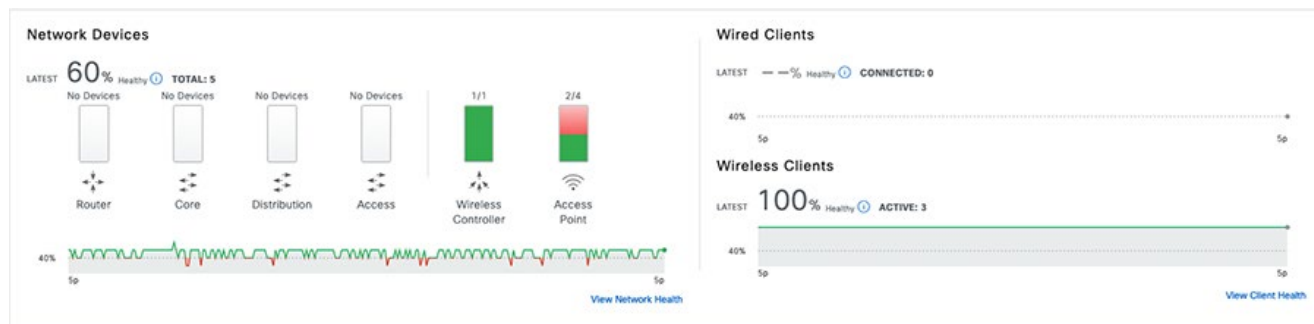
This section provides an overview of how you can use Cisco DNA Assurance to monitor and troubleshoot the WLAN deployment. Cisco DNA Assurance provides the ability to monitor the health of Cisco WLCs, APs, and wireless clients.

Cisco DNA Center Wireless Assurance

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

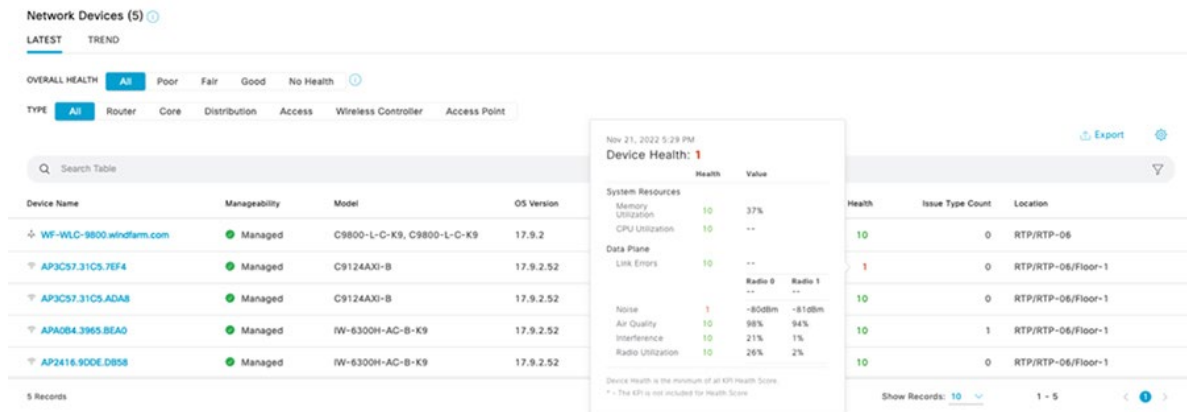
The **Overall Health Dashboard** depicts the health of all the wired and wireless devices in the network.

Figure 7-26: Overall Health Dashboard



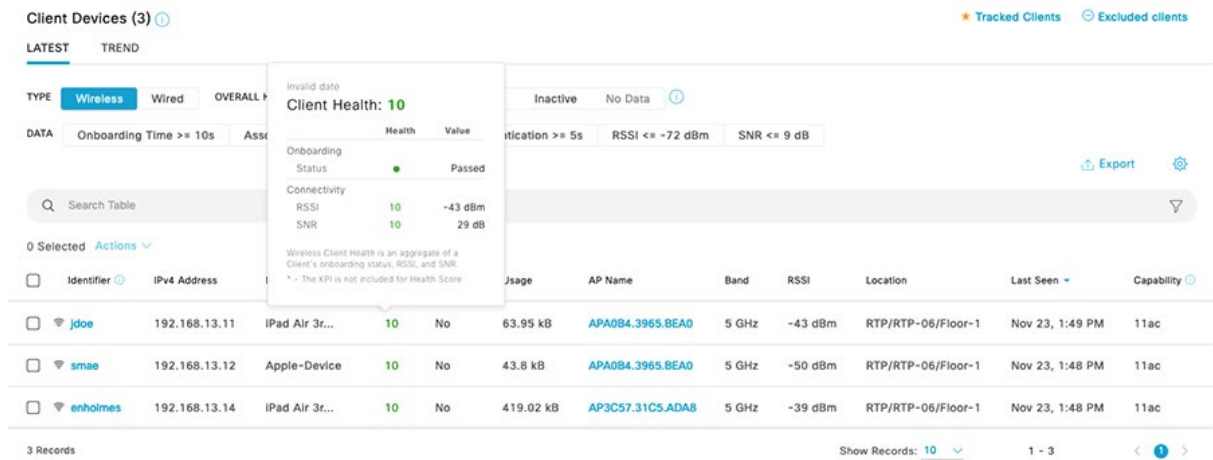
You also can view **Network Device Health**, which shows the health of wireless devices (WLCs and APs) by clicking the **Network** tab under **Assurance > Dashboards > Health**.

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



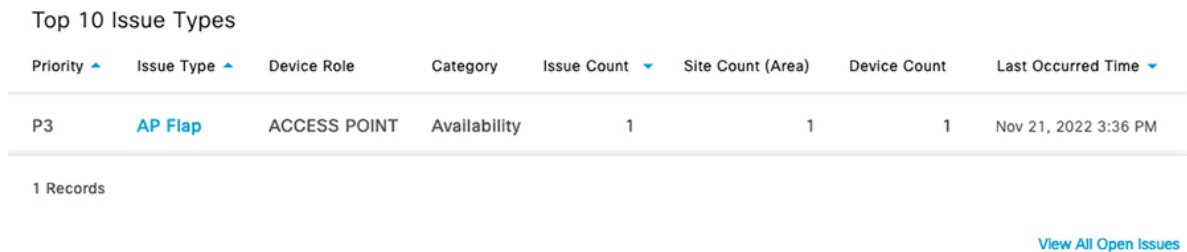
DNA Assurance also displays the health of each wireless client. Choose the **Client** tab under **Assurance > Dashboards > Health** to view client health status.

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

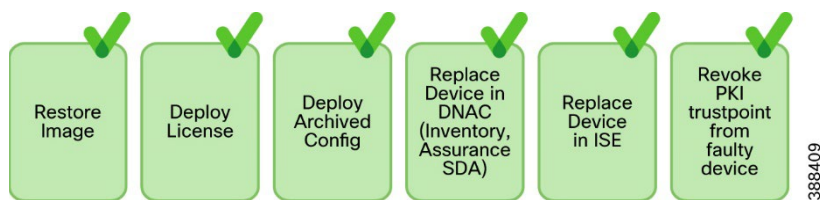


DNA Assurance also helps monitor the status of the AAA server (ISE server) and DHCP server (Active Directory) on the **Overall Health Dashboard**.

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

Defective AP Replacement (RMA) using Cisco DNA Center

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

Figure 7-31: Cisco DNA Center RMA Features


Replace a Faulty Access Point

Using the Cisco DNA 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 DNA 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 DNA 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**.

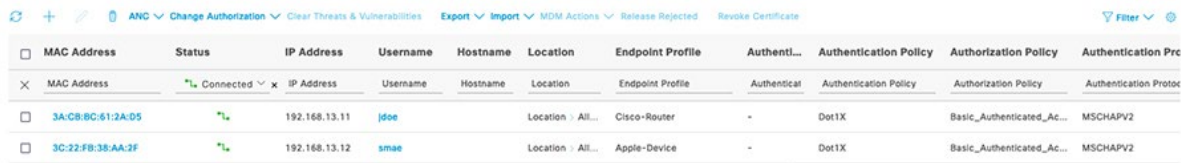
The RMA process begins.

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 DNA 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



MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authenti...	Authentication Policy	Authorization Policy	Authentication Prc
3A:CB:8C:61:2A:D5	Connected	192.168.13.11	jdoe		Location : All...	Cisco-Router	-	Dot1X	Basic_Authenticated_Ac...	MSCHAPV2
3C:22:FB:38:AA:2F	Connected	192.168.13.12	smae		Location : All...	Apple-Device	-	Dot1X	Basic_Authenticated_Ac...	MSCHAPV2

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

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

Cisco ISE

Overview

Event: **5200 Authentication succeeded**

Username: **jdoo**

Endpoint Id: **88-66:5A:54-AA:C8**

Endpoint Profile: **Apple-Device**

Authentication Policy: **Default >> Dot1X**

Authorization Policy: **Default >> Basic_Authenticated_Access**

Authorization Result: **PermitAccess**

Steps

11001 Received RADIUS Access-Request

11017 RADIUS created a new session

15049 Evaluating Policy Group

15008 Evaluating Service Selection Policy

11507 Extracted EAP-Response/Identity

12500 Prepared EAP-Request proposing EAP-TLS with challenge

12625 Valid EAP-Key-Name attribute received

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12301 Extracted EAP-Response/NAK requesting to use PEAP instead

12300 Prepared EAP-Request proposing PEAP with challenge

12625 Valid EAP-Key-Name attribute received

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12302 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated

12319 Successfully negotiated PEAP version 1

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12807 Prepared TLS Certificate message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12305 Prepared EAP-Request with another PEAP challenge

Authentication Details

Source Timestamp: 2022-11-18 16:51:47.568

Received Timestamp: 2022-11-18 16:51:47.568

Policy Server: Windfarm-ISE

Event: **5200 Authentication succeeded**

Username: **jdoo**

Endpoint Id: **88-66:5A:54-AA:C8**

Calling Station Id: **88-66-5a-54-aa-c8**

Endpoint Profile: **Apple-Device**

Authentication Identity Store: **WF_AD**

Identity Group: **Profiled**

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

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 2 Clients

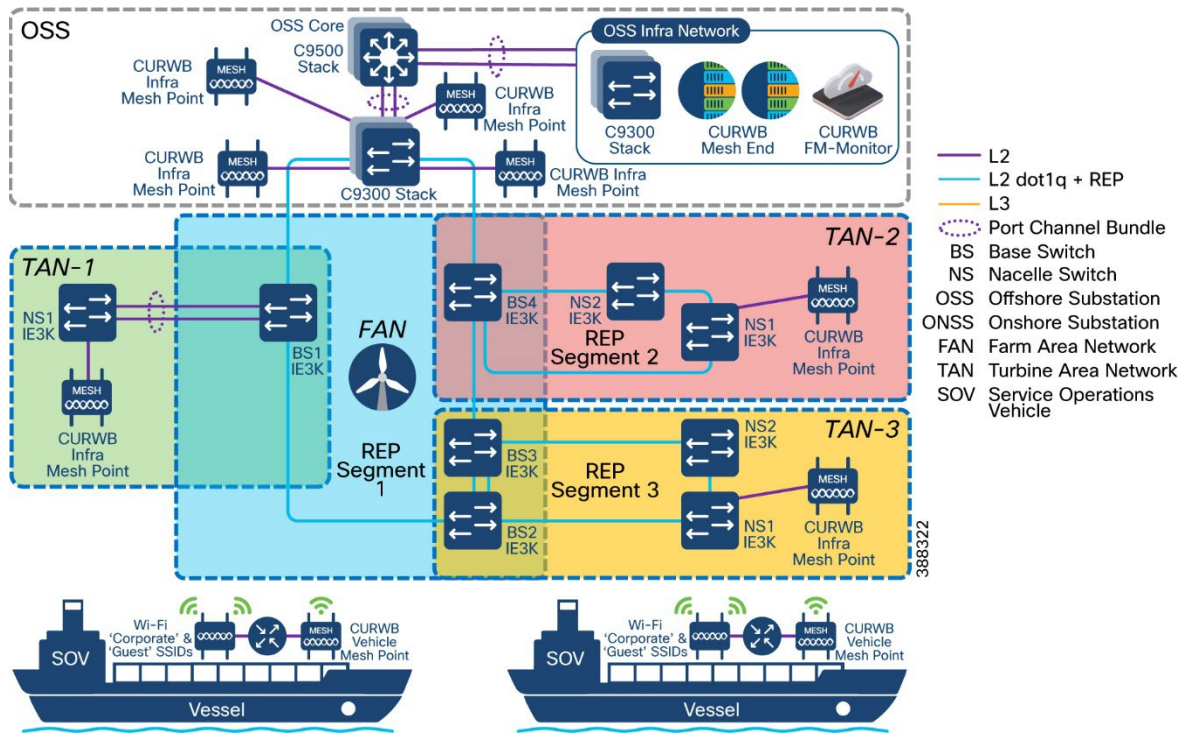
Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
3acb.bc61.2ad5	192.168.13.11	fe80::1436:681d:ea37:aae4	AP3C57.31C5.ADA8	Corp	18	WLAN	Run	11ac	jdoo	iPad Air 3rd Gen	Local
3c22.fb38.aa2f	192.168.13.12	fe80::186f:936:120d:4cad	AP3C57.31C5.ADA8	Corp	18	WLAN	Run	11ac	smae	OS_X-Workstation	Local

1 - 2 of 2 clients

Offshore Wind Farm CURWB Implementation for SOV to OSS Connectivity

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

Figure 7-35: Offshore Wind Farm CURWB 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 CURWB wireless deployment for SOV to OSS wireless backhaul connectivity.

- The switch ports where CURWB mesh ends are connected must be configured as trunk ports allowing both the CURWB management VLAN and the traffic VLAN.
- The native VLAN for the trunk must be the CURWB Management VLAN.
- The switch ports where CURWB radios are connected must be configured as access ports in the CURWB 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 CURWB-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

```

Implementing Wireless Access Networks

```
!  
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 CURWB-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 access vlan 106  
  switchport mode access  
!  
interface GigabitEthernet1/0/2  
  description connected to OSS Radio 2  
  switchport access vlan 106  
  switchport mode access  
!  
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 access vlan 106
```

Implementing Wireless Access Networks

```
    switchport mode access
!
interface GigabitEthernet2/0/2
  description connected to OSS Radio 4
  switchport access vlan 106
  switchport mode access
!
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 CURWB-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
!
```


CURWB Network Configuration

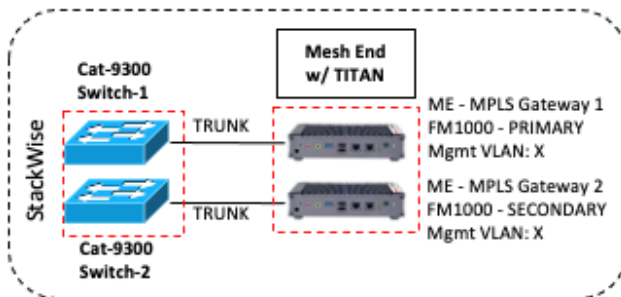
This section provides sample configurations for a CURWB deployment to provide SOV to OSS connectivity.

- A pair of CURWB mesh ends should be deployed for redundancy and high availability.
- The TITAN high availability plug-ins should be applied to both mesh ends for fast failover.
- The switch ports where CURWB mesh ends are connected must be configured as trunk ports, allowing both CURWB management VLAN and traffic VLAN. The native VLAN on a trunk must be the CURWB Management VLAN.
- Each mesh end should be connected to a different Cisco Catalyst 9300 switch within the stack.
- The CURWB 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 CURWB APs and the mesh ends must be configured with the same passphrase.

OSS Infrastructure FM1000 Mesh End

Figure 7-36 shows the deployment topology for a redundant pair of CURWB FM1000 mesh ends in the OSS network.

Figure 7-36: CURWB FM1000 Mesh End High Availability Deployment



The following example shows a snippet of the running configuration from a CURWB FM1000 mesh end gateway:

```
##### GENERAL CONFIG #####
 02:50:56 up 10 days, 5:01, 1 user, load average: 0.00, 0.01, 0.05
RACER mode: Offline
Monitoring: disabled
Device name: OSS-FM1000-1
Model: 1000
Firmware: 1.6.0
SP: fluidmesh-1000-10000-sp1
IP: 10.10.106.10
Netmask: 255.255.255.0
Gateway: 10.10.106.1
Nameservers:
Mesh End mode
Passphrase: windfarm
MPLS layer: 2
##### FLUIDITY CONFIG #####
Fluidity enabled
Infrastructure mode
Large network optimization: disabled
Master-pseudowire enforcement: enabled
FMQuadro telemetry: enabled
##### MPLS CONFIG #####
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
reduce-broadcast: disabled
pwlist: all
```

Implementing Wireless Access Networks

```

Cluster ID: disabled
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 1864232102 debug 0 auto_pw 1
local_gw 5.100.119.5 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 }
lsp 4
##### VLAN CONFIG #####
VLAN status: disabled
Management VID: 106
Native VID: 106
##### ADVANCED CONFIG #####
Gratuitous-arp: enabled
    Delay: 150 ms
Jumbo-frames: enabled
NTP: disabled
Current date: Thu Apr 7 02:50:58 CEST 2022
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
BPDU snooping: enabled
Link guard: 0 second(s)
BPDU forwarding: 1
blacklist size 0
TLS supported version: 1.2, 1.1, 1.0
L2TP is disabled
PROFINET disabled
QNET disabled
CANBUS disabled
SNMP: disabled
LLDP: disabled
SNMP MIB: disabled
TFTP Server:                               unavailable
Automatic firmware upgrade: disabled
##### PLUGINS CONFIG #####
Plug-in List
FM1000-UN                                LICENSED
FM-TITAN                                  LICENSED

```

OSS Infrastructure FM3500 Mesh Point

The following example shows a snippet of the running configuration from a CURWB FM3500 mesh point radio:

```

##### GENERAL CONFIG #####
18:12:00 up 10 days, 5:00, load average: 0.06, 0.09, 0.13
RACER mode: Offline
Monitoring: disabled
Device name: OSS-FM3500-1
Model:          FM3500
Firmware: 9.4
IP:            10.10.106.11

```

Implementing Wireless Access Networks

```
netmask: 255.255.255.0
Gateway: 10.10.106.1
Nameservers:
Mesh Point mode
Prodigy version: 2
##### WIRELESS CONFIG #####
Passphrase: windfarm
Frequency: 5200 MHz
Channel Width: 40 MHz
TX Chains: both enabled
AES encryption: disabled
Current TX power: 13 dBm
Antenna gain: not selected
Country: UNITED STATES
Max TX MCS: 9
Max TX NSS: 2
RTS protection: disabled
NAV timer override: disabled
TX calibration data: factory
Target Power data: default
Retry limit: 8
Fallback levels: 8
Single Stream Fallback: enabled
Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1 cw_min=3 cw_max=7 txop=15 (1 ms) ampdu=0
vi: aifs=1 cw_min=7 cw_max=15 txop=31 (3 ms) ampdu=32
be: aifs=3 cw_min=15 cw_max=63 txop=31 (3 ms) ampdu=32
bk: aifs=7 cw_min=7 cw_max=15 txop=0 (0 ms) ampdu=32
AMPDU aggregation reorder buffer timeout: 100 ms
Mesh beacon period: 100 ms
Mesh beacon MCS: 0
Mesh beacon jitter: 0
##### FLUIDITY CONFIG #####
Fluidity enabled
Infrastructure mode
Backhaul-check: disabled
Mesh-end backhaul-check: disabled
Color: none
Rate control: advanced
Flags: 0x2F
VHT mcs sets: 0 3 1 4 2 5 4 7 5 9 7 9
HT mcs sets: 0 2 1 3 2 4 3 5 4 7 5 7
VHT group sets: 12 19 12 19 12 19 12 19 12 19 16 19
HT 40Mhz group sets: 0 7 0 7 0 7 0 7 0 7 4 7
HT 20Mhz group sets: 0 3 0 3 0 3 0 3 0 3 0 3
Statistics update period: 50 50 50 50 50 50 ms
Network type: flat (layer 2)
Warmup time: 20000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Master-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
##### INTRA-CAR CONFIG #####
Intra-car feature unavailable (unit is not in bridge mode)
##### MPLS CONFIG #####
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
```

Implementing Wireless Access Networks

```

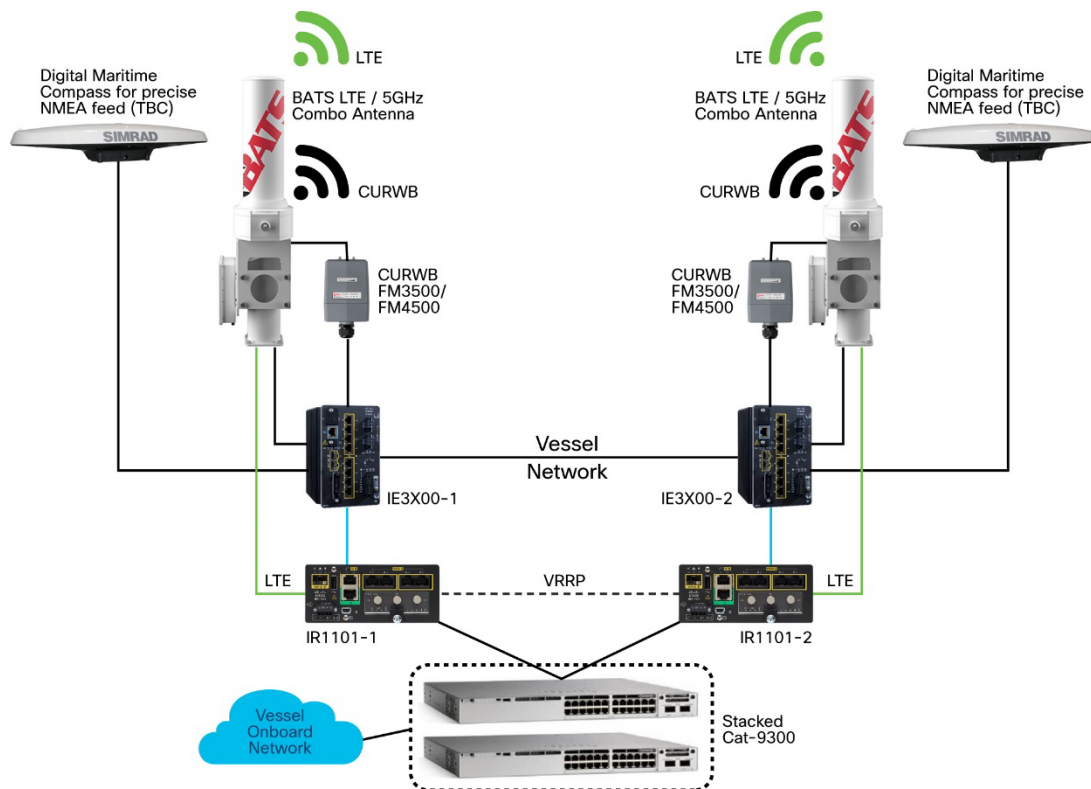
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
MPLS fast failover is disabled
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255  dynamic
MPLS tunnels:
ldp_id 231835902 debug 0 auto_pw 1
local_gw 5.100.119.5 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0 }
lsp 4
##### VLAN CONFIG #####
VLAN plugin not available
##### ADVANCED CONFIG #####
FluidMAX Mode: OFF
Cluster ID: fluidmesh
Current state: MT76X2_P2MP_CSMA
Gratuitous-arp: enabled
    Delay: 150 ms
Jumbo-frames: enabled
NTP: disabled
Current date: Thu Aug 5 18:12:10 UTC 2021
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
BPDU snooping: enabled
Link guard: 0 second(s)
BPDU forwarding: 1
blacklist size 0
TLS supported version: 1.2, 1.1, 1.0
SNMP: disabled
LLDP: disabled
SNMP MIB: disabled
telnet access disabled
TFTP Server:                unavailable
Automatic firmware upgrade: disabled
##### PLUGINS CONFIG #####
Plug-in List
FM3500-MOB-TRK-UN          LICENSED

```

Service Operations Vessel Network

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

Figure 7-37: SOV Network Topology



388325

SOV Wired Network

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

IE3X00-1

```

!
vlan 106
 name CURWB-Mgmt
!
spanning-tree vlan 106 priority 4096
!
interface GigabitEthernet1/3
 description V-FM3500-1
 switchport access vlan 106
 switchport mode access
 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 CURWB-Mgmt  
!  
interface GigabitEthernet1/3  
  description V-FM3500-2  
  switchport access vlan 106  
  switchport mode access  
  spanning-tree portfast  
!  
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
```

Implementing Wireless Access Networks

```
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
```


Implementing Wireless Access Networks

```

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
!

```

CURWB Configuration

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

Service Operations Vessel FM3500-1 (Mobile)

```

##### GENERAL CONFIG #####
17:50:04 up 4:22, load average: 0.31, 0.20, 0.20
RACER mode: Offline
Monitoring: disabled
Device name: V-FM3500-1
Model:          FM3500
Firmware: 9.3
IP:            10.10.106.21
netmask:      255.255.255.0
Gateway:      10.10.106.1
Nameservers:
Mesh Point mode
Prodigy version: 2
##### WIRELESS CONFIG #####
Passphrase:      windfarm
Frequency:        5200 MHz
Channel Width:    40 MHz
TX Chains:        both enabled
AES encryption:   disabled
Current TX power: 30 dBm
Antenna gain:     not selected
Country:          UNITED STATES
Max TX MCS:       9
Max TX NSS:       2
RTS protection:   disabled
NAV timer override: disabled
TX calibration data: factory
Target Power data: default
Retry limit:      8
Fallback levels:  8
Single Stream Fallback: enabled
Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1      cw_min=3    cw_max=7    txop=15    (1 ms) ampdu=0
vi: aifs=1      cw_min=7    cw_max=15   txop=31    (3 ms) ampdu=32
be: aifs=3      cw_min=15   cw_max=63   txop=31    (3 ms) ampdu=32
bk: aifs=7      cw_min=7    cw_max=15   txop=0     (0 ms) ampdu=32
AMPDU aggregation reorder buffer timeout: 100 ms
Mesh beacon period: 100 ms
Mesh beacon MCS:  0
Mesh beacon jitter: 0
##### FLUIDITY CONFIG #####
Fluidity enabled
Vehicle ID: automatic, current 83957950 (master unit)
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
RSSI low/high zones threshold: 35

```

Implementing Wireless Access Networks

```
Color: enabled, current 0
Rate control: advanced
Flags: 0x12F
VHT mcs sets: 0 3 1 4 2 5 4 7 5 9 7 9
HT mcs sets: 0 2 1 3 2 4 3 5 4 7 5 7
VHT group sets: 12 19 12 19 12 19 12 19 12 19 16 19
HT 40Mhz group sets: 0 7 0 7 0 7 0 7 0 7 4 7
HT 20Mhz group sets: 0 3 0 3 0 3 0 3 0 3 0 3
Statistics update period: 50 50 50 50 50 50 ms
Network type: flat (layer 2)
Warmup time: 20000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Master-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
##### INTRA-CAR CONFIG #####
Intra-car feature unavailable (unit is not in bridge mode)
##### MPLS CONFIG #####
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
MPLS fast failover: enabled
Node failover timeout: 100 ms
L2TP WAN update delay: disabled
Preemption delay: 70 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 1233510339 debug 0 auto_pw 1
local_gw 5.100.119.5 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id 83957950 v2v_handoff 0 v2v_pws false auto_en true static_pws {
0.0.0.0 }
lsps 4
##### VLAN CONFIG #####
VLAN plugin not available
##### ADVANCED CONFIG #####
FluidMAX Mode: OFF
Cluster ID: fluidmesh
Current state: MT76X2_P2MP_CSMA
Gratuitous-arp: enabled
Delay: 150 ms
Jumbo-frames: enabled
NTP: disabled
Current date: Mon Jul 26 17:50:15 UTC 2021
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
BPDU snooping: enabled
```

Implementing Wireless Access Networks

```

Link guard: 0 second(s)
BPDU forwarding: 1
blacklist size 0
TLS supported version: 1.2, 1.1, 1.0
SNMP: disabled
LLDP: disabled
SNMP MIB: disabled
telnet access enabled
TFTP Server:                unavailable
Automatic firmware upgrade: disabled
##### PLUGINS CONFIG #####
Plug-in List
FM3500-UN                    LICENSED
FM3500-MOB-MOB-UN           LICENSED
FM-TITAN                    LICENSED

```

Service Operations Vessel FM3500-2 (Mobile)

```

##### GENERAL CONFIG #####
16:06:02 up 2 days, 2:48, load average: 0.25, 0.27, 0.30
RACER mode: Offline
Monitoring: disabled
Device name: V-FM3500-2
Model:          FM3500
Firmware: 9.3
IP:            10.10.106.22
netmask:      255.255.255.0
Gateway:      10.10.106.1
Nameservers:
Mesh Point mode
Prodigy version: 2
##### WIRELESS CONFIG #####
Passphrase:      windfarm
Frequency:        5200 MHz
Channel Width:    40 MHz
TX Chains:        both enabled
AES encryption:   disabled
Current TX power: 13 dBm
Antenna gain:     not selected
Country:          UNITED STATES
Max TX MCS:       9
Max TX NSS:       2
RTS protection:   disabled
NAV timer override: disabled
TX calibration data: factory
Target Power data: default
Retry limit:      8
Fallback levels: 8
Single Stream Fallback: enabled
Enhanced Distributed Channel Access (EDCA) configuration
vo: aifs=1        cw_min=3    cw_max=7    txop=15    (1 ms) ampdu=0
vi: aifs=1        cw_min=7    cw_max=15   txop=31    (3 ms) ampdu=32
be: aifs=3        cw_min=15   cw_max=63   txop=31    (3 ms) ampdu=32
bk: aifs=7        cw_min=7    cw_max=15   txop=0     (0 ms) ampdu=32
AMPDU aggregation reorder buffer timeout: 100 ms
Mesh beacon period: 100 ms
Mesh beacon MCS:  0
Mesh beacon jitter: 0
##### FLUIDITY CONFIG #####
Fluidity enabled
Vehicle ID: automatic, current 83957950 (slave unit)
Handoff logic: standard
Handoff hysteresis high threshold: 6

```

Implementing Wireless Access Networks

```
Handoff hysteresis low threshold: 3
RSSI low/high zones threshold: 35
Color: enabled, current 0
Rate control: advanced
Flags: 0x12F
VHT mcs sets: 0 3 1 4 2 5 4 7 5 9 7 9
HT mcs sets: 0 2 1 3 2 4 3 5 4 7 5 7
VHT group sets: 12 19 12 19 12 19 12 19 12 19 16 19
HT 40Mhz group sets: 0 7 0 7 0 7 0 7 0 7 4 7
HT 20Mhz group sets: 0 3 0 3 0 3 0 3 0 3 0 3
Statistics update period: 50 50 50 50 50 50 ms
Network type: flat (layer 2)
Warmup time: 20000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Master-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
Monitor host: 10.10.10.30:30000
FMQuadro telemetry: enabled
##### INTRA-CAR CONFIG #####
Intra-car feature unavailable (unit is not in bridge mode)
##### MPLS CONFIG #####
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
MPLS fast failover: enabled
Node failover timeout: 100 ms
L2TP WAN update delay: disabled
Preemption delay: 70 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 691943144 debug 0 auto_pw 1
local_gw 5.100.119.5 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id 83957950 v2v_handoff 0 v2v_pws false auto_en true static_pws {
0.0.0.0 }
lsp 4
##### VLAN CONFIG #####
VLAN plugin not available
##### ADVANCED CONFIG #####
FluidMAX Mode: OFF
Cluster ID: fluidmesh
Current state: MT76X2_P2MP_CSMA
Gratuitous-arp: enabled
Delay: 150 ms
Jumbo-frames: enabled
NTP: disabled
Current date: Wed Jul 28 16:06:13 UTC 2021
QoS: enabled
CoS map:
  0 1 2 3 4 5 6 7
  | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
```

Implementing Wireless Access Networks

```
qos-8021p disabled
Radius: disabled
BPDU snooping: enabled
Link guard: 0 second(s)
BPDU forwarding: 1
blacklist size 0
TLS supported version: 1.2, 1.1, 1.0
SNMP: disabled
LLDP: disabled
SNMP MIB: disabled
telnet access disabled
TFTP Server:                unavailable
Automatic firmware upgrade: disabled
##### PLUGINS CONFIG #####
Plug-in List
FM3500-MOB-MOB-UN          LICENSED
FM-TITAN                   LICENSED
```

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
```

Implementing WAN Backhaul and Control Center

```
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 Substation 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 DNA 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 DNA 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 DNA Center Installation and Configuration

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

Cisco DNA 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 DNA Center, see *Cisco DNA 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 DNA 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 DNA Center for dynamic mapping of users and devices to scalable groups, which simplifies end-to-end security policy management and enforcement at a greater scale than traditional network policy implementations that rely on IP address access lists.

ISE Installation and Initial Configuration

A centralized standalone deployment of ISE is configured with Cisco DNA 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 DNA Center. For instructions, see “Cisco DNA Center and Cisco ISE Integration” in *Cisco DNA 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 DNA Center, ensure that PxGrid services are online on the ISE and that the cluster node is up in Cisco DNA Center.

After integrating ISE with Cisco DNA Center using PxGrid, information sharing between ISE and Cisco DNA Center is enabled, including sharing of device information and group information. This sharing allows Cisco DNA Center to define policies that are pushed to ISE and then rendered into the network infrastructure by the ISE policy service nodes (PSNs). When integrating ISE and Cisco DNA 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 from 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 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>

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 DNA 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 DNA Center Templates
- Adding a New Switch to a FAN REP Ring
- Network Assurance

Preparing Cisco DNA Center and Switches for Device Onboarding

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

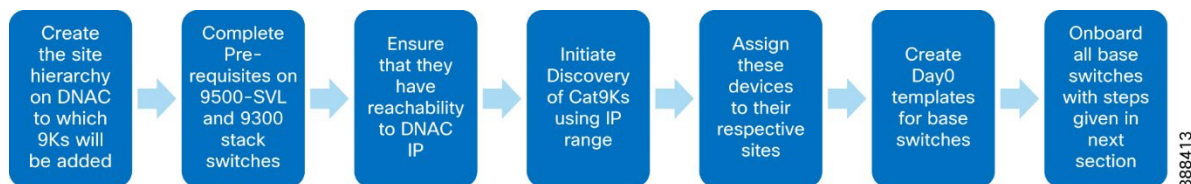
For more detailed information about Cisco DNA Center and related configurations, see *Cisco DNA Center User Guide, Release 2.3.5*:

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 DNA 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 DNA Center.

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



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

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

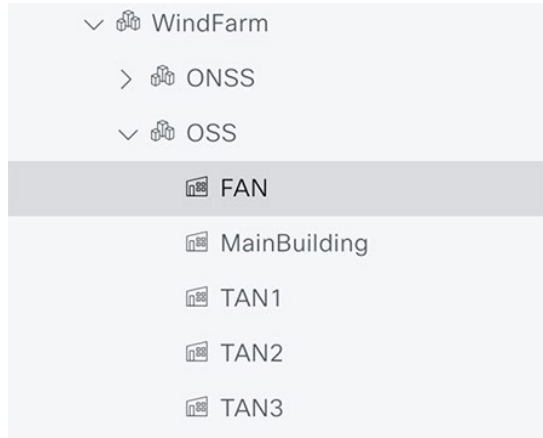
1. Choose **Design > Network Hierarchy** to create the site hierarchy in Cisco DNA Center to which Cisco 9000 and 3400 devices are to be added.

For detailed steps and an explanation of network hierarchy, see *Cisco DNA 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 DNA 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

```

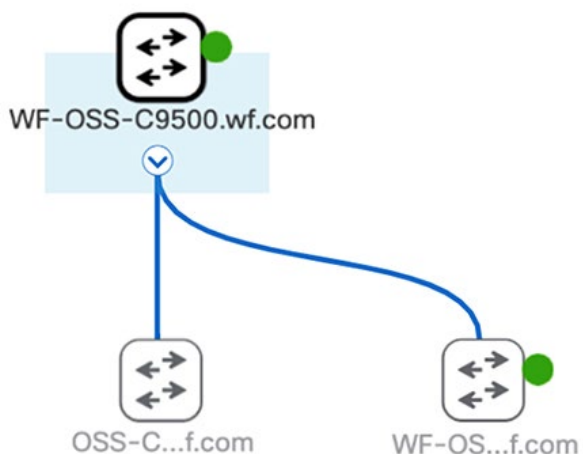
3. Verify that all three devices can reach Cisco DNA Center by initiating a ping to Cisco DNA Center from each of the three devices.
4. Perform the following actions to initiate the discovery of core switches in the OSS network.

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)

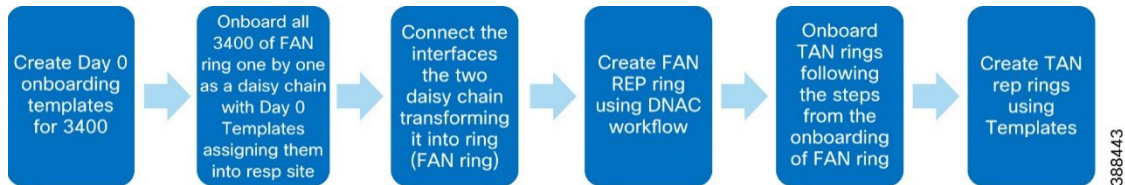
FAN and TAN rings consist of 3400 switches that are onboarded to Cisco DNA Center as separate daisy chains that are later closed to form a ring.

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 DNA Center for PnP. The switches are sequentially

onboarded to Cisco DNA 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 DNA 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 DNA Center, see *Cisco DNA Center User Guide, Release 2.3.52*:

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:

```

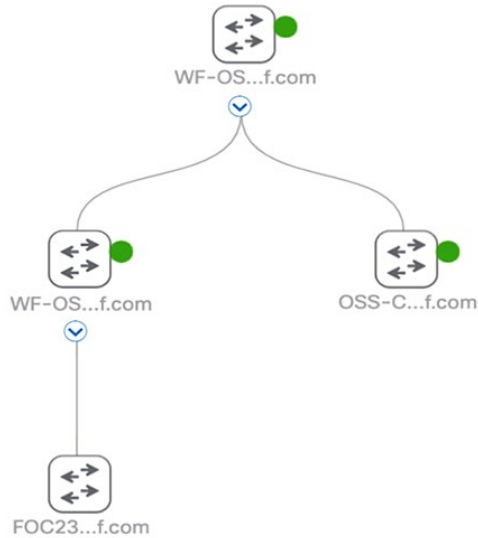
delete /force sflash:vlan.dat
delete /force sflash:*.cer
delete /force sflash:pn*
delete /force /recursive sflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pn*tech*time
delete /f flash:pn*tech*discovery*summary
#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 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.

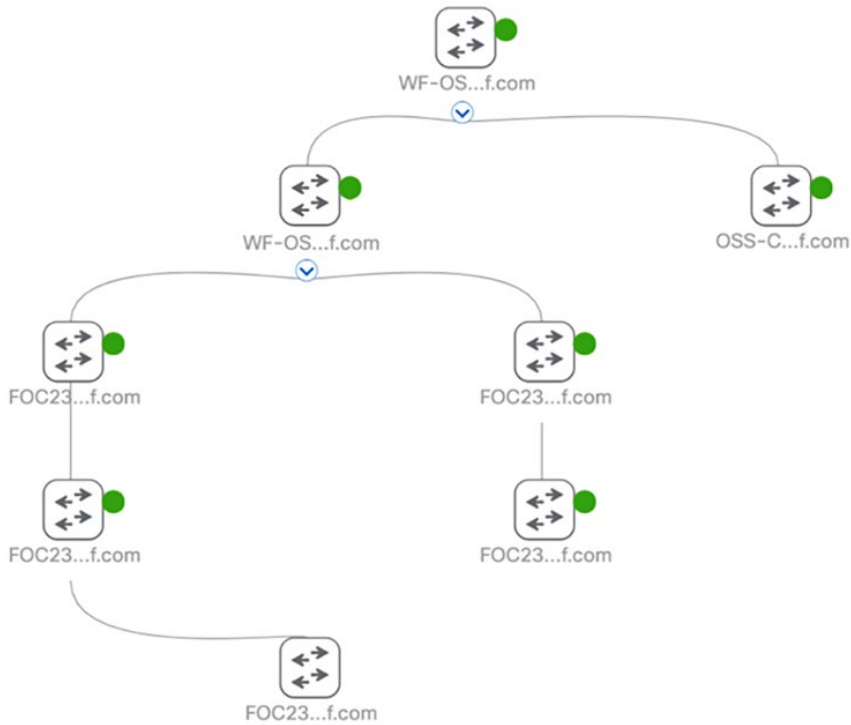
Figure 9-5: Onboarding the First 3400 Switch



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.

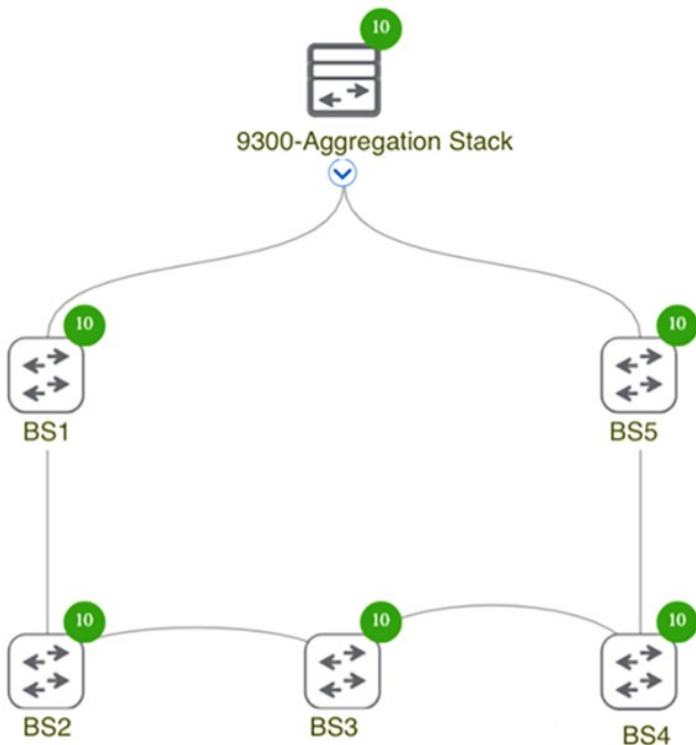
After onboarding the 3400 switches of both daisy chains of the ring is complete, verify the topology by choosing **Provision > Inventory > Topology**. The display should resemble the example shown in Figure 9-6.

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 DNA 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 DNA 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](#).

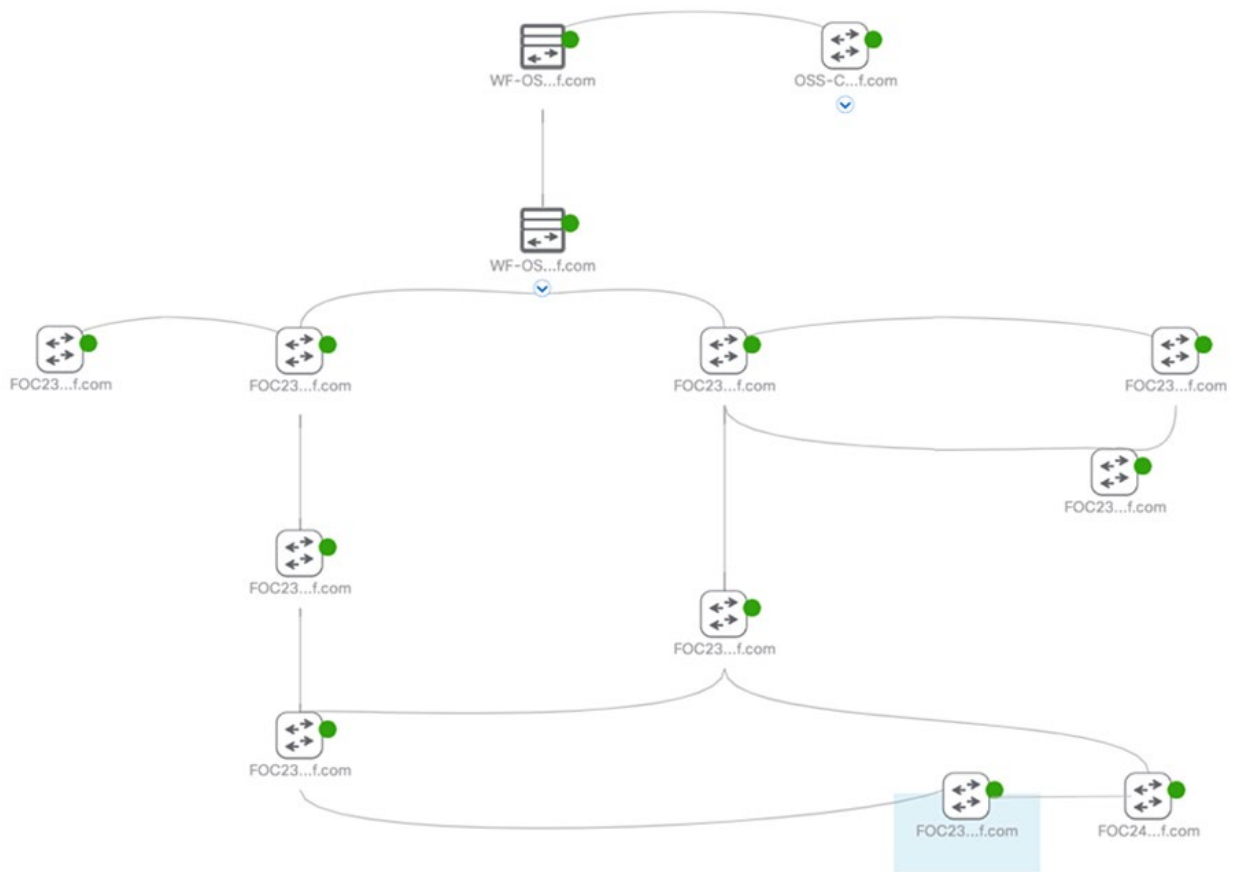
To onboard a TAN without HA (TAN1), connect the 3400 switch linearly to one of the FAN ring members (represented as BS1 in Figure 2-1) then follow Steps 2 to 4 in [Onboard the FAN Ring](#).

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 DNA 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 DNA Center by choosing **Provision > Inventory > Topology**. Figure 9-8 shows an example topology display.

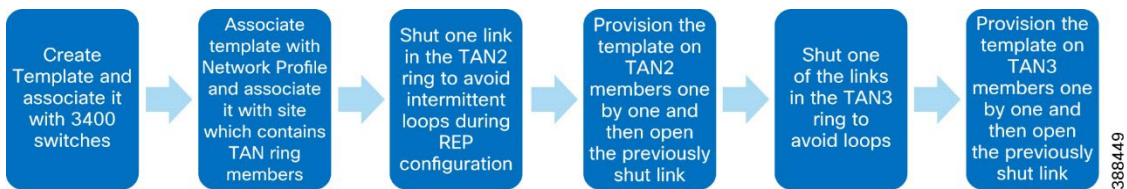
Figure 9-8: Cisco DNA Center Topology with all Devices Onboarded



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 DNA Center templates. Figure 9-9 shows the workflow for configuring TAN open and closed REP rings using Cisco DNA 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 DNA Center to configure REP in the TAN rings.

Cisco DNA 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 DNA Center see “Create Templates to Automate Device Configuration Changes” in *Cisco DNA 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

The screenshot shows a web-based configuration form titled "Add New Template". The form is divided into several sections:

- Project Name:** A dropdown menu with "DayNTemplates" selected.
- Template Type:** Two radio buttons: "Regular Template" (selected) and "Composite Sequence".
- Template Language:** Two radio buttons: "JINJA" and "VELOCITY" (selected).
- Software Type:** A dropdown menu with "IOS-XE" selected.
- Device Type Details:** A section with the instruction "Add the types of devices you want to associate with the template". It includes a link "Edit Device Details" and a table:

DEVICE DETAILS*	Edit Device Details
Device Family	Switches and Hubs
Devices	Cisco Catalyst IE3400 Rugged Series
Device Tags	
Device Tags	

At the bottom of the form are "Cancel" and "Continue" buttons.

- 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 DNA 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 DNA 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 DNA 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. In 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 DNA 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 DNA Center Templates

Configuration updates can be made on wind farm devices by using Cisco DNA Center templates. Templates can be created on Cisco DNA 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 DNA 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 DNA 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.

Implementing Network Management and Automation

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 DNA 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 DNA 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 DNA 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 DNA 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: filesystem
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
Libvirt 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](#) 1 > 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 DNA 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.

NetFlow 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
```

Implementing Network Security and QoS

```

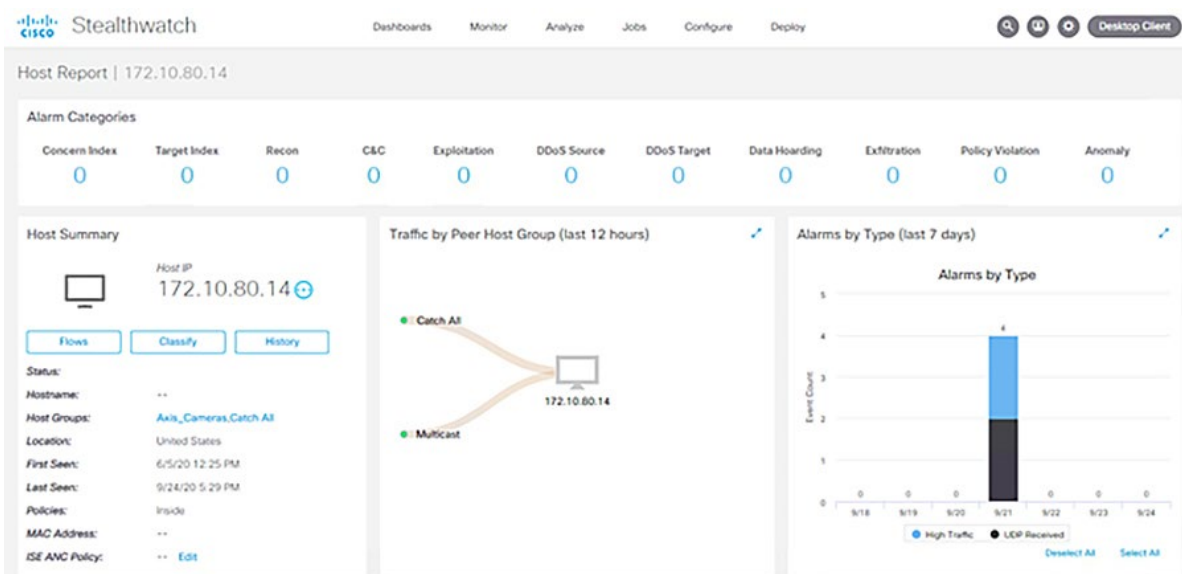
option application-table timeout 10
exit
##Configure the Flow Monitor##
flow monitor fnf-mon
exporter fnf-exp
cache timeout active 60
record fnf-rec
exit
##Apply to an interface##
interface $wired_interface
ip flow monitor fnf-mon input

```

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

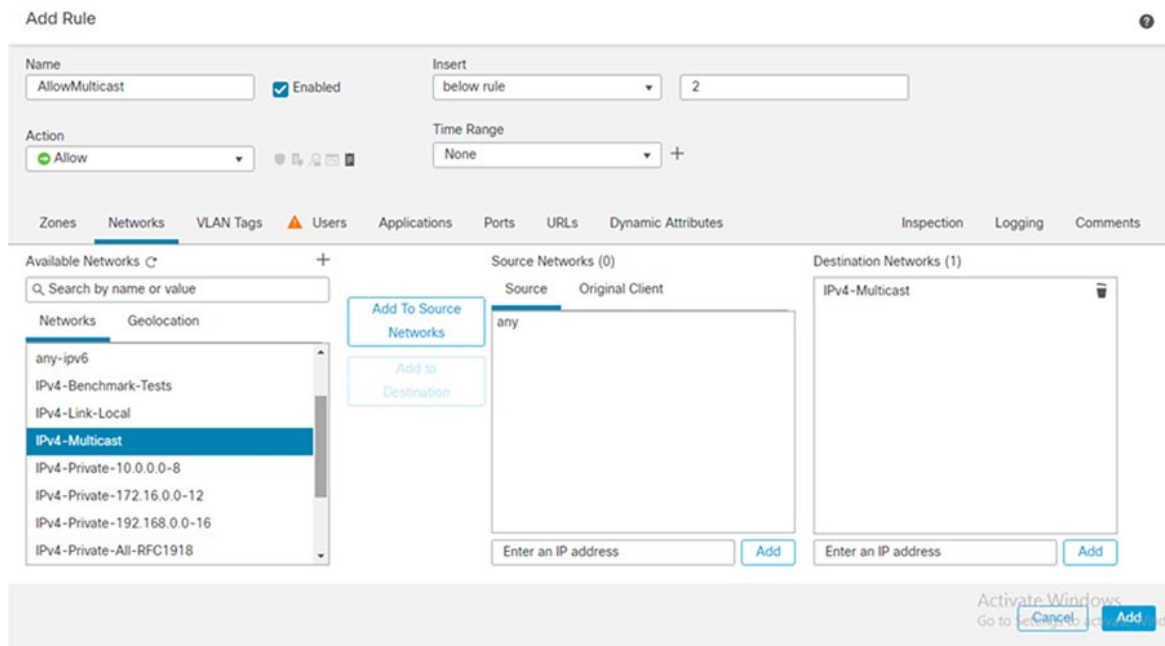


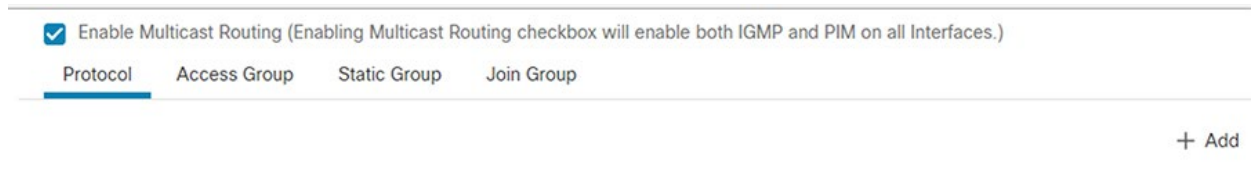
Figure 10-6 shows how an added policy appears.

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

The screenshot shows a configuration window titled "Edit IGMP parameters". The window contains the following fields and controls:

- Interface:***: A dropdown menu with "OPC_UA_ServerIntf" selected.
- Enable IGMP:**: A checked checkbox.
- Forward Interface:**: A dropdown menu with "OPC_Client_Int" selected.
- Version:**: A dropdown menu with "2" selected.
- Query Interval:**: An empty text input field.
- Response Time:**: An empty text input field.
- Group Limit:**: An empty text input field.
- Query Timeout:**: An empty text input field.
- At the bottom right, there are two buttons: "Cancel" and "OK".

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

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
```


Configuration Examples

```
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
```

Configuration Examples

```
!  
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
```

Configuration Examples

```
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-channell
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
```

Configuration Examples

```

!
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

```

Configuration Examples

```
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
!
```

Configuration Examples

```
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
```

Configuration Examples

```

!
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
!

```


Configuration Examples

```

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

```

Configuration Examples

```

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 6ADFOF0D 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 adventurerprise
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 sentry069!
!
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 sentry0
!
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

```

Configuration Examples

```
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
```

Configuration Examples

```
!
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
```

Configuration Examples

```
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
!
```

Configuration Examples

```

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 ptpdp 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 ptpdp 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 ptpdp 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 ptpdp 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 ptpdp R4 R5 R6 R8

```

Configuration Examples

```

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 ptpd 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 ptpd 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 ptpd 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 ptpd 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 ptpd 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 ptpd 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 ptpd 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 ptpd 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
  !

```

Configuration Examples

```
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
```


Configuration Examples

```
    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
!
```

Configuration Examples

```
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
```

Configuration Examples

```

!
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

```

Configuration Examples

```
!
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
```

Configuration Examples

```
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
```

Configuration Examples

```
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
```

Configuration Examples

```
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
```

Configuration Examples

```

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
!

```


Configuration Examples

```
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
!
```

Configuration Examples

```

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
  rsa-keypair 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 $9$rT5UEjrW0cqDA.$e2FNehaH33QAJmEoMFTYOs1VMrUmX2wD5IymWpNaSDo
!
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

```

Configuration Examples

```

    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,EGRException,NflSampled
  ,RpfFailed
class-map match-any scavenger
  match ip dscp cs1
!
policy-map system-cpp-policy
policy-map output
  class voice_o

```

Configuration Examples

```
    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
```

Configuration Examples

```
    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
```

Configuration Examples

```
!  
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  
!
```

Configuration Examples

```
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
```

Configuration Examples

```

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

```


Configuration Examples

```
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 udd link-fail-rpt
snmp-server enable traps udd 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
```

Configuration Examples

```

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 e2transparent
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

```

Configuration Examples

```
memory free low-watermark processor 63461
!
errdisable recovery cause uddl
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-miscabbling
errdisable recovery cause loopdetect
!
alarm-profile defaultPort
  alarm not-operating
  syslog not-operating
  notifies not-operating
!
enable secret 9 $9$WvAxOEesAznN.$mRkA6cTyFxVetsh9504kUwfrC8RwL6bTpBCrpk3iX.
!
username dna privilege 15 secret 9
$9$yD0gMvOokBX0RE$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
```

Configuration Examples

```
!  
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-V1101  
  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
```

Configuration Examples

```
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
```

Configuration Examples

```

!
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

```

Configuration Examples

```

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

```

Configuration Examples

```
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 DNA Center Day N Templates

Cisco DNA 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 DNA 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
```

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 DNA Center	Cisco Digital Network Architecture Center
CLI	Command line interface
CoS	Class of service
CTS	Cisco Trustsec
CURWB	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

Acronyms and Initialisms

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

Acronyms and Initialisms

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

Acronyms and Initialisms

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

Acronyms and Initialisms

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

Acronyms and Initialisms

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

Acronyms and Initialisms

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