Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1
Implementation Guide
April 2024
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.”

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

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

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

©2024 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
  VLAN Name ....................................................................................................................................... 9
  VLAN ID ........................................................................................................................................... 9
  Description ....................................................................................................................................... 9
  IP Addressing ................................................................................................................................... 9
  Solution Components ....................................................................................................................... 10

Chapter 3: Offshore Substation Network Implementation ..................................................................... 13
  Offshore Substation Core Network Implementation ......................................................................... 13
  Configuring FAN Ring Aggregation Switch Stack ............................................................................ 17
  Configuring OSS Infrastructure Network Access ............................................................................ 18
  OSS Network DMZ with Firewall ..................................................................................................... 19

Chapter 4: Farm Area Network Implementation ................................................................................... 25
  Configuring a Farm Area Network Ring ............................................................................................ 25
  Configuring a Turbine Area Network ............................................................................................... 26

Chapter 5: Implementing OSS Infrastructure Applications and Services .......................................... 28
  Cisco Cyber Vision Center Local Installation and Configuration ................................................... 28
  Cisco Stealthwatch Flow Collector Installation and Configuration ................................................. 28
  SCADA OPC-UA Server Installation and Configuration ................................................................... 29
  Cisco Cyber Vision Sensor installation on a 9300 Switch to Detect OPC-UA Traffic ......................... 32

Chapter 6: Implementing the Onshore Substation Network ................................................................. 38
  Onshore Substation (ONSS) Core Network Implementation ............................................................. 38
  Configuring ONSS Infrastructure Network Access ......................................................................... 40
  OSS Network DMZ with Firewall ..................................................................................................... 40

Chapter 7: Implementing Wireless Access Networks ......................................................................... 41
  Offshore Wind Farm Wi-Fi Implementation ..................................................................................... 42
  Operating the Wireless Network ....................................................................................................... 56
  Offshore Wind Farm URWB Implementation for SOV to OSS Connectivity ................................. 60

Chapter 8: Implementing WAN Backhaul and Control Center ........................................................... 78
  Implementing WAN Backhaul ........................................................................................................... 78
  Implementing Network Control Center and Application Services ................................................... 80
Chapter 9: Implementing Network Management and Automation

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

Chapter 10: Implementing Network Security and QoS

- Implementing Network Security
- Implementing QoS
- OSS QoS Configuration for OSS C9300 and C9500 Switches
- Implementing Multicast Traffic Support in an Offshore Substation

Chapter 11: Turbine Operator Network Implementation

- Turbine Operator Core Network Implementation
- TSN non-HA
- Configuring TSN HA
- Configuring Private VLANs
- Configuring MACSec
- Configuring certificate-based MACsec

Appendix A: Configuration Examples

- 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)

Appendix B: Cisco Catalyst Center Day N Templates

Appendix C: Turbine Operator Network Configuration

Acronyms and Initialisms
Preface

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

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

Document Objective and Scope

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

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


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

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

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

Audience

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

You should be familiar with networking protocols and IP routing, basic network security, and QoS. You also should have some understanding of server virtualization using hypervisor and the Cisco Renewable Energy Offshore Wind Farm Solution Architecture, which is described in Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide.
Chapter 1: Introduction

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

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

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

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

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

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

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

Implementation Flow

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

Figure 1-1: Wind Farm Solution Implementation Flow

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

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

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

- Implementation of an onshore substation (ONSS) network, which includes ONSS core Catalyst 9500 Series switches StackWise Virtual (SVL), an ONSS network access switch stack using Catalyst 9300 Series switches, and an ONSS DMZ network with a firewall.
- Implementation of WAN backhaul using Cisco Industrial 8340 Series rugged routers (IR8340) leveraging a Cisco SD-WAN deployment.
- Deployment of wind farm control center network components, including a WAN headend, a firewall, and applications such as Cisco Catalyst Center, Cisco ISE, Cyber Vision Global Center, SNA Manager, and so on.
- Deployment of wireless network components, such as WLC, access points, URWB radios, and so on for wind farm wireless network access.
- Implementation of network management services using Cisco Catalyst Center, and automated provisioning of wind farm network components using Cisco Catalyst Center workflows and day N template features.
- Configuration of network security components, such as Firepower, Cyber Vision network sensors, SNA NetFlow, and so on, and quality of service (QoS) provisioning in the OSS network.
Chapter 2: Solution Network Topology and Addressing

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

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

Solution Validation Topologies

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

- Offshore wind farm wired network topology with turbine area networks (TAN), a farm area network (FAN), an offshore substation (OSS), an onshore substation (ONSS), WAN backhaul, and a control center. See Figure 2-1, which shows the offshore wind farm wired network topology, including endpoints for various validated wind farm use cases.

- Offshore wind farm wireless network topology, consisting of Cisco WLCs and access points that provide Wi-Fi access for the OSS, FAN, and TAN, and a URWB network that provides wireless connectivity for SOVs back to the OSS. See Figure 2-2.
Figure 2-1: Wind Farm 1.1 Wired Network Topology

[Diagram showing network topology with various components and connections, including Control Center, ONSS, OSS, TAN1, TAN2, TAN3, and network elements such as Cisco Catalyst, RSE, AD/DHCP Servers, C3850 Stack, C9500 Stack, and more.]

Legend:
- L2: Offshore Substation
- L2 dot1q + REP: Onshore Substation
- L3: Farm Area Network
- Port Channel Bundle: Turbine Area Network
- BS: Base Switch
- NS: Nacelle Switch
- SOV: Service Operations Vehicle
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

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

### Table 2.2 VLANs used in Turbine operator network

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast_VLAN</td>
<td>5</td>
<td>Used for multicast</td>
</tr>
<tr>
<td>PVLAN_vlan</td>
<td>10</td>
<td>Primary VLAN (Used for OPC-UA)</td>
</tr>
<tr>
<td>Traffic-test</td>
<td>20</td>
<td>Traffic test VLAN</td>
</tr>
<tr>
<td>Isolated_vlan</td>
<td>101</td>
<td>Isolated secondary VLAN</td>
</tr>
<tr>
<td>Management_VLAN</td>
<td>111</td>
<td>Management VLAN</td>
</tr>
</tbody>
</table>

### 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.
Solution Network Topology and Addressing

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

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

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

<table>
<thead>
<tr>
<th>Hardware Model</th>
<th>Role in Offshore Wind Farm</th>
<th>Software or Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE3400-8P2S, IE3400-8T2S</td>
<td>Turbine nacelle switch, non-HA</td>
<td>17.11.1</td>
</tr>
<tr>
<td>IE3400-8P2S, IE3400-8T2S</td>
<td>Turbine nacelle switch, HA</td>
<td>17.11.1</td>
</tr>
<tr>
<td>IE3400-8P2S, IE3400-8T2S</td>
<td>Turbine base switch</td>
<td>17.11.1</td>
</tr>
<tr>
<td>C9300-24UX</td>
<td>Farm area aggregation</td>
<td>17.11.1</td>
</tr>
<tr>
<td>C9500-16X</td>
<td>OSS core switch, HA</td>
<td>17.11.1</td>
</tr>
<tr>
<td>C9300-24UX</td>
<td>OSS IT network access switch</td>
<td>17.11.1</td>
</tr>
<tr>
<td>C3850-24UX</td>
<td>ONSS core switch</td>
<td>16.12.1</td>
</tr>
<tr>
<td>Firepower 2140</td>
<td>OSS and ONSS DMZ firewall</td>
<td>7.0.1</td>
</tr>
<tr>
<td>Firepower Management Center (FMC)</td>
<td>Firewall management application</td>
<td>7.0.1</td>
</tr>
<tr>
<td>IR8340</td>
<td>ONSS WAN edge router</td>
<td>17.11.1</td>
</tr>
<tr>
<td>DN2-HW-APL</td>
<td>Cisco Catalyst Center Network Management Appliance</td>
<td>2.3.6.0</td>
</tr>
<tr>
<td>UCS-C240-M5S</td>
<td>Unified Computing System (UCS)</td>
<td>3.1.3c</td>
</tr>
<tr>
<td>Cisco ISE Virtual Appliance</td>
<td>AAA server</td>
<td>3.2</td>
</tr>
<tr>
<td>IoX Sensor App</td>
<td>Cyber Vision network sensors</td>
<td>4.1.2</td>
</tr>
<tr>
<td>Cisco Cyber Vision Center Global and local</td>
<td>OT security dashboard</td>
<td>4.1.2</td>
</tr>
<tr>
<td>C9800-L-C-K9</td>
<td>Wireless LAN controller</td>
<td>17.11.1</td>
</tr>
<tr>
<td>IW6300-AP</td>
<td>Cisco IW6300 ruggedized AP for Wi-Fi access</td>
<td>17.11.1</td>
</tr>
<tr>
<td>AIR-AP9120</td>
<td>Cisco AP for Wi-Fi access</td>
<td>17.11.1</td>
</tr>
<tr>
<td>URWB FM3500 and FM4500</td>
<td>URWB mesh point</td>
<td>9.4</td>
</tr>
<tr>
<td>URWB FM1000 Gateway</td>
<td>URWB mesh gateway</td>
<td>1.6.0</td>
</tr>
<tr>
<td>URWB FM-Monitor VM</td>
<td>URWB FM-Monitor</td>
<td>1.0.1</td>
</tr>
<tr>
<td>Cisco Secure Network Analytics (Stealthwatch)</td>
<td>IT and OT security management</td>
<td>7.4.1</td>
</tr>
<tr>
<td>ASR-1002-HX</td>
<td>Control center headend router</td>
<td>17.3.4a</td>
</tr>
<tr>
<td>Cisco SD-WAN vManage, vSmart, vBond</td>
<td>WAN management</td>
<td>20.8.1</td>
</tr>
</tbody>
</table>
Table 2-4: Third-party Hardware and Software Validated in this Wind Farm Solution

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

**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

![Diagram showing DAD and SVL links for 9500 SVL](image)

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

![Workflow diagram](image)

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):

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

1. Perform these actions to configure SVL:
   
a. Reassign the switch numbers of the two switches to switch numbers 1 and 2, and assign priorities as follows:
      
      **9500-1:**
      Switch 1 priority 15
      
      **9500-2:**
      switch 1 renumber 2
      switch 1 priority
   
b. Complete the following SVL configuration on each of the switches:
      
      **9500-1:**
      
      ```
      stackwise-virtual
      domain 2
      
      interface TenGigabitEthernet1/1/1
      stackwise-virtual link 1
      
      interface TenGigabitEthernet1/1/5
      stackwise-virtual dual-active-detection
      ```
      
      **9500-2:**
      
      ```
      interface TenGigabitEthernet2/1/1
      stackwise-virtual link 1
      
      interface TenGigabitEthernet2/1/5
      stackwise-virtual dual-active-detection
      ```
   
c. Reload the two switches to cause the SVL configuration to take effect.
   
d. Enter the following command on each 9500 switch to verify that switches are now in SVL mode:
      
      ```
      show stackwise-virtual
      ```
      The command output should show that the two switches are in Active Standby mode and show their configured switch numbers.

2. Configure layer 3 for 9500 SVL:
   
a. Configure a switched virtual interface (SVI) for management VLAN 101, assign an IP address to it, and forwarding VRF in Management_VRF:
      
      ```
      hostname WF-OSS-C9500
      vlan 100
      name OSS_INFRA_VLAN
      
      vlan 101
      name OSS_NET_MGMT
      
      interface Vlan101
      vrf forwarding Management_VRF
      ip address 10.10.101.1 255.255.255.0
      
      vrf definition Management_VRF
      rd 100:1
      
      address-family ipv4
      route-target export 100:1
      route-target import 100:1
      route-target export 100:1
      stitching
      route-target import 100:1
      stitching
      exit-address-family
      
      address-family ipv6
      route-target export 100:1
      ```
Offshore Substation Network Implementation

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

b. Configure OSPF routing for underlay network reachability between OSS and ONSS core switches:
   router ospf 1
   router-id 192.168.5.2
   network 172.16.1.0 0.0.0.3 area 0
   network 192.168.2.2 0.0.0.0 area 0
   network 192.168.5.2 0.0.0.0 area 0
   network 192.168.7.2 0.0.0.0 area 0

c. Configure the core face VLAN on the C9500 SVL VTEP:
   !
   vlan configuration 11
   member vni 5000
   !
d. Configure Switch Virtual Interface (SVI) for the core facing VLAN:
   interface Vlan11
   vrf forwarding Management_VRF
   ip unnumbered Loopback0
   no autostate

e. Configure Switch Virtual Interface (SVI) for the access facing VLAN:
   interface Vlan100
   vrf forwarding Management_VRF
   ip address 10.10.100.1 255.255.255.0
   ip helper-address 192.168.6.2
   !
f. Configure loopback interface on the VTEP:
   interface Loopback0
   ip address 192.168.5.2 255.255.255.255
   !
g. Configure NVE interface on the VTEP:
   interface nve1
   no ip address
   source-interface Loopback0
   host-reachability protocol bgp
   member vni 5000 vrf Management_VRF
   !
h. Configure BGP with IPv4 or IPv6 or both address families on the VTEP:
   router bgp 1
   bgp log-neighbor-changes
   bgp update-delay 1
   bgp graceful-restart
   no bgp default ipv4-unicast
   neighbor 192.168.5.1 remote-as 1
   neighbor 192.168.5.1 update-source Loopback0
   !
address-family ipv4
exit-address-family
!
address-family l2vpn evpn
neighbor 192.168.5.1 activate
neighbor 192.168.5.1 send-community both
exit-address-family
!
address-family ipv4 vrf Management_VRF
advertise l2vpn evpn
redistribute static
redistribute connected
exit-address-family
!
address-family ipv6 vrf Management_VRF
redistribute connected
redistribute static
advertise l2vpn evpn
exit-address-family
!

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

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

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

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

| Network Distinguisher: 100:1 (default for vrf Management_VRF) |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| Route           | Next Hop        | Metric | LocPrf | Weight | Path |
| *> [5][100:1][0][16][172.114.0.0]/17 | 0.0.0.0 | 0 | 32768 | ? |
| *> [5][100:1][0][24][10.10.1.0]/17 | 0.0.0.0 | 32768 | ? |
| *> [5][100:1][0][24][10.10.100.0]/17 | 0.0.0.0 | 32768 | ? |
| * i [5][100:1][0][24][10.10.201.0]/17 | 192.168.5.1 | 0 | 100 | 0 |
Refer to the following URL for more details on EVPN VXLAN BGP Core routing implementation steps network VTEPs:

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.
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:

2. Configure layer 3 for the 9300 switch stack:
   a. Configure the management SVI interface as Vlan101 and assign an IP address to Vlan101:
      ```
      hostname WF-OSS-C9300Agg
      vlan 101
      interface Vlan101
      ip address 10.10.101.13 255.255.255.0
      ```
   b. Configure the `ip routing` command and then configure the default route to point to the 9500 SVL:
      ```
      ip routing
      ip route 0.0.0.0 0.0.0.0 10.10.101.1
      ```

3. Configure Layer 2 for the Cisco Catalyst 9300 switch stack:
   a. Configure port-channels and trunk port on links going to the Catalyst 9500 SVL:
      ```
      interface TenGigabitEthernet1/1/3
      description ##ConnectionTo9500##
      channel-group 1 mode desirable
      ```
      ```
      interface TenGigabitEthernet2/1/3
      description ##ConnectionTo9500##
      channel-group 1 mode desirable
      ```
      ```
      interface Port-channel1
      switchport mode trunk
      ```
   b. Enter the following command to verify that the port-channel is up and that the trunk port is created:
      ```
      show etherchannel summary
      ```

Configuring OSS Infrastructure Network Access

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

1. Perform these actions to complete the layer 3 configuration for the C9300 stack from the CLI:
   a. Configure the management VLAN and the SVI in Vlan101:
      ```
      hostname OSS-C9300-Access
      vlan 101
      interface Vlan101
      ip address 10.10.101.5 255.255.255.0
      ```
b. Configure the Catalyst 9500 SVL as the default gateway:
   ip default-gateway 10.10.101.1
!

2. Perform these actions to configure layer 2 for the C9300 stack from the CLI:
   a. Configure port-channels and the trunk port on links that are connected to the Catalyst 9500 SVL:
      interface TenGigabitEthernet1/1/1
description ##ConnectionTo9500##
   channel-group 1 mode desirable
!
   interface TenGigabitEthernet2/1/1
description ##ConnectionTo9500##
   channel-group 1 mode desirable
!
   interface Port-channel1
   switchport mode trunk
   
   b. Enter the following command to verify that the port-channel is up and that the trunk port is created:
      show etherchannel summary
      --------Output Omitted---------
      Number of channel-groups in use: 1
      Number of aggregators:         1
      Group Port-channel Protocol Ports
      + + +
      1 Po1 (SU) PAgP Te1/1/1 (P) Te2/1/1 (P)
      
      show interfaces trunk
      Port   Mode     Encapsulation Status Native vlan
      Pol1   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:

v70/introduction_to_the_cisco_firepower_system.html
After the FMC is installed as a virtual appliance as described in “Getting Started With Firepower,” open the FMC console and configure the management IP address (which should have reachability to the FPR management IP address), configure the default gateway, and log in credentials.

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

Firepower Installation and High Availability Configuration

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

A third-party turbine vendor SCADA network connects to the OSS DMZ network through a firewall, as described in Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide:


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:
   

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:


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:

2. Perform the following steps to configure Firepower interfaces:

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

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

Figure 3-6: Configuring Interfaces

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

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

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

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

b. Click the Routing tab.

c. Click Static Route.

d. Click Add Route.
Offshore Substation Network Implementation

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.

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:


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

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

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.
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

Click Deploy.

g. Click Deploy.

Figure 3-13: Rules Configured Under Access Control Policy
Chapter 4: Farm Area Network Implementation

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

This chapter includes the following topics:

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

Configuring a Farm Area Network Ring

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

![Figure 4-1: FAN Ring Bring-up Workflow]

FAN Ring Topology and REP Ring Configuration

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

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

A sample configuration for a 3400 switch is as follows:

```
hostname FAN-BS1
vlan 101
name Management_vlan
vlan 105
name REP_ADMIN_VLAN
rep admin vlan 105
interface Vlan101
ip address dhcp
interface range gi 1/1-2
switchport mode trunk
```

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

```bash
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:

## 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:

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

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

### Configuring TAN with High Availability and REP Subtended Ring

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

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

#### TAN2 Ring Configuration

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

- **Base switch configuration:**
  ```bash
  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:**
  ```bash
  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.
  ```bash
  FAN-BS4#conf t
  Int range Gi 2/1
  Rep segment 3 edge
  rep stcn segment 1
  FAN-BS3#conf t
  ```
Int range Gi 2/1
Rep segment 3 edge
rep stcn segment 1
TAN3-BS1#conf t
Rep admin vlan 105
Int range gi 1/1-1/2
Rep segment 3
Chapter 5: Implementing OSS Infrastructure Applications and Services

This chapter includes the following topics:
- Cisco Cyber Vision Center Local Installation and Configuration
- Cisco Stealthwatch Flow Collector Installation and Configuration
- SCADA OPC-UA Server Installation and Configuration
- Cisco Cyber Vision Sensor installation on a 9300 Switch to Detect OPC-UA Traffic

Cisco Cyber Vision Center Local Installation and Configuration

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

Cisco Cyber Vision Center Installation

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

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

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

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


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:

Cisco Stealthwatch Flow Collector Installation and Configuration

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

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

For more detailed information about Stealthwatch design, see “Cisco Secure Network Analytics (Stealthwatch)” in Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide:
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:


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


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:


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

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>936</td>
<td>125.913849</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>140</td>
<td>Hello message</td>
</tr>
<tr>
<td>937</td>
<td>125.968843</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>82</td>
<td>Acknowledge message</td>
</tr>
<tr>
<td>938</td>
<td>135.947761</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>186</td>
<td>OpenSecureChannel message: OpenSecureChannelRequest</td>
</tr>
<tr>
<td>939</td>
<td>135.957395</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>189</td>
<td>OpenSecureChannel message: OpenSecureChannelResponse</td>
</tr>
<tr>
<td>940</td>
<td>135.959055</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>1382</td>
<td>UA Secure Conversation Message: CreateSessionRequest</td>
</tr>
<tr>
<td>941</td>
<td>136.891659</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>1354</td>
<td>UA Secure Conversation Message: CreateSessionResponse (Message Reassembled)</td>
</tr>
<tr>
<td>942</td>
<td>136.892228</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>938</td>
<td>UA Secure Conversation Message: CreateSessionResponse (Message Reassembled)</td>
</tr>
<tr>
<td>943</td>
<td>136.893731</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>203</td>
<td>UA Secure Conversation Message: ActivateSessionRequest</td>
</tr>
<tr>
<td>944</td>
<td>136.895498</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>159</td>
<td>UA Secure Conversation Message: ActivateSessionResponse</td>
</tr>
<tr>
<td>945</td>
<td>136.896798</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>170</td>
<td>UA Secure Conversation Message: CreateSubscriptionRequest</td>
</tr>
<tr>
<td>946</td>
<td>136.125188</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>126</td>
<td>UA Secure Conversation Message: CreateSubscriptionResponse</td>
</tr>
<tr>
<td>947</td>
<td>136.125839</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>412</td>
<td>UA Secure Conversation Message: CreateMonitoredItemsRequest</td>
</tr>
<tr>
<td>948</td>
<td>136.128914</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>252</td>
<td>UA Secure Conversation Message: CreateMonitoredItemsResponse</td>
</tr>
<tr>
<td>949</td>
<td>136.139478</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>182</td>
<td>UA Secure Conversation Message: ReadRequest</td>
</tr>
<tr>
<td>950</td>
<td>136.146802</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>491</td>
<td>UA Secure Conversation Message: ReadResponse</td>
</tr>
<tr>
<td>951</td>
<td>136.146468</td>
<td>10.10.100.5</td>
<td>10.10.100.11</td>
<td>OPC-UA</td>
<td>182</td>
<td>UA Secure Conversation Message: ReadRequest</td>
</tr>
<tr>
<td>952</td>
<td>136.150277</td>
<td>10.10.100.11</td>
<td>10.10.100.5</td>
<td>OPC-UA</td>
<td>256</td>
<td>UA Secure Conversation Message: ReadResponse</td>
</tr>
</tbody>
</table>

### 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**

![Security Modes and Policies](image1)

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**

![Client Fetching Data](image2)

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.
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*.
Implementing OSS Infrastructure Applications and Services

Guide:

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: DSS-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

DSS-C9300-Access#

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

1. Configure the following IP addresses on the 9300 switch to bring up the Cyber Vision sensor application and integrate the switch with CVC:
   - CVC Admin Interface (eth0)
   - Collection interface (eth1)
   - Collection network gateway
   - NTP

2. Configure the IP addresses in Cisco Cyber Vision as shown in Figure 5-9 (sample IP addresses shown).

   Figure 5-9: Cyber Vision Configuration Parameters

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: | 10.10.100.4 |
| Capture IP address: | 169.254.1.2 |
| Capture VLAN number: | 2580 |
| Collection prefix length: | 30 |
| Collection gateway: | 10.10.101.1 |
| Disk size: | Use up to 15GB |

| Device port: | 443 |
| Capture prefix length: | 30 |
| Collection IP address: | 10.10.101.5 |
| Collection VLAN number: | 101 |
| Use global credentials: | No |

3. Enable iox on the C-9300 switch:

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

n_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:
   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:
Implementing OSS Infrastructure Applications and Services


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

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

---

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

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

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

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

   ```
   OSS-C9300-Access#app-hosting connect appid ccv_sensor_iox_x86_64 session
   sh-5.0# cd /iox_data/etc/flow/
   sh-5.0# vi config.yaml
gopacket:
   ```
2. Enter the following command to reload the 9300 switch:

   flowctl reload

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

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

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

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

Figure 5-13 shows a more detailed view the OPC-UA traffic flow on the Cyber Vision Center dashboard.
Implementing OSS Infrastructure Applications and Services

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:

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

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

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

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

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

Interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.5.2</td>
<td>0 100 0</td>
<td>0 100 0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network VNI Type Peer-IP RMAC/Num_RTs eVNI state flags UP time

<table>
<thead>
<tr>
<th>Network</th>
<th>VNI</th>
<th>Type</th>
<th>Peer-IP</th>
<th>RMAC/Num_RTs</th>
<th>eVNI</th>
<th>state</th>
<th>flags</th>
<th>UP time</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve1</td>
<td>5000</td>
<td>L3CP</td>
<td>192.168.5.2</td>
<td>a4b2.392a.9554</td>
<td>5000</td>
<td>UP</td>
<td>A/M/4</td>
<td>3w6d</td>
</tr>
</tbody>
</table>

WF-ONSS-9500#show bgp l2vpn evpn all
BGP table version is 67, local router ID is 192.168.7.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-path, c RIB-compressed, t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

WF-ONSS-9500#ping vrf Management_VRF 10.10.100.1 source vlan 201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.201.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WF-ONSS-9500#

Configuring ONSS Infrastructure Network Access

Configure the ONSS C9300 stack by following the steps in Configuring OSS Infrastructure Network Access.
Similarly, configure C9300 aggregation, if required, by following the steps in Configuring FAN Ring Aggregation Switch Stack.

OSS Network DMZ with Firewall

Cisco Next Generation Firewall (NGFW) Implementation

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

Turbine Vendor OPC-UA client

The OPC-UA client connects to the OPC-UA server by using either Open, a username and password, or AES-128/256 security keys.
Chapter 7: Implementing Wireless Access Networks

This chapter includes the following topics:

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

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

Figure 7-1: Offshore Wind Farm Wireless Architecture
Offshore Wind Farm Wi-Fi Implementation

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

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

Implementing Wireless Access Networks

Configuring C9800 WLC High Availability from Cisco Catalyst Center

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

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

1. From the main Cisco Catalyst Center dashboard choose Provision.
   
   The main provisioning screen appears, which displays the devices within the inventory. By default, the Focus: is set for Inventory.

2. Locate and check the check box next to the Catalyst 9800-40 WLC, which will be the primary of the HA SSO WLC pair.

3. From the drop-down menu under Actions, choose Provision > Configure WLC HA.
Implementing Wireless Access Networks

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

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

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

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

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

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

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

An example is shown in Figure 7-4.
7. Verify the redundancy status on the WLC by choosing Monitoring > General > System.
An example is shown in Figure 7-5. You also can monitor the status on the C9800 WLC CLI by executing the `show redundancy` command as shown in Figure 7-6.

Figure 7-5: Verifying WLC High Availability Status on the WLC Monitoring Page
Figure 7-6: Verifying High Availability Status from the C9800 CLI

```
MP-AC-9800(show redundancy
Redundant System Information:
Available system uptime = 4 days, 2 hours, 31 minutes
Switchovers system experienced = 2
Standby failures = 0
Last swtichover 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 = 10 minutes
Image Version = Cisco IOS Software [Dublin], C9800 Software (C9800_IOS9XE-K9), Experimental Version 17.11.2023#185:BB4252 [BLD_V1711_THROTTLE_LATEST_2023185_081642/ncobackup/mcpre/s2c-build-ws 185]
Compiled Thu 05-Jan-23 08:42 by mcp
BOOT = bootflash:packages.conf,12;
CONFIG_FILE =
Configuration register = 0x1b2
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_IOS9XE-K9), Experimental Version 17.11.2023#185:BB4252 [BLD_V1711_THROTTLE_LATEST_2023185_081642/ncobackup/mcpre/s2c-build-ws 185]
Compiled Thu 05-Jan-23 08:42 by mcp
BOOT = bootflash:packages.conf,12;
CONFIG_FILE =
Configuration register = 0x1b2
```

Configuring Wi-Fi APs using Cisco Catalyst Center

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

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

Figure 7-7: Select APs to Provision

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

Figure 7-8: Assign Each AP to a Site

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Devices</th>
<th>AP Zone Name</th>
<th>RF Profile</th>
<th>SSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOC243919K1</td>
<td>AP3C57.31C5.7EF4</td>
<td>Not Applicable</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FJC25251V6Q</td>
<td>AP3C57.31C5.ADA8</td>
<td>Not Applicable</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FCW2415P0ET</td>
<td>AP2416.9DDE.DB58</td>
<td>Not Applicable</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FCW2350PKCW</td>
<td>APA084.3965.BEA0</td>
<td>Not Applicable</td>
<td>LOW</td>
<td>2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Device Name</th>
<th>RF Profile</th>
<th>SSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOC243919K1</td>
<td>AP3C57.31C5.7EF4</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FJC25251V6Q</td>
<td>AP3C57.31C5.ADA8</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FCW2415P0ET</td>
<td>AP2416.9DDE.DB58</td>
<td>LOW</td>
<td>2</td>
</tr>
<tr>
<td>FCW2350PKCW</td>
<td>APA084.3965.BEA0</td>
<td>LOW</td>
<td>2</td>
</tr>
</tbody>
</table>

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

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

### Figure 7-11: Warning Pop-up Window

8. Click **Yes**.

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

9. Navigate to the Cisco Catalyst Center Task Status page to monitor the status of the “Provision APs” task.
Figure 7-12: Provision APs Task Status page

Upgrading C9800 WLC and AP Images Using Cisco Catalyst Center

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

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

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

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Version</th>
<th>Devices</th>
<th>Advisories</th>
<th>Golden Image</th>
<th>Device Roles &amp; Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9800-L-universalk9_wlc.17.10.01.SPA.bin</td>
<td>17.10.01.0.1444 (Latest) Add On (N/A)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

2. **Choose** [Provision > Inventory](#). Cisco Catalyst Center flags the WLC as non-compliant due to its current image not matching the Golden Image.

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

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

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

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

3. **Navigate to the Cisco Catalyst Center Inventory** page and check the check box for the C9800 WLC device to upgrade.
4. Review the current image on the C9800 WLC and the image being upgraded to, then click **Next**.

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

- **Device**: WF-WLC-9800.windfarm.com
- **From Image**: C9800-L-universal9_wlc.17.09.01.SPA.bin
- **To Image**: C9800-L-universal9_wlc.17.10.01.SPA.bin
- **Comment**: Update Readiness Report

5. Configure the software distribution checks, then click **Next**.
Figure 7-18: Software Distribution Checks

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

Figure 7-19: Image Activation Configuration

Configure the software distribution and activation tasks, then click **Next**.
Figure 7-20: Schedule Update and Clean Up

8. Review the Image Upgrade Summary, then click Submit.
9. Monitor the image upgrade process on Cisco Catalyst Center and verify that it completes successfully.

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*

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

*Figure 7-24: Account Created Window*

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

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

Cisco Catalyst Center Wireless Assurance

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

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

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

DNA Assurance also helps monitor the status of the AAA server (ISE server) and DHCP server (Active Directory) on the Overall Health Dashboard.
Defective AP Replacement (RMA) using Cisco Catalyst Center

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

Replace a Faulty Access Point

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

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

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

The RMA process begins.
11. To monitor the replacement status, under What’s Next, click Monitor Replacement Status.

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

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

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

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

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

If the faulty AP replacement fails, then the Replace Status column shows an error message with the reason for the failure. You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.

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

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

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

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

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

Troubleshooting Wireless Client Authentication

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

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

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

Offshore Wind Farm URWB Implementation for SOV to OSS Connectivity

This section provides sample configuration snippets for the offshore wind farm URWB deployment.
This section provides samples of configurations to apply to the OSS wired network to support a URWB wireless deployment for SOV to OSS wireless backhaul connectivity.

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

### C9500 Core-Stack

```text
! Vlan 106
  name URWB-mgmt
! interface Vlan106
  ip address 10.10.106.1 255.255.255.0
! interface Port-channel1
  description Connected to OSS Access 9300 Stack
  switchport mode trunk
! interface Port-channel2
  description Connected to FAN 9300 Stack
  switchport mode trunk
! interface TwentyFiveGigE1/0/25
  switchport mode trunk
  channel-group 1 mode active
```
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 URWB-Mgmt
! interface Port-channel1
    description Connected to OSS-Core-C9500 Stack
    switchport mode trunk
! interface GigabitEthernet1/0/1
    description connected to OSS Radio 1
    switchport trunk allowed vlan 106, 217
    switchport trunk native vlan 106
    switchport mode trunk!

interface GigabitEthernet1/0/2
    description connected to OSS Radio 2
    switchport trunk allowed vlan 106, 217
    switchport trunk native vlan 106
    switchport mode trunk!

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

switchport trunk native vlan 106
switchport mode trunk!
!
interface GigabitEthernet2/0/2
description connected to OSS Radio 4
switchport trunk allowed vlan 106, 217
switchport trunk native vlan 106
switchport mode trunk!
!
interface TenGigabitEthernet2/1/7
description Connected to OSS-Core-C9500 Stack
switchport mode trunk
channel-group 1 mode active
!
interface TenGigabitEthernet2/1/8
description Connected to OSS-Core-C9500 Stack
switchport mode trunk
channel-group 1 mode active
!

C9300 Access Stack

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

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

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

OSS Infrastructure IW9167E/IEC6400 Mesh End

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

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

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

```
# GENERAL CONFIG
Device name: OSS-9167ME-1
IP: 10.10.106.10
Netmask: 255.255.255.0
Gateway: 10.10.106.1
Nameservers:
Mesh End mode
# FLUIDITY CONFIG
Fluidity enabled
Fluidity interface: none
Infrastructure mode
Backhaul-check: handoff-inhibition
Mesh-end backhaul-check: handoff-inhibition
Color: enabled, current: 0
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled
# MPLS CONFIG
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: disabled (broadcasting allowed)
reduce-broadcast: disabled
pwlist: all
```
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover: enabled
Node failover timeout: 0 ms
L2TP WAN update delay: disabled
Preemption delay: 70 s
Virtual IP: 0.0.0.0
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255 local dynamic
MPLS tunnels:
  ldp_id 519374131 debug 0 auto_pw 1
  local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0 }
lsps
VLAN status: enabled
Management VID: 106
Native VID: 217

########### ADVANCED CONFIG ###########
Gratuitous-arp: enabled
  Delay: 150 ms
QoS: enabled
CoS map:
  | | | | | | | |
  [ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
go-shaping disabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500

OSS Infrastructure IW9167E Mesh Point

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

########### GENERAL CONFIG ###########
Device name: OSS-9167-1
IP: 10.10.106.11
Implementing Wireless Access Networks

netmask: 255.255.255.0
Gateway: 10.10.106.1
Nameservers:
Mesh Point mode

################ WIRELESS CONFIG ################
SLOT 1 Config
Interface: enabled
Mode: fluidity

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

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

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

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

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

SLOT 2 Config
Interface: disabled
Mode: fluidity

Frequency: 5300 MHz
Channel: 60
Channel width: 40 MHz
Antenna number: 2
TX power level: 7
TX power: 2 dBm
Implementing Wireless Access Networks

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

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

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

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

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

Fluidity enabled
Fluidity interface: 1
Infrastructure mode
Backhaul-check: handoff-inhibition
Mesh-end backhaul-check: handoff-inhibition
Color: enabled, current: 0
Network type: flat (layer 2)
Warmup time: 30000 ms
Wireless timeout: 800 ms
Wireless fastdrop: disabled
Frequency scan: disabled
Large network optimization: disabled
Routes: backhaul
Primary-pseudowire enforcement: disabled
Max number of clients: unlimited
DoP settings: limit 0, client 10, bias 0
FMQuadro telemetry: enabled

MPLS enabled
Layer 2
unicast-flood: enabled (limited rate)
ar-p-unicast: enabled (broadcasting not allowed)
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover is disabled
ARP limit: rate 0 grace 30000 block 0
Multicast rules and static routes:
224.0.0.10/255.255.255.255 -> 5.255.255.255 dynamic
MPLS tunnels:
ldp_id 1570886916 debug 0 auto_pw 1
Implementing Wireless Access Networks

local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { } 
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true 
static_pws { 0.0.0.0 }

lsps 4

######################## VLAN CONFIG #########################
VLAN status: enabled
Management VID: 106
Native VID: 217

######################## ADVANCED CONFIG #########################
Gratuitous-arp: enabled
    Delay: 150 ms
QoS: enabled
CoS map:
    0 1 2 3 4 5 6 7
   | | | | | | | |
[ 0 1 2 3 4 5 6 7 ]
qos-shaping disabled
qos-8021p disabled
Radius: disabled
blocklist size 0
L2TP is disabled
SNMP: disabled
Configured MTU: 1530
Current WIRED0 MTU: 1500

Service Operations Vessel Network

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

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

IE3X00-1

```plaintext
! vlan 106
  name URWB-Mgmt
! spanning-tree vlan 106 priority 4096
! interface GigabitEthernet1/3
  description V-9167E-1
  switchport trunk allowed
  vlan 106, 217
  switchport trunk native vlan
  106
  switchport mode trunk!
  spanning-tree portfast
  ! interface GigabitEthernet1/4
  description connected to IR1101-1 gig0/0/5
  switchport trunk allowed vlan 106
  switchport mode trunk!
  ! interface GigabitEthernet1/10
  description connected to IE3200-2 gig1/10
  switchport trunk allowed vlan 106
  switchport mode trunk!
```
IE3X00-2

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

IR1101-1

! vlan 106,200-201
! interface GigabitEthernet0/0/0  
  description connected to C9300 gig2/0/1  
  switchport  
  switchport trunk allowed vlan 106,200,201  
  switchport mode trunk  
  media-type rj45
! interface GigabitEthernet0/0/5  
  description connected to IE3200-1 gig1/4  
  switchport trunk allowed vlan 106
  switchport mode trunk
! interface Vlan100  
  ip address 10.10.10.101 255.255.255.255.0
! 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

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

**URWB Configuration**

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

**Service Operations Vessel IW9167E-1 (Mobile)**

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

################ WIRELESS CONFIG ################
SLOT 1 Config
Interface: enabled
Mode: fluidity
Frequency: 5180 MHz
Channel: 36
Channel width: 40 MHz
Antenna number: 2
TX power level: 6
TX power: 3 dBm
Antenna gain: 7 dBi
Maximum tx mcs: 9
High-efficiency: enabled
Maximum tx nss: 2
RTS protection: 512
guard-interval: 800 ns
ampdu max length: 255
distance: 3000 m

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

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

Passphrase: windfarm
AES encryption: enabled
AES key-control: disabled
Key rotation: disabled
Key rotation timeout: 0(second)
```
Cisco Offshore Wind Farm Solution Implementation Guide

Implementing Wireless Access Networks

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFS region</td>
<td>B</td>
</tr>
<tr>
<td>DFS radar role</td>
<td>auto</td>
</tr>
<tr>
<td>Radar detected</td>
<td>0</td>
</tr>
<tr>
<td>Indoor deployment</td>
<td>disable</td>
</tr>
<tr>
<td>Rx-SOP Threshold</td>
<td>0 dBm(AUTO)</td>
</tr>
</tbody>
</table>

Fluidity enabled

Fluidity interface: 1, 2

Vehicle ID: automatic, current ID: 100017752 current role: mobile primary unit

Handoff logic: standard

Handoff hysteresis high threshold: 6

Handoff hysteresis low threshold: 3

RSSI low/high zones threshold: 35

Color: enabled, current: 0

Color min RSSI threshold: 20

Network type: flat (layer 2)

Warmup time: 30000 ms

Wireless timeout: 800 ms

Wireless fastdrop: disabled

Frequency scan: disabled

Large network optimization: disabled

Routes: backhaul

Primary-pseudowire enforcement: disabled

Max number of clients: unlimited

DoP settings: limit 0, client 10, bias 0

FMQuadro telemetry: enabled

MPLS tunnels:

LDP_ID 312290134 debug 0 auto_pw 1
local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }

Cluster ID: disabled

Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block

MPLS fast failover is enabled

Node failover timeout: 0 ms

L2TP WAN update delay: disabled

Preemption delay: 100 s

Virtual IP: 10.10.10.10

ARP limit: rate 0 grace 30000 block 0

Multicast rules and static routes:

224.0.0.10/255.255.255.255 -> 5.255.255.255 dynamic

MPLS tunnels:

lsps 4

VLAN status: enabled

Management VID: 106

Native VID: 217

Gratuitous-arp: enabled

Delay: 150 ms

QoS: enabled

CoS map:

0 1 2 3 4 5 6 7
||| | | | |
[ 0 1 2 3 4 5 6 7 ]

qos-shaping disabled

qos-8021p enabled

Radius: disabled

blocklist size 0

L2TP is disabled

SNMP: disabled

Configured MTU: 1530

Current WIRED0 MTU: 1500

LICENSED
Service Operations Vessel IW9167E -2(Mobile)

GENERAL CONFIG

Device name: V-9167E-2
IP: 10.10.106.22
netmask: 255.255.255.0
Gateway: 10.10.106.1
Nameservers:

WIRELESS CONFIG

SLOT 1 Config

Interface: enabled
Mode: fluidity

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

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

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

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

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

FLUIDITY CONFIG

Fluidity enabled
Fluidity interface: 1, 2
Vehicle ID: automatic, current ID: 100017753 current role: mobile secondary unit
Handoff logic: standard
Handoff hysteresis high threshold: 6
Handoff hysteresis low threshold: 3
Rssi low/high zones threshold: 35
Color: enabled, current: 0
Implementing Wireless Access Networks

- Color min RSSI threshold: 20
- Network type: flat (layer 2)
- Warmup time: 30000 ms
- Wireless timeout: 800 ms
- Wireless fastdrop: disabled
- Frequency scan: disabled
- Large network optimization: disabled
- Routes: backhaul
- Primary-pseudowire enforcement: disabled
- Max number of clients: unlimited
- DoP settings: limit 0, client 10, bias 0
- PMQuadro telemetry: enabled

##### MPLS CONFIG #######

- layer 2
- unicast-flood: enabled (limited rate)
- arp-unicast: enabled (broadcasting not allowed)
- reduce-broadcast: enabled
- pwlist: all
- Cluster ID: disabled
- Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
- MPLS fast failover is enabled
- Node failover timeout: 0 ms
- L2TP WAN update delay: disabled
- Preemption delay: 100 s
- Virtual IP: 10.10.10.10
- ARP limit: rate 0 grace 30000 block 0
- Multicast rules and static routes:
  - 224.0.0.10/255.255.255.255 -> 5.255.255.255 dynamic
- MPLS tunnels:
  - ldp_id 312290134 debug 0 auto_pw 1
  - local_gw 5.246.39.136 global_gw 0.0.0.0 pwlist { }
- mobility true vehicle_id 100017752 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0 }
- lsps 4

##### VLAN CONFIG #######

- VLAN status: enabled
- Management VID: 106
- Native VID: 217
- CoS map:
  - { 0 1 2 3 4 5 6 7 }
  - qos-shaping disabled
  - qos-8021p enabled
- Radius: disabled
- blocklist size 0
- L2TP is disabled
- SNMP: disabled
- Configured MTU: 1530
- Current WIRED0 MTU: 1500

**IW Monitor**

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

Figure 7-38 IW Monitor Dashboard

Figure 7-39 IW Monitor Topology View

For complete IW Monitor Installation steps please see the IW Monitor User guide.
Implementing Wireless Access Networks

**IW Service on OPERATIONS DASHBOARD**

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

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

- **Online Configuration method:**
  - Automated template provisioning using the Operations Dashboard to push pre built configuration templates to IP reachable URWB devices.

- **Offline Configuration method:**
  - Operations dashboard generated configuration files, to upload locally to URWB devices.
  - Local manual configuration via the local URWB device gui.

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

**Note:** For in depth IW service configuration guidance please see Operations Dashboard.
Chapter 8: Implementing WAN Backhaul and Control Center

This chapter includes the following topics:

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

Implementing WAN Backhaul

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

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

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

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

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

VRF Services in the Substation Router

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

```plaintext
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
```

78
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:

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:

79
Implementing WAN Backhaul and Control Center

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

To configure this link:

1. Configure the active router as shown in the following example.
   This example assumes that VLAN 2001 is enabled for the management_VRF.
   ```
   Interface Vlan 2001
   ip address 10.201.201.2 255.255.255.0
   standby 1 ip 10.201.201.100
   standby 1 priority 10
   standby 1 preempt
   standby 1 track 100 decrement 10
   ```

2. Configure the standby router as shown in the following example:
   ```
   Interface Vlan 2001
   ip address 10.201.201.3 255.255.255.0
   standby 1 ip 10.201.201.100
   standby 1 preempt
   standby 1 track 100 decrement 10
   ```

3. Enter the following CLI command to track the status of the WAN interface.
   If the WAN interface on the active router goes down, the standby router becomes active. When the recovery happens, both routers go back to the states they had before the failure.
   ```
   Configure the track command cli on the global configuration on router.
   “track 100 interface GigabitEthernet 0/0/0 line-protocol”
   ```

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

Implementing Network Control Center and Application Services

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

Configuring a DHCP Server

A dynamic host configuration protocol (DHCP) server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard DHCP to respond to broadcast queries by clients.

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

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

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

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

Domain Name Server

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

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

Cisco Catalyst Center Installation and Configuration

Cisco Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. Cisco Catalyst Center provides a centralized management dashboard for complete control of wind farm networks.
Cisco Catalyst Center is a dedicated hardware appliance powered through a software collection of applications, processes, services, packages, and tools, and is the centerpiece for Cisco Digital Network Architecture (Cisco DNA). This software provides full automation capabilities for provisioning and change management, reducing operations by minimizing the touch time required to maintain the network.

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


**Cisco ISE Installation and Configuration and Integration with Cisco Catalyst Center**

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

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

**ISE Installation and Initial Configuration**

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

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


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


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

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

**Cisco Firepower Management Center installation and Configuration**

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

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


**Cisco Cyber Vision Center Global Center**

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

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

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

**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*:


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*:


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*:


**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*:

Chapter 9: Implementing Network Management and Automation

This chapter includes the following topics:

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

Preparing Cisco Catalyst Center and Switches for Device Onboarding

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

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

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

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

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

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

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

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

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

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.
Implementing Network Management and Automation

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 Cisco123
  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 Cisco123
  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:**

---

**Figure 9-2: Site Hierarchy in Cisco Catalyst Center**

- WindFarm
  - ONSS
  - OSS
- FAN
  - MainBuilding
  - TAN1
  - TAN2
  - TAN3
hostname WF-OSS-C9300Access
ip domain name wf.com
username dna privilege 15 password 0 Cisco@123
enable secret 0 C!sco123
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 15
login local
transport input ssh
transport preferred none
!
snmp-server group default v3 priv
snmp-server group ciscogrp v3 priv read SNMPv3All write SNMPv3None
snmp-server view SNMPv3All iso included
snmp-server view SNMPv3None iso excluded
snmp-server community cisco123 RW
snmp-server user cisco default v3 auth sha cisco123 priv aes 128 cisco123
!
netconf-yang

3. Verify that all three devices can reach Cisco Catalyst Center by initiating a ping to Cisco Catalyst Center from each of the three devices.

4. Perform the following actions to initiate the discovery of core switches in the OSS network.

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

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

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

Figure 9-3: Discovered Core Switches

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

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

As a prerequisite for onboarding the FAN and TAN rings, the intended final ring must be broken into two daisy chains to ensure that there is only one upstream switch via which the switch is being reached by Cisco Catalyst Center for PnP. The switches are sequentially
Implementing Network Management and Automation

onboarded to Cisco Catalyst Center one by one until the entire topology onboard is complete. For selecting the linear daisy chain for the intended final ring topology, the ring can be broken at any desired point, resulting in two daisy chains. For optimization, we recommend that the ring be broken in the middle.

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

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

Create Day 0 Templates for 3400 Onboarding

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


The day 0 template should include the following content:

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

Onboard the FAN Ring

1. Connect the first 3400 switches of both daisy chains (obtained by breaking the FAN ring in the middle) to be onboarded to the 9300 aggregation per the wind farm topology.
   (The two daisy chains must be connected on separate stack members of the 9300 aggregation stack to achieve full redundancy.)

2. Reload the 3400 switch to trigger the PnP if it has no previous configuration.
   If the 3400 switch has any existing configuration, enter the following commands on the switch to remove all configurations before starting the onboarding process:

```
delete /force sdflash:vlan.dat
delete /force sdflash:*.cer
delete /force sdflash:pnp*
delete /force /recursive sdflash:.installer
delete /f flash:vlan.dat
delete /f flash:config.text
delete /f flash:private config.text
delete /f /r flash:dc_profile_dir
delete /f flash:pnp-tech-time
delete /f flash:pnp-tech-discovery-summary
#Delete all the certificates in NVRAM
delete /f nvram:*.cer
conf t
crypto key zeroize
  Yes
  !
no crypto pki certificate pool
Yes
vtp mode transparent
End
write erase

Reload
no
3. After the switch reboots, PNP is triggered and the device appears under Provision > Plug and Play with a state of Unclaimed, check the checkbox for the device and choose Actions > Claim.

4. Enter the hostname and site to which the switch is to provisioned in the Hostname and Site fields.

5. Attach a day 0 template by clicking the attach symbol and choosing the template from the list of available templates. The State field for the device changes from Planned to Onboarding and then to Provisioned. After the device is onboarded, the device appears in the topology under Main menu > Provision > Inventory > Topology, as shown in figure 9-2. Nodes can be added to this chain by connecting the new 3400 to the last onboarded 3400 switch of the daisy chain and repeating the steps 1 through 4.

Figure 9-5: Onboarding the First 3400 Switch

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

After onboarding the 3400 switches of both daisy chains of the ring is complete, verify the topology by choosing Provision > Inventory > Topology. The display should resemble the example shown in Figure 9-6.
Connect the interfaces of the end nodes of the two daisy chains, which transforms the two daisy chains into the FAN ring. The FAN ring topology should be as shown in Figure 9-7. You can verify the topology by choosing Provision > Inventory > Topology.

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

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

To create the FAN REP ring, follow these steps:

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

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

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

Onboard TAN Switches

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

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

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

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

To onboard TAN with HA:

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

- **TAN3 ring onboarding:** First connect two TAN3 ring members to two different switches of the FAN ring (identified as BS2 and BS3 in the wind farm topology), then follow the FAN ring onboarding steps. BS2 and BS3 act as edge switches for the REP open segment.

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

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

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

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

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


   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

Add New Template

Project Name:
DayNTemplates

Template Type
- Regular Template
- Composite Sequence

Template Language
- Jinja
- Velocity

Software Type:
IOS-XE

Device Type Details
Add the types of devices you want to associate with the template
Device Family:
Switches and Hubs
Devices:
Cisco Catalyst IE3400 Rugged Series
Device Tags:

Enter the contents of the template as follows:

```bash
# 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.

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

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

   NS2 → NS1 → BS4

   To provision the REP configuration template:

   a. From the Main menu, choose **Provision > Inventory**.
   b. Check the checkbox next to TAN2 switch under the configuration (NS2/NS1/BS4).
   c. From the Actions drop down menu, choose **Provision > Provision Device**, then click **Next**.
   d. 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**

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Use</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply_rep</td>
<td>To apply or remove rep configuration</td>
<td>1/0</td>
</tr>
<tr>
<td>rep_admin_vlan</td>
<td>REP admin VLAN</td>
<td>VLAN ID to be used as REP admin VLAN</td>
</tr>
<tr>
<td>isedge</td>
<td>Edge port or non edge port (1 for edge port and 0 for non edge ports)</td>
<td>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)</td>
</tr>
<tr>
<td>int_first</td>
<td>First interface ID of device that is a part of the TAN ring</td>
<td>Interface ID used in TAN ring formation</td>
</tr>
<tr>
<td>segment</td>
<td>TAN REP ring segment ID</td>
<td>Segment ID of choice (segment ID 2 is used in the wind farm topology for TAN2 as an example)</td>
</tr>
<tr>
<td>mainRingSegId</td>
<td>FAN REP ring segment 1</td>
<td>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)</td>
</tr>
</tbody>
</table>
Implementing Network Management and Automation

<table>
<thead>
<tr>
<th>int_second</th>
<th>Second interface ID of the device that is a part of the TAN ring.</th>
<th>Second interface of the device used in TAN ring formation</th>
</tr>
</thead>
</table>

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

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

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

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

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Use</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply_rep</td>
<td>To apply or remove rep configuration.</td>
<td>1/0 (1 to apply REP, 0 to remove REP configuration).</td>
</tr>
<tr>
<td>rep_admin_vlan</td>
<td>REP admin VLAN.</td>
<td>VLAN ID to be used as REP admin VLAN.</td>
</tr>
<tr>
<td>isedge</td>
<td>Edge port or non edge port. (1 for edge port and 0 for non edge port.)</td>
<td>Enter 1 for BS2 and BS3 and 0 for NS1 and NS2.</td>
</tr>
<tr>
<td>int_first</td>
<td>First interface ID of the device that is a part of the TAN ring.</td>
<td>Interface ID used in TAN ring formation.</td>
</tr>
<tr>
<td>segment</td>
<td>TAN REP ring segment ID.</td>
<td>Segment ID of choice (segment ID 2 is used in the wind farm topology for TAN2 as an example).</td>
</tr>
<tr>
<td>mainRingSegId</td>
<td>FAN REP ring segment ID.</td>
<td>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).</td>
</tr>
<tr>
<td>int_second</td>
<td>Second interface ID of the device that is a part of the TAN ring.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Day N Configurations using Cisco Catalyst Center Templates

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

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

Adding a New Switch to a FAN REP Ring

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

1. Verify that the interfaces to which the new switch is going to be connected has a REP segment ID configured and ZTP enabled by entering the command `show run interface interface-id` on the switch console.

2. Connect the new switch between the two existing 3400 switches using the same physical connection that was used between the existing 3400 switches.
3. Onboard the new switch by triggering PnP and ensuring that no previous configuration exists on the newly added switch. See the onboarding steps in FAN and TAN Ring Devices Onboarding (Day-0 Provisioning).

   Ensure that you add this new switch in the same Cisco Catalyst Center site as the FAN switches.

4. Click the REP rings tab and verify that the switch has been added to the REP ring automatically.

**Network Assurance**

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

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

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:


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

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

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

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

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

   FAN-IE3400-BS1# show vlan

   VLAN Name        Status       Ports
   1  default        active       Gi1/3, Gi1/4, Gi1/5, Gi1/6, Gi1/7, Gi1/8, Gi1/10, Ap1/1, Gi2/1, Gi2/2, Gi2/3, Gi2/6, Gi2/7, Gi2/8
   Gi2/4, Gi2/5

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: sentry069!

**CVS:**
- Capture IP address: 169.254.1.2
- Capture subnet mask: 30
- Capture VLAN number: 2508
- Collection IP address: 10.10.112.101
- Collection subnet mask: 24
- Collection gateway: 10.10.112.100
- Collection VLAN number: 102

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

- Configure access to SSH
- Configure basic parameters

The following steps show the configuration that is needed on IE3400 switches for the sensor installation to then register it with the CVC:
1. Format sdflash and enable IOx on the IE switch by using the following CLI commands:

   FAN-IE3400-BS1# format sdflash: ext4
   FAN-IE3400-BS1# show sdflash: filesys
   Filesystem: sdflash
   Filesystem Path: /flash11
   Filesystem Type: ext4
   Mounted: Read/Write

   FAN-IE3400-BS1# configure terminal
   FAN-IE3400-BS1#(config)# iox
   FAN-IE3400-BS1#(config)# end
   FAN-IE3400-BS1# show iox

   IOx Infrastructure Summary:
   ........................................
   IOx service (CAF) : Running
   IOx service (HA) : Not Supported
   IOx service (IOxman) : Running
   IOx service (Sec storage) : Running
   Libvirtd 5.5.0 : Running
   Dockerd v19.03.13-ce : Running

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

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

   configure terminal
   vtp mode off
   vlan 2508
   remote-span
   end
   
   !
   interface AppGigabitEthernet 1/1
   switchport mode trunk
   exit
   end

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
Implementing Network Security and QoS

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:


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:


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

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.
Implementing Network Security and QoS

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

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:

Configuring Stealthwatch (SNA) NetFlow

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

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

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

NetFlow Configuration on an IE3400

```
ip flow-export destination fc_ip fc_port

##Configure the Flow Record##
flow record fnf-rec
match ipv4 tomatch ipv4 protocol
timeout 30
match ipv4 source address
timeout 30
match transport source-port
timeout 30
match transport destination-port
timeout 30
collect counter bytes long
option interface-table

##Configure the Exporter##
flow exporter fnf-exp
destination fc_ip
timeout 30
transport udp fc_port
timeout 30
template data timeout 30
```
Implementing Network Security and QoS

```plaintext
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](image)

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:


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:
   

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.
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.
   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

![IGMP Configuration Interface]

- Click **Save**, then click **Deploy** in the Main menu.
Chapter 11 Turbine Operator Network Implementation

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


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

Figure 11-1 Network implementation flow for Turbine operator Scada

Turbine Operator Core Network Implementation

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

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

Figure 11-2 Configuration sequence for Core network devices

1. Complete physical cabling of the devices as per the topology below:
2. Complete hostname, NTP and domain configuration on all core switches. Following is an example configuration for the same:

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

3. Configuring SVIs on 9300s

**C9300-1:**

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

!
vlan 10
!
interface Vlan10
ip address 10.10.1.2 255.255.255.0
!
Vlan 20
interface Vlan20
ip address 10.20.1.2 255.255.0.0
!
Vlan 111
interface Vlan111
```
ip address 10.111.1.2 255.255.255.0
!

C9300-2:

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

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

4. Configuring HSRP

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

C9300-1:

interface Vlan5
standby 5 ip 10.5.1.1
!

interface Vlan10
standby 1 ip 10.10.1.1
!

interface Vlan20
standby 20 ip 10.20.1.1
!

interface Vlan111
standby 111 ip 10.111.1.1
!

Repeat the same on C9300-2

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

SCADA-C9300-1 #show standby brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>P State</th>
<th>Active</th>
<th>Standby</th>
<th>Virtual IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vl15</td>
<td>5</td>
<td>100</td>
<td>Standby</td>
<td>10.5.1.3</td>
<td>local</td>
<td>10.5.1.1</td>
</tr>
<tr>
<td>Vl10</td>
<td>1</td>
<td>105</td>
<td>Active</td>
<td>local</td>
<td>10.10.1.3</td>
<td>10.10.1.1</td>
</tr>
<tr>
<td>------</td>
<td>---</td>
<td>----</td>
<td>--------</td>
<td>-------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Vl20</td>
<td>20</td>
<td>100</td>
<td>Standby</td>
<td>10.20.1.3</td>
<td>local</td>
<td>10.20.1.1</td>
</tr>
<tr>
<td>Vl111</td>
<td>111</td>
<td>100</td>
<td>Active</td>
<td>local</td>
<td>10.111.1.3</td>
<td>10.111.1.1</td>
</tr>
</tbody>
</table>

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

5. Configuring IE9Ks
   IE9K-1:
   Vlan 10,20,11
   interface Vlan111
   ip address 10.111.1.4 255.255.255.0
   ip route 0.0.0.0 0.0.0.0 10.111.1.1

   IE 9K-2:
   Vlan 10,20,11
   interface Vlan111
   ip address 10.111.1.5 255.255.255.0
   ip route 0.0.0.0 0.0.0.0 10.111.1.1

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

7. Bringing up port-channel between the two core C9300 and configuring it as trunk port
   Configure the two links between the C9300 switches as port-channels as shown below:
   C9300-1:

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

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

   interface Port-channel1
   switchport mode trunk

   Repeat the same on C9300-2

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

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

   C9300-1:
   interface TenGigabitEthernet1/1/1
   switchport mode trunk
   rep segment 1 edge
IE9k-1:
```plaintext
interface TenGigabitEthernet1/0/27
  switchport mode trunk
  rep segment 1

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

IE9k-2:
```plaintext
interface TenGigabitEthernet1/0/27
  switchport mode trunk
  rep segment 1

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

C9300-2:
```plaintext
interface TenGigabitEthernet1/1/1
  switchport mode trunk
  rep segment 1 edge
```

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

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

Configuring WAN Edge Routing

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

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

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

2. Configuring routing on the Firepower

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


3. Allowing ports in the Firepower to enable communication

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

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

This completes WAN edge routing.

### Configuring FSN Ring

In the turbine operator network, the IE3400 and/or IE3100 Series switches as the base SCADA switch from each wind turbine is connected in a ring topology using a 1G fiber cable with Cisco Industrial Ethernet 9300 switches to form a farm area SCADA network (FSN) ring. A REP is configured in the FSN ring to provide FAN resiliency for faster network convergence if a REP segment fails. For understanding more on FSN design refer to [Cisco Solution for Renewable Energy: Offshore Wind Farm 1.1 Design Guide](https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/Wind_Farm/WF_1-1_DG.pdf?dtid=odicdc000509): section Farm Area SCADA Network (FSN) Design.

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

#### Figure 11-5  Workflow for FSN ring configuration

1. Complete physical cabling

Connect the devices to the IE9K of the core REP ring as shown in Figure 11-6.
2. Complete hostname, NTP and domain configuration on all switches. Following is an example configuration for the same:

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

3. Configure vlan, IP and default gateway

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

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

4. Configure MACsec

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

5. Configuring REP on FSN ring

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

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

   **IE9K-1:**

   interface TenGigabitEthernet1/0/25
   switchport mode trunk
   rep segment 100 edge
Base Scada Switch1:

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

IE9K-2:

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

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

```
WF-SCADA-FSN-3400-Y1FB#sh rep topo
REP Segment 100
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
WF-SCADA-IE9320-1                Te1/0/25   Pri  Open
WF-SCADA-FSN-3400-Y1FB           Gi1/2           Open
WF-SCADA-FSN-3400-Y1FB           Gi1/1           Open
3400-P48G                        Gi1/1           Open
3400-P48G                        Gi1/2           Open
WF-SCADA-FSN03-V0NS              Gi1/2           Open
WF-SCADA-FSN03-V0NS              Gi1/1           Open
WF-SCADA-FSN04-Y2BT              Gi1/2           Open
WF-SCADA-FSN04-Y2BT              Gi1/1           Open
WF-SCADA-FSN05-V0SZ              Gi1/2           Open
WF-SCADA-FSN05-V0SZ              Gi1/1           Open
WF-SCADA-IE9320-2                Te1/0/25   Sec  Alt
```

Configuring TSN Rings

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

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

**TSN non-HA**

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

**Figure 11-7 Workflow for TSN non-HA configuration**

1. Complete physical cabling.

Physical cabling of switch to a Base Scada Switch is done with two links for redundancy as shown in diagram below.
2 Complete hostname, NTP, and domain configuration on all switches. Following is an example configuration for the same.

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

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

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

   **SCADA Switch:**
   
   ```
   interface range GigabitEthernet1/1-2
   channel-group 1 mode active
   ```

   **Base SCADA Switch:**

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

   end

5 Complete vlan, interface, and layer 2 configs:

   Configure the switches as shown below:
SCADA switch:

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

Base SCADA Switch:

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

This completes the configuration of TSN non-HA.

**Configuring TSN HA:**

The following diagram describes the sequence for TSN HA configuration:

![Figure 11-9 Workflow for configuring TSN HA](image-url)

1. Completing physical cabling

Physical cabling of switches to a Base Scada Switch forms a closed ring as shown in Figure 11-10 below.
2. Complete hostname, NTP and domain configuration on all switches. Following is an example configuration for the same:

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

3. Configure vlan and interface

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

4. Configure MACsec

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

5. Configure REP segment.

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

   **Base SCADA Switch:**

   interface GigabitEthernet1/3
   switchport mode trunk
   rep segment 101 edge
Nacelle Switch1:

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

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

Nacelle Switch2:

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

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

```
sh rep topology
REP Segment 101
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
3400-P48G                        Gi1/4      Pri  Open
SCADA-TSN-Y0ZJNacelleSw1         Gi1/4           Open
SCADA-TSN-Y0ZJNacelleSw1         Gi1/1           Open
WF-SCADA-TSN-Y1SL                Gi1/2           Open
WF-SCADA-TSN-Y1SL                Gi1/3           Open
3400-P48G                        Gi1/3      Sec  Alt
```

This completes TSN HA ring configuration.

**Configuring Private VLANs**

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

A PVLAN uses VLANs in the following three ways:

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

To learn more about PVLANs refer to the link that follows:
To configure PVLAN in Turbine Operator SCADA network follow the sequence shown in diagram below:

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

```
! vtp mode transparent
!
```

2. Creating primary and secondary vlans

```
vlan 10
  name PrivateVLANvlan
  private-vlan primary

vlan 101
  private-vlan isolated
```

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

3. Creating association between primary and secondary vlan

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

4. Creating mapping on the SVI of primary vlan

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

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

5. Configuring an interface in a secondary vlan

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

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

Alternatively, the port can also be configured as **promiscuous**.
The private vlan configuration can be verified by issuing “show vlan private-vlan”

```
Show vlan private-vlan
```

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>101</td>
<td>isolated</td>
<td>Gi1/3</td>
</tr>
</tbody>
</table>

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

This completes the PVLAN configuration.

### Configuring MACSec

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

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

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


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

### Configuring Pre-shared key-based Macsec

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

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

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

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

   ```
   key chain MAC-SEC macsec
   key 4000000000000000000000000000000000000000000000000000000000000000
   cryptographic-algorithm aes-128-cmac
   key-string 7 106D283F2034332D29270B010B1213074324372524067A7975715E2039307C08
   lifetime local 00:00:00 Jan 1 1993 infinite
   ```
2. Configure an mka policy as shown below:

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

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

   For C9300 & IE9320:

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

   For 3400:
   Macsec
   mka policy MKA-POLICY
   mka pre-shared-key key-chain MAC-SEC

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

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

Configuring certificate-based MACsec

This section covers the configuration of certificate based MACsec in brief. To learn details about the same refer to the link below:


For configuring certificate based MACsec, a CA server must be first setup. Certificate can be obtained from the CA, in the following two ways:
1. Manual installation of certificates from a CA
2. Certificate installation via SCEP

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

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

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

Pre-requisites for configuring certificate based MACsec:

i. All devices must be synchronized to the same NTP

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

Manual installation of certificates from a CA

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

For detailed steps refer to the link below:

1. Generating a key-pair
   Generate a key pair for use in trustpoint as shown in the example below:
   ```
crypto key generate rsa modulus 4096 label my-4096rsa-key
   
   !
   ```

2. Creating Trustpoint
   Following commands show an example for creation of trustpoint
   ```
crypto pki trustpoint my-trustpoint
   enrollment terminal pem
   C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN= WF-SCADA-IE9320-1.wf.com
   subject-alt-name WF-SCADA-IE9320-1.wf.com
   serial-number none
   ip-address none
   revocation-check none
   rsakeypair my-4096rsa-key
   ```

3. Generating CSR
   A Certificate Signing Request will be created and the same will be displayed on the screen. This CSR needs to be copied to a file and saved it with file_name.cer. Following is the command to generate CSR and display it on the screen:
   ```
crypto pki enroll my-trustpoint
   ```

4. Obtaining CA root certificate
   For authenticating the CA, the CA certificate must be installed on the device using the following command:
5. Importing device certificate

In this step the file that was given by the CA on submission of CSR is going to be imported on the device using the command below:

```
crypto pki import my-trustpoint certificate
```

With this, the device is now ready to use the certificate for MACsec configuration

### Certificate installation via SCEP

For installing a certificate via SCEP complete the sequence shown in following diagram:

![Figure 11-14 Workflow for configuring SCEP](image)

For detailed step refer to the link below:


1. **Generate key-pair**
   - Generate a key pair as covered in Manual certificate install section.
   ```
crypto key generate rsa modulus 4096 label my-4096rsa-key
```

2. **Create a trustpoint with enrolment URL pointing to the reachable CA as shown in example below:**
   ```
crypto pki trustpoint CA
   enrollment url http://10.20.200.1:80
   serial-number
   ip-address none
   subject-name CN=Y819
   revocation-check none
   rsakeypair my-4096rsa-key
   hash sha512
```

3. **Downloading the CA root certificate**
   - Download the CA root certificate by issuing the command shown below:
   ```
crypto pki authenticate <TRUSTPOINT_NAME>
```
   Example: `crypto pki authenticate my-trustpoint`

4. **Enrolling the certificate**
   - Issue the below command to enroll the device certificate
   ```
crypto pki enroll <TRUSTPOINT_NAME>
```
   Example: `crypto pki enroll my-trustpoint`
The certificate should be successfully obtained. Verify the same using the following CLI:

```bash
show crypto pki certificates verbose my-trustpoint
```

**Certificate based MACsec configuration**

After certificates have been installed on the devices, MACsec can be configured as shown in the diagram below:

**Figure 11-15 Workflow for configuring certificate based MACSec**

1. **Configuring AAA**
   
   Following is the example configuration to configure AAA:
   ```bash
  conf t
   aaa new-model
   aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
   aaa authorization credential-download MACSEC-UPLINK local
   aaa authentication dot1x MACSEC-UPLINK local
   aaa authorization network MACSEC-UPLINK local
   !
   end
   ```

2. **Creating Local Username for 802.1x Authentication**
   
   This username will be referenced in the dot1x Cred Set section below.
   ```bash
   aaa attribute list MUST-SECURE
      attribute type linksec-policy must-secure
   !
   username usr-macsec aaa attribute list MUST-SECURE
   !
   ```

3. **Creating a policy map for MACsec Uplink**
   
   Configure the policy-map that will be applied to interfaces that connect the switches
   ```bash
   policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
      event session-started match-all
         10 class always do-until-failure
      event authentication-failure match-all
         10 class always do-until-failure
         10 terminate dot1x
      event authentication-restart 10
      event authentication-success match-all
         10 class always do-until-failure
         10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
   ```

4. **Configuring EAPTLS AuthC Profile and 802.1x Credential Set**
   
   Enable dot1x in this section and create authentication profiles:
   ```bash
   dot1x system-auth-control
   !
   eap profile EAP-PROFILE
      method tls
   pki-trustpoint my-trustpoint
   ```
5. Configuring the Switchport for VLAN Trunking, dot1x & MACsec Network Link

```plaintext
interface g1/1
switchport mode trunk
macsec network-link
authentication periodic
authentication timer reauthenticate 1800
access-session host-mode multi-host
access-session closed
access-session port-control auto
dot1x pae both
dot1x credentials DOT1X-CREDS
dot1x supplicant eap profile EAP-PROFILE
dot1x authenticator eap profile EAP-PROFILE
service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
```

6. Verification

Verify that the macsec session is established by issuing a show mka session

---

**Implementing Quality of Service**

The WindFarm turbine operator network uses the QoS model described in the section TSN Quality-of-Service Design of the Windfarm Design Guide to guarantee network performance and operation by streamlining traffic flow, differentiating network services, and reducing packet loss, jitter, and latency.

The following diagram shows the QoS model implemented on FSN and TSN rings:

**Figure 11-16 QoS design for IE switches in TSN and FSN**
For configuring QoS in the Turbine Operator Network use the following workflow:

**Figure 11-17 QoS configuration sequence**

1. **Classifying the traffic**

   Traffic can be classified using the source marked DSCP value or by configuring an access-list to segregate traffic based on source ip and matching against this access-list. Following is configuration required this step.

   ```
   ip access-list standard 1
   10 permit 10.1.10.0 0.0.0.255
   class-map match-any MCD
   match dscp cs5  ef  cs6  cs7
   class-map match-any LPD
   match dscp default cs1
   class-map match-any MPD
   match dscp cs2  af21  af22  af23
   class-map match-any HPD
   match dscp cs3  af31  af32  af33  cs4  af41  af42  af43
   match access-group 1
   class-map HPD_Output
   match dscp CS4
   ```

2. **Creating ingress policy-map for remarking**

   An input policy-map is to be created to use the above created class-maps and setting the dscp value as per the QoS design. Following is an example configuration:

   ```
   policy-map WF_SCADA_Ingress_Policy
   class MCD
   set ip dscp EF
   class HPD
   set ip dscp CS4
   class MPD
   set ip dscp CS2
   class LPD
   set ip dscp CS1
   ```

3. **Creating Egress policy-map**

   An output policy-map is to be created as per the QoS design. Following is an example configuration:

   ```
   policy-map WF_SCADA_Egress_Policy
   class MCD
   priority
   queue-limit 48 packets
   class HPD_Output
   bandwidth remaining percent 40
   queue-limit 48 packets
   class MPD
   bandwidth remaining percent 30
   queue-limit 48 packets
   class LPD
   bandwidth remaining percent 30
   queue-limit 272 packets
   ```

4. **Applying the Ingress and Egress policies on interface**

   The following is the example configuration to apply the policies on the interfaces
This completes QoS configuration on the devices.

Implementing Multicast in Offshore Substation

This section describes how to enable support for multicast traffic in a turbine operator network. To enable multicast between devices configure the C9300s in the core network as a rendezvous point for multicast. For details on how to configure multicast refer to the link below:

Figure 11-18 Workflow for Enabling Multicast

1. Enable multicast on C9300s
   Enter the following commands on the 9300s to enable multicast:
   ```
   ip multicast-routing
   ```

2. Enabling PIM under SVIs of C9300
   Enter the following commands under interface vlan on both C9300s:
   ```
   interface Vlan5
   ip pim sparse-mode
   ```

3. Configuring RP
   RP Address has to be configured on the C9300s. Following is the example config:
   ```
   ip pim rp-address 10.5.1.1
   ```

   The source can be connected on the core ring and destination in FSN/TSN ring to send/receive the multicast.

   This completes the multicast implementation for the Turbine operator network.
Appendix A: Configuration Examples

This appendix includes the following topics:

- WAN PE Configuration
- WAN HER Configuration
- FAN Ring Switch Configuration (Non Edge Switch that is Not a Part of TAN Rings)
- QoS on IE-3400
- QoS on FAN Aggregation and on the OSS and ONSS (C-9300/C-9500)

WAN PE Configuration

```
hostname PE
!
boot-start-marker
boot system bootflash:asr900rsp2-universalk9_npe.17.05.01.SPA.bin
boot-end-marker
!
vti definition Management_VRF
  rd 100:1
  route-target export 100:1
  route-target import 100:201
!
address-family ipv4
  exit-address-family
!
vti definition Mgmt-intf
  rd 199:105
  route-target export 199:105
  route-target import 199:105
!
address-family ipv4
  exit-address-family
!
vti 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
!
mls ldp explicit-null
mls ldp graceful-restart
mls ldp session protection
mls 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 ivsg0123
!
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-tunne1
  interval min-tx 100 min-rx 100 multiplier 3
!
bfd-template single-hop bfd-tunnel2
  interval min-tx 4 min-rx 4 multiplier 3
!
bsd-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 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 625000
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-channel1
   ip address 192.168.119.1 255.255.255.0
   no negotiation auto
   bfd interval 50 min_rx 50 multiplier 3
   lacp max-bundle 2
!
interface Multilink1
   ip address 11.11.11.1 255.255.255.0
   ppp multilink
   ppp multilink group 1
!
interface pseudowire1
   encapsulation mpls
   neighbor 3.3.3.3 3
   mtu 1508
   control-word include
!
interface pseudowire2
   encapsulation mpls
   neighbor 17.17.17.17 28
   bandwidth 2144 persistent
!
interface pseudowire3
   encapsulation mpls
   neighbor 2.2.2.2 4
   bandwidth 64 persistent
!
interface TenGigabitEthernet0/0/0
   no ip address
   shutdown
!
interface Serial0/1/0:1
   no ip address
   encapsulation ppp
   ppp multilink
   ppp multilink group 1
!
interface GigabitEthernet0/2/0
   ip address 192.168.81.2 255.255.255.0
   ip ospf network point-to-point
   ip ospf 1 area 0
   load-interval 30
   negotiation auto
   cdp enable
   mpls ip
   mpls label protocol ldp
   mpls ldp discovery transport-address 192.168.201.10
   mpls traffic-eng tunnels
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-universalk9.17.03.0a.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
  default-router 192.168.85.1

ip dhcp pool IR1101-cEDGE
  network 192.168.8.0 255.255.255.0
  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
|
mls label protocol ldp
mls ldp igp sync holddown 1
mls 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 49F5352D 53656C66 2D536967 6E65642D 43657274
65666963 35748552D 30139356 38393736 3434301E 170D3139 30313033 32333337
31305A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03312649
4F5F32D5 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39363538
37373634 34302D01 22300D06 92038648 86F70D01 01010050 3832010F 00380201
0A028201 0100C714 667262F0 6F62CA62B B50D37FD 43657274
|
! Renewable
| Energy
|
| – Wind
|
| Farm 1.0
|
| Design
|
| Guide

quit
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 3DB4C73 E890DD06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 96331C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD4681E 3A5673AB 903D3B1 6C9E3D8B
D98987BF E40CB9DE 1AECAC0C2 2189BB5C 8FA85686 CD88B646 5575B146 8DFC66A8
4F6A3D4F 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF998 E973DE7F 5BDEEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 A48A229 C37C1E69 39FD087B
80DDCD16 D6BAACE7 EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E8F73 932E35B5 8862F0A8 0275156F 719BB2F0
D697DF7F 28 quit
!
license udi pid ASR1002-HX sn JAE225206PR
license accept end user agreement
license boot suite FoundationSuiteK9
license boot suite AdvUCSuiteK9
license boot level adventerprise
license solution level appxk9
license solution level securityk9
memory free low-watermark processor 991004
!
spanning-tree extend system-id
diagnostic bootup level minimal
!
username cisco privilege 15 password 0 Cisco@123
username admin privilege 15 password 0 sentryo69!
!
redundancy
mode none
!
bridge-domain 1
member vni 6001
member GigabitEthernet0/2/15 service-instance 1
!
bridge-domain 601
no mac learning
!
bridge-domain 1000
crypto ikev2 authorization policy default_No_cert
route set interface
route set access-list FLEX_ACL
!
no crypto ikev2 authorization policy default
!
crypto ikev2 redirect gateway init
!(IKEv2 Cluster load-balancer is not enabled)
crypto ikev2 proposal FlexVPN_IKEv2_Proposal_No_cert
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FlexVPN_IKEv2_Policy_No_cert
proposal FlexVPN_IKEv2_Proposal_No_cert
!
crypto ikev2 keyring ANY
peer ANY
!  address 0.0.0.0 0.0.0.0
pre-shared-key sentryo
!
crypto ikev2 profile FLEX_SERVER_PROF_No_cert_1
match identity remote address 0.0.0.0
match identity remote fqdn domain isg.cisco.com
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
Cisco Solution for Renewable Energy – Wind Farm 1.0 Design Guide

Configuration Examples

```plaintext
! 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
```

137
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 port 1
mtu 9216
no ip address
load-interval 30
negotiation auto

! interface GigabitEthernet0/0/2.1201
capsulation dot1Q 1201
vrf forwarding VRF_SCADA
ip address 12.0.1.1 255.255.255.0

! interface GigabitEthernet0/0/2.1202
capsulation dot1Q 1202
vrf forwarding VRF_TSCADA
ip address 12.0.2.1 255.255.255.0

! interface GigabitEthernet0/0/2.1203
capsulation dot1Q 1203
vrf forwarding VRF_PLANTLINK
ip address 12.0.3.1 255.255.255.0

! interface GigabitEthernet0/0/2.1204
capsulation dot1Q 1204
vrf forwarding VRF_MGMT
ip address 12.0.4.1 255.255.255.0

! interface GigabitEthernet0/0/2.1205
capsulation dot1Q 1205
vrf forwarding VRF_GRIDMON
ip address 12.0.5.1 255.255.255.0

! interface GigabitEthernet0/0/2.1206
capsulation dot1Q 1206
vrf forwarding VRF_BUSINESS
ip address 12.0.6.1 255.255.255.0

! interface GigabitEthernet0/0/2.3001
capsulation dot1Q 3001
ip address 30.1.0.1 255.255.255.0

! interface GigabitEthernet0/0/2.3002
capsulation 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
capsulation dot1q 990
rewrite ingress tag pop 1 symmetric
bridge-domain 601

!
service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1000

interface GigabitEthernet0/0/3.140
  encapsulation dot1q 140
  ip address 140.140.140.1 255.255.255.0

interface GigabitEthernet0/0/3.799
  encapsulation dot1q 799
  xconnect 192.168.199.1 799 encapsulation mpls

interface GigabitEthernet0/0/3.2001
  description For Windfarm Testbed
  encapsulation dot1q 2001
  vrf forwarding Management_VRF
  ip address 201.201.201.1 255.255.255.0

interface GigabitEthernet0/0/4
  ip address 99.99.99.100 255.255.255.0
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3

interface GigabitEthernet0/0/5
  description connected to 10.104.56.148 PC ethernet - asr G5
  ip address 192.168.228.1 255.255.255.252
  negotiation auto

interface GigabitEthernet0/0/6
  description Phy_Loop
  no ip address
  negotiation auto
  service instance 990 ethernet
  encapsulation dot1q 990
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD RF
  bridge-domain 601 split-horizon group 0

! service instance 997 ethernet
  encapsulation dot1q 997
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD RF
  bridge-domain 1000

! service instance 998 ethernet
  encapsulation dot1q 998
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD RF
  bridge-domain 1000

! service instance 1001 ethernet
  encapsulation dot1q 1001
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8 R9 RA RB RC RD RF
  bridge-domain 1000

! service instance 1002 ethernet
  encapsulation dot1q 1002
  rewrite ingress tag pop 1 symmetric
  l2protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
Cisco Solution for Renewable Energy – Wind Farm 1.0 Design Guide

Configuration Examples

R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1052 ethernet
encapsulation dot1q 1052
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1053 ethernet
encapsulation dot1q 1053
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1054 ethernet
encapsulation dot1q 1054
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1055 ethernet
encapsulation dot1q 1055
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1056 ethernet
encapsulation dot1q 1056
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1057 ethernet
encapsulation dot1q 1057
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 1058 ethernet
encapsulation dot1q 1058
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 1000
!!
service instance 2502 ethernet
encapsulation dot1q 2502
rewrite ingress tag pop 1 symmetric
 12protocol forward cdp stp vtp dtp pagp dot1x lldp lacp udld esmc elmi ptppd R4 R5 R6 R8
R9 RA RB RC RD RF
bridge-domain 601 split-horizon group 1
!!
interface GigabitEthernet0/0/7
  description Phy_Loop
  no ip address
  load-interval 30
  negotiation auto
!!
Configuration Examples

```plaintext
interface GigabitEthernet0/0/7.989
  encapsulation dot1Q 989
  xconnect 192.168.205.2 989 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.990
  encapsulation dot1Q 990
  xconnect 192.168.220.3 990 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.991
  encapsulation dot1Q 991
  xconnect 192.168.205.2 991 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.992
  encapsulation dot1Q 992
  xconnect 192.168.205.2 992 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.993
  encapsulation dot1Q 993
  xconnect 192.168.223.1 993 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.994
  encapsulation dot1Q 994
  xconnect 192.168.223.1 994 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.995
  encapsulation dot1Q 995
  xconnect 192.168.223.1 995 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.996
  encapsulation dot1Q 996
  xconnect 192.168.223.1 996 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.997
  encapsulation dot1Q 997
  xconnect 192.168.223.1 997 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.998
  encapsulation dot1Q 998
  xconnect 192.168.202.2 998 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.1001
  encapsulation dot1Q 1001
  xconnect 192.168.199.2 1001 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2502
  encapsulation dot1Q 2502
  xconnect 192.168.199.2 2502 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2503
  encapsulation dot1Q 2503
  xconnect 192.168.199.2 2503 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2504
  encapsulation dot1Q 2504
  xconnect 192.168.199.2 2504 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2505
  encapsulation dot1Q 2505
  xconnect 192.168.199.2 2505 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2506
  encapsulation dot1Q 2506
  xconnect 192.168.199.2 2506 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2507
```
encapsulation dot1Q 2507
xconnect 192.168.199.2 2507 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2508
encapsulation dot1Q 2508
xconnect 192.168.199.2 2508 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2509
encapsulation dot1Q 2509
xconnect 192.168.199.2 2509 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface GigabitEthernet0/0/7.2560
encapsulation dot1Q 2560
xconnect 192.168.199.2 2560 encapsulation l2tpv3 pw-class L2TP_PW_TEST
!
interface TenGigabitEthernet0/1/0
description connected to FPR4010 port 8
ip address 192.168.70.2 255.255.255.0
service-policy input HOST-INPUT-MARKING
!
interface TenGigabitEthernet0/1/0.106
encapsulation dot1Q 106
vrf forwarding Management_VRF
ip address 106.106.0.2 255.255.255.0
ip nat inside
ip ospf network point-to-point
!
interface TenGigabitEthernet0/1/1
no ip address
!
interface TenGigabitEthernet0/1/2
ip address 192.168.84.1 255.255.255.0
ip ospf network point-to-point
ip ospf 1 area 0
!
interface TenGigabitEthernet0/1/2.2
description connected to NCS-002-TenGigE0/0/0/6.2
encapsulation dot1Q 2
ip address 192.168.75.2 255.255.255.0
!
interface TenGigabitEthernet0/1/3
no ip address
shutdown
!
interface TenGigabitEthernet0/1/4
no ip address
!
interface TenGigabitEthernet0/1/5
no ip address
!
interface TenGigabitEthernet0/1/6
no ip address
!
interface TenGigabitEthernet0/1/7
no ip address
!
interface GigabitEthernet0/2/0
description connected to ixia 10.64.66.36 card 1 port 14
no ip address
negotiation auto
!
interface GigabitEthernet0/2/0.143
encapsulation dot1Q 143
ip address 143.143.143.1 255.255.255.0
!
interface GigabitEthernet0/2/1
  description connected to Laptop SCADA FEP
  ip address 192.168.189.1 255.255.255.0
  negotiation auto
!
interface GigabitEthernet0/2/2
  description connected to ixia card 1 port 10
  no ip address
  negotiation auto
!
interface GigabitEthernet0/2/2.501
  encapsulation dot1Q 501
  ip address 171.171.171.1 255.255.255.0
!
interface GigabitEthernet0/2/3
  no ip address
  negotiation auto
!
interface GigabitEthernet0/2/4
  ip address 10.64.66.77 255.255.255.0
  negotiation auto
!
interface GigabitEthernet0/2/5
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/2/6
  description connected to sumatra-pp-2 on G0/0/0
  ip address 89.89.89.1 255.255.255.0
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet0/2/7
  no ip address
  speed 1000
  no negotiation auto
!
interface GigabitEthernet0/2/7.152
  encapsulation dot1Q 152
  ip address 152.152.152.1 255.255.255.0
!
interface GigabitEthernet0/2/8
  no ip address
  negotiation auto
!
interface GigabitEthernet0/2/9
  description connected to SA-1002HX-002 gi0/0/0
  ip address 192.168.60.1 255.255.255.0
  ip nat inside
  negotiation auto
  mpls ip
  mpls label protocol ldp
!
interface GigabitEthernet0/2/10
  description connected to UCS 10.104.56.170 on VMNIC 8
  ip address 192.168.85.1 255.255.255.0
  ip nat inside
  negotiation auto
  cdp enable
!
interface GigabitEthernet0/2/11
  no ip address
  shutdown
  negotiation auto
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
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 12vpn 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_SCRADA
   redistribute connected
exit-address-family

ip tcp path-mtu-discovery
ip telnet source-interface GigabitEthernet0/0/0
ip http server
Cisco Solution for Renewable Energy – Wind Farm 1.0 Design Guide

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
Cisco Solution for Renewable Energy – Wind Farm 1.0 Design Guide

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
79 permit ip 192.168.6.0 0.0.0.255 any
80 permit tcp 192.168.6.0 0.0.0.255 any
81 permit udp 192.168.6.0 0.0.0.255 any
82 permit icmp 192.168.6.0 0.0.0.255 any
83 permit esp 192.168.6.0 0.0.0.255 any
84 permit ahp 192.168.6.0 0.0.0.255 any
85 permit ip 192.168.7.0 0.0.0.255 any
86 permit tcp 192.168.7.0 0.0.0.255 any
87 permit udp 192.168.7.0 0.0.0.255 any
88 permit icmp 192.168.7.0 0.0.0.255 any
89 permit esp 192.168.7.0 0.0.0.255 any
90 permit ahp 192.168.7.0 0.0.0.255 any
91 permit ip 192.168.8.0 0.0.0.255 any
92 permit tcp 192.168.8.0 0.0.0.255 any
93 permit udp 192.168.8.0 0.0.0.255 any
94 permit icmp 192.168.8.0 0.0.0.255 any
95 permit esp 192.168.8.0 0.0.0.255 any
96 permit ahp 192.168.8.0 0.0.0.255 any
97 permit ip 106.106.0.0 0.0.0.255 any
98 permit tcp 106.106.0.0 0.0.0.255 any
99 permit udp 106.106.0.0 0.0.0.255 any
100 permit icmp 106.106.0.0 0.0.0.255 any
101 permit esp 106.106.0.0 0.0.0.255 any
102 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-JAE225206Q1.cfg
tftp-server bootflash:ciscosdwan.cfg
tftp-server bootflash:asr1000-universalk9.17.03.04a.SPA.bin
!
control-plane
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  transport input all
  transport output all
!
call-home
  If contact email address in call-home is configured as sch-smart-licensing@cisco.com
  the email address configured in Cisco Smart License Portal will be used as contact email
  address to send SCH notifications.
  contact-email-addr sch-smart-licensing@cisco.com
  profile "CiscoTAC-1"
    active
      destination transport-method http
ntp master
ntp server 45.86.70.11
ntp server 10.104.56.158
!
end

9500
hostname WF-OSS-C9500
!
vrf definition Management_VRF
  rd 100:1
  !
  address-family ipv4
    route-target export 100:1
    route-target import 100:1
  exit-address-family
  !
vrf definition Mgmt-vrf
    --More--
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
vrf definition OT_VRF
  rd 700:1
  !
  address-family ipv4
    route-target export 700:1
    route-target import 700:1
  exit-address-family
  !
vrf definition VnV_VRF
  rd 500:1
  !
  address-family ipv4
    route-target export 500:1
    route-target import 500:1
  exit-address-family
  !
    --More--
    no aaa new-model
switch 1 provision c9500-16x
switch 2 provision c9500-16x
ip routing
!!
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
  rsakeypair TP-self-signed-3141569633
  hash sha256

crypto pki trustpoint DNAC-CA
  enrollment mode ra
  enrollment terminal
  usage ssl-client
  revocation-check crl none
  source interface Vlan101
  hash sha256
!
license boot level network-advantage addon dna-advantage
memory free low-watermark processor 131093
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
enable secret 9 $9$rT5UEjrWOCqDA.$e2FNehaH33QAkJmEcMFTYOs1VMrUmX2wD5IymWpNaSDo
!
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

```plaintext
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-12lvx-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-12-control
    description L2 control
    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
    match ip dscp af11
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
    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, L2LVXCtrl, ProtoSnoo, PuntWebauth, MCASTData, Transit, DOT1XAuth, Swfwd, LOGGING, L2LVXData, ForusTraffic, ForusARP, McastEndStn, Openflow, Exception, EGRExcept, NFLSampled, RPFFailed
class-map match-any scavenger
    match ip dscp cs1
!
policy-map system-cpp-policy
policy-map output
    class voice_o
```

152
priority level 1
class video
  bandwidth remaining percent 10
class ot_traffic
  bandwidth remaining percent 10
class network_control
  bandwidth remaining percent 10
class bulk_data
  bandwidth remaining percent 10
class scavenger
  bandwidth remaining percent 10
class class-default
  bandwidth remaining percent 15
policy-map input
  class voice
    set dscp ef
  class video
    set dscp af41
  class ot_traffic
    set dscp af21
  class network_control
    set dscp cs2
  class bulk_data
    set dscp af11
  class scavenger
    set dscp cs1
  class class-default
    set dscp default

interface Loopback0
  ip address 192.168.5.2 255.255.255.255

interface Port-channel1
  switchport mode trunk

interface Port-channel2
  switchport trunk allowed vlan 101,500,700
  switchport mode trunk

interface Port-channel11

interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  no ip address
  negotiation auto

interface TenGigabitEthernet1/0/1
  description connectedToFPROldY015
  switchport access vlan 100
  switchport mode access

interface TenGigabitEthernet1/0/2
  switchport access vlan 101
  switchport mode access

interface TenGigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode active
  service-policy input input
  service-policy output output

interface TenGigabitEthernet1/0/4

interface TenGigabitEthernet1/0/5
  switchport access vlan 100
switchport mode access
!
interface TenGigabitEthernet1/0/6
!
interface TenGigabitEthernet1/0/7
  switchport access vlan 100
  switchport mode access
!
interface TenGigabitEthernet1/0/8
!
interface TenGigabitEthernet1/0/9
  switchport access vlan 100
  switchport mode access
!
interface TenGigabitEthernet1/0/10
!
interface TenGigabitEthernet1/0/11
  switchport mode trunk
interface TenGigabitEthernet1/0/12
!
interface TenGigabitEthernet1/0/13
  switchport access vlan 214
  switchport mode access
!
interface TenGigabitEthernet1/0/14
!
interface TenGigabitEthernet1/0/15
  shutdown
!
interface TenGigabitEthernet1/0/16
!
interface TenGigabitEthernet1/1/1
  stackwise-virtual link 1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
  description Connected to Port TenGig1/1/1 on OSS-C9300-Access SW
  switchport mode trunk
  channel-group 11 mode desirable
  service-policy input input
  service-policy output output
!
interface TenGigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/5
  stackwise-virtual dual-active-detection
!
interface TenGigabitEthernet1/1/6
!
interface TenGigabitEthernet1/1/7
  switchport trunk allowed vlan 101,500,700
  switchport mode trunk
  channel-group 2 mode active
!
interface TenGigabitEthernet1/1/8
!
interface FortyGigabitEthernet1/1/1
!
interface FortyGigabitEthernet1/1/2
!
interface TenGigabitEthernet2/0/1
  description connectedToFPRNewX02B
  switchport access vlan 100
  switchport mode access
Configuration Examples

```plaintext
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
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
    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

157
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 stackwise
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
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 vrf-mib 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

158
Configuration Examples

```bash
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
  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)**

```bash
hostname FAN-BS4
!
no aaa new-model
rep ztp
rep autodisc
ptp mode e2etransparent
vtp mode transparent
vtp version 1
!
ip domain name wf.com
!
login on-success log
!
flow exporter 192.168.6.100
  destination 192.168.6.100
  transport udp 6007
!
device-tracking tracking
!
device-tracking policy IPDT_POLICY
  no protocol udp
  tracking enable
!
diagnostic bootup level minimal
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
archive
log config
logging enable
logging size 500
```
memory free low-watermark processor 63461
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause psp
errdisable recovery cause mrp-miscabling
errdisable recovery cause loopdetect
!
alarm-profile defaultPort
  alarm not-operating
  syslog not-operating
  notifies not-operating
!
enable secret 9 $9$WvAxOEesAzfnN.$SmRkA6cTyFxVetsh9504kUwfrc8RwL6bTpBcrpmk3iX.
!
username dna privilege 15 secret 9
  $9$yD0gMv0okBX0RES$GNM0GJx7jEFqdaufVf/IVwO./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-Vl101
ip address dhcp
!
no ip http server
ip http authentication local
no ip http secure-server
ip http client source-interface Vlan101
ip forward-protocol nd
!
ip ssh bulk-mode 131072
ip ssh source-interface Vlan101
ip scp server enable
!
logging source-interface Vlan101
logging host 192.168.6.100
!
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
snmp-server view DNAC-ACCESS iso included
snmp-server trap-source Vlan101
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps power-ethernet police
snmp-server enable traps rep
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
```
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 ips1a
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 attch
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-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
snmp-server enable traps scheduled-test-fail
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
snmp-server enable traps 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 Catalyst Center Day N Templates

Cisco Catalyst Center templates can be used to apply configurations to multiple switches at a time. The following are various templates that can be created on Cisco Catalyst Center for easy configuration changes on wind farm devices.

**VLAN Creation**

```plaintext
clan $vlan_id  
name $vlan_name
```

**Vrf Creation**

```plaintext
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**

```plaintext
interface Vlan$vlan_id  
vrf forwarding $VRF_name  
ip address 10.10.$vlan_id.1 255.255.255.0  
!
```

**Port-channel Creation**

```plaintext
interface $int_one  
channel-group $PCNo mode desirable  
no shut  
interface $int_two  
channel-group $PCNo mode desirable  
no shut
```

**Shut/Unshut an Interface**

```plaintext
# if ($shut == 1)  
interface $int_name  
shut

#else  
interface $int_name  
no shut  
# end
```
Appendix C: Turbine Operator Network Configuration

C9300 Switch:

hostname SCADA-C9300-1
!
!
vrf definition Mgmt-vrf
!
    address-family ipv4
    exit-address-family
!
    address-family ipv6
    exit-address-family
!
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
aaa authentication dot1x default group radius local
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization exec default local
aaa authorization network default group radius local
aaa authorization network MACSEC-UPLINK local
aaa authorization auth-proxy default group radius
aaa authorization credential-download default local
aaa authorization credential-download MACSEC-UPLINK local
aaa accounting identity default start-stop group radius
!
!
aaa attribute list MUST-SECURE
    attribute type linksec-policy must-secure
!
aaa session-id common

! clock timezone UTC 5 30
boot system switch all flash:cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20231115_063559_V17_14_0_13.SSA.bin
switch 1 provision c9300-24ux

! eap profile EAP-PROFILE
    method tls
    pki-trustpoint CA
!
!
! ip routing
!
!
! ip multicast-routing
ip domain name wf.com
!
!
! login on-success log
vtp mode transparent
!
!
Turbine Operator Network Configuration

access-session mac-move deny

key chain MAC-SEC macsec
  key 4000000000000000000000000000000000000000000000000000000000000000
cryptographic-algorithm aes-128-cmac
  key-string CAFECAFECAFECAFECAFECAFE0CAFE0CAFE0
  lifetime local 00:00:00 Jan 1 1993 infinite

crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
  hash sha256

  crypto pki trustpoint TP-self-signed-1953829722
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-1953829722
    revocation-check none
    rsakeypair TP-self-signed-1953829722
    hash sha256

  crypto pki trustpoint my-trustpoint
    enrollment terminal pem
    serial-number none
    ip-address 10.10.101.25
    subject-name C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN=SCADA-C9300-1-Y819.wf.com
    subject-alt-name SCADA-C9300-1-Y819.wf.com
    revocation-check none
    rsakeypair my-4096rsa-key
    hash sha512

  crypto pki trustpoint CA
    enrollment url http://10.20.200.1:80
    serial-number none
    subject-name CN=Y819
    revocation-check none
    rsakeypair my-4096rsa-key
    hash sha512

  crypto pki certificate chain SLA-TrustPoint
    certificate ca 01
    30820321 30820209 A0030201 02002010 30006069 2A864886 F70D0101 0B050030
    32310B00 C060305 040A1305 43697363 6F312030 1E060355 04031317 43697363
    6F204C69 63656E73 69666275 6C6C6572 73736F69 6E6720 52657374 6F72616C
    73732030 33203530 31393438 34375A 170D3338 30353330 31393438 34375A30 32310E30
    0C060355 04031317 43697363 6F204C69 63656E73 69666275 6C6C6572 73736F69 6E6720
    52656669 74656475 73204120 82043413 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
    82010A02 82010100 A6BCBD96 131E05F7 145E72C 2CD686E6 17222EA1 F1EFEF64D
    CB84C798 212AA147 C655D8DD 9741380D 8711441E 1AAF071A 9CAE6398 8A38E520
    1C934D78 462EF239 C659F715 B98CA059 5BBB5CBD 0CFBEBEA3 700A8BF7 D8F256EE
    4AA4E8E0 DB6FD1C9 60B1FD18 FFC69C9E 6F68957 A21617E7 104FDC5F EA2956AC
    7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
    68E69491 20F320E7 948517D A633C84 F10684C7 4BC8E00F 539BA42B 42C68BB7
    C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5DFB88 8F27D191
    C55F0D76 61F9A4CC 3D992327 A8BB03BD 4E6D7069 79B9F8B4 DF5F4368 9515E44E
    DFC76CCF 04D7FD1 02030100 01A34230 40300E06 03551D0F 01FF04 04030201
    06300F06 03551D13 0101FF04 05300301 01FF0301 0603551D 0E01600D 1449DC85
    48BD3D1E 1B3E6A17 606AF333 3D3B4C73 E8300D06 02A86486 86F7D001 010B5000
    03820101 00507F24 D3932A66 862059D9 E838AE5C 6D4DF6B0 49631C78 240DA905
    604ECDCE FF4F0FDB 71FC460E CD63F6DB DD4E681E 3A5673AB 0933DB01 6C9E3D88
    D98987BF EB0CB90E 1A030D02 2189B55C 8F8A8568 CD98B646 55751468 8DFC66AB
    467A3DF4 4D567000 6ADP0F0D CF835015 3C04FF7C 21E878AC 11E9AC02 55A9232C
Turbine Operator Network Configuration

service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template webauth-global-inactive
  inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
  username usr-macsec
  pki-trustpoint CA

memory free low-watermark processor 131696
! diagnostic bootup level minimal
! spanning-tree mode rapid-pvst
spanning-tree extend system-id
! !
mka policy MKA-POLICY
  key-server priority 150
  sak-rekey interval 65535
! !
username usr-macsec aaa attribute list MUST-SECURE
! redundancy
  mode sso
! !
! transceiver type all
  monitoring
! vlan 5
  name Multicast_VLAN
! vlan 10
  name PrivateVLANvlan
    private-vlan primary
    private-vlan association 101,102
! vlan 20
  name IXIA_TrafficTestVLAN
! !
    vlan 101
    name isolated_VLAN
    private-vlan isolated
! !
  vlan 111
  name Management_VLAN
! !
lldp run
! !
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
  event authentication-failure match-all
Turbine Operator Network Configuration

10 class always do-until-failure
terminate dot1x
20 authentication-restart 10
event authentication-success match-all
10 class always do-until-failure
activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
policy-map system-cpp-policy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
Turbine Operator Network Configuration

interface TenGigabitEthernet1/0/12

interface TenGigabitEthernet1/0/13

interface TenGigabitEthernet1/0/14

interface TenGigabitEthernet1/0/15

interface TenGigabitEthernet1/0/16

interface TenGigabitEthernet1/0/17

interface TenGigabitEthernet1/0/18

interface TenGigabitEthernet1/0/19

interface TenGigabitEthernet1/0/20

interface TenGigabitEthernet1/0/21

interface TenGigabitEthernet1/0/22
  switchport mode trunk
  macsec network-link
  access-session host-mode multi-host
  access-session closed
  access-session port-control auto
  channel-group 1 mode active
  service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK

interface TenGigabitEthernet1/0/23
  switchport private-vlan mapping 10 101
  switchport mode private-vlan promiscuous

interface TenGigabitEthernet1/0/24
  switchport mode trunk
  macsec network-link
  access-session host-mode multi-host
  access-session closed
  access-session port-control auto
  channel-group 1 mode active
  service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK

interface GigabitEthernet1/1/1
  switchport mode private-vlan promiscuous

interface GigabitEthernet1/1/2

interface GigabitEthernet1/1/3

interface GigabitEthernet1/1/4

interface TenGigabitEthernet1/1/1
  switchport mode trunk
  rep segment 1 edge
  macsec network-link
  mka policy MKA-POLICY
  mka pre-shared-key key-chain MAC-SEC
  service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK

interface TenGigabitEthernet1/1/2
  switchport mode trunk
  mka policy MKA-POLICY
  mka pre-shared-key key-chain MAC-SEC

interface TenGigabitEthernet1/1/3

interface TenGigabitEthernet1/1/4
Turbine Operator Network Configuration

interface TenGigabitEthernet1/1/5
!
interface TenGigabitEthernet1/1/6
!
interface TenGigabitEthernet1/1/7
!
interface TenGigabitEthernet1/1/8
!
interface FortyGigabitEthernet1/1/1
!
interface FortyGigabitEthernet1/1/2
!
interface TwentyFiveGigE1/1/1
!
interface TwentyFiveGigE1/1/2
!
interface AppGigabitEthernet1/0/1
!
interface Vlan1
  no ip address
!
interface Vlan5
  ip address 10.5.1.2 255.255.0.0
  ip pim sparse-mode
  standby 5 ip 10.5.1.1
  private-vlan mapping 501,502
!
interface Vlan10
  ip address 10.10.1.2 255.255.255.0
  standby 1 ip 10.10.1.1
  standby 1 priority 105
  private-vlan mapping 101,102
!
interface Vlan20
  ip address 10.20.1.2 255.255.0.0
  standby 20 ip 10.20.1.1
!
interface Vlan100
  ip address 10.10.100.2 255.255.255.0
!
interface Vlan111
  ip address 10.111.1.2 255.255.255.0
  ip helper-address 10.10.1.10
  standby 111 ip 10.111.1.1
!
router ospf 1
  network 1.1.1.0 0.0.0.255 area 0
  network 10.1.0.0 0.0.255.255 area 0
  network 10.10.1.0 0.0.255.255 area 0
  network 10.10.100.0 0.0.255.255 area 0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip pim rp-address 10.5.1.1
ip ssh bulk-mode 131072
!
!
!
!
control-plane
  service-policy input system-cpp-policy
!
!
Turbine Operator Network Configuration

```bash
line con 0
    stopbits 1
line vty 0 4
    transport input ssh
line vty 5 31
    transport input ssh
!
call-home
    ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
    ! the email address configured in Cisco Smart License Portal will be used as contact email address to
    ! send SCH notifications.
    contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
        destination transport-method http
ntp server 10.10.1.10
!
!
!
!
!
end

IE9320 Switch:

```bash
hostname WF-SCADA-IE9320-1
!
no logging console
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
    aaa authentication dot1x MACSEC-UPLINK local
    aaa authorization network MACSEC-UPLINK local
    aaa authorization credential-download MACSEC-UPLINK local
!
    aaa attribute list MUST-SECURE
        attribute type linksec-policy must-secure
!
    aaa session-id common
!
!
    clock timezone UTC 5 30
boot system switch all flash:ie9k_iosxe.BLD_POLARIS_DEV_LATEST_20240313_033241_V17_15_0_18.SSA.bin
switch 1 provision ie-9320-22s2c4x
eap profile EAP-PROFILE
    method tls
    pki-trustpoint CA
!
rep ztp
!
!
!
ip routing
!
!
!
login on-success log
```
Turbine Operator Network Configuration

vtp mode transparent
!
!
!
!
!
access-session mac-move deny
!
key chain MAC-SEC macsec
key 4000000000000000000000000000000000000000000000000000000000000000

  cryptographic-algorithm aes-128-cmac
  key-string CAFECafeCAFECAFE0CAFE0CAFE0CAFE0

  lifetime local 00:00:00 Jan 1 1993 infinite
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pks12
  revocation-check crl
  hash sha256
!
crypto pki trustpoint TP-self-signed-2076045765
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2076045765
  revocation-check none
  rsakeypair TP-self-signed-2076045765
  hash sha256
!
crypto pki trustpoint my-trustpoint
  enrollment terminal pem
  serial-number none
  ip-address none
  subject-name C=IN, ST=KAR, L=BLR, O=cisco, OU=IOT, CN=WF-SCADA-IE9320-1.wf.com
  subject-alt-name WF-SCADA-IE9320-1.wf.com
  revocation-check none
  rsakeypair my-4096rsa-key
  hash sha256
!
crypto pki trustpoint CA
  enrollment url http://10.20.200.1:80
  serial-number
  fqdn IE9320-1.wf.com
  ip-address none
  subject-name CN=IE9320-1
  subject-alt-name IE9320-1.wf.com
  revocation-check none
  rsakeypair myrsakeys
  auto-enroll regenerate
  hash sha512
!
crypto pki certificate chain SLA-TrustPoint
  certificate ca 01
  30820321 30820209 A0D02021 02020101 300D0609 2A864886 F70D0101 0B300303
  32310830 0C060355 040A1305 43697363 6F312030 05030101 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B4790B6 B4CB2D62 EA2F505D 7B062A4A 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3DF925327 ABBB03BD 4ED706E9 7CBADF8B DF5F4368 95135E44
  DBC7C6CF 04D7FD1D 02030100 01A54230 40300E06 03551D0F 0101FF04 04303021
  06300F06 03551D13 0101FF04 05300301 01FF301D 0630551D 0E041604 1449DC85
  4B3D31E5 1B386A17 606AF333 303B4C73 E8300D06 092A8648 86F70D01 0B050030
Cisco Solution for Renewable Energy – Wind Farm 1.1 Implementation Guide

1. Implementation Guide

Turbine Operator Network Configuration

quit
crypto pki certificate chain TP-self-signed-2076045765
crypto pki certificate chain my-trustpoint
certificate ca 3557E375F43B3AA14CC7023E5EF23AD1

quit
certificate ca 3557E375F43B3AA14CC7023E5EF23AD1

Cisco Solution for Renewable Energy – Wind Farm 1 Implementation Guide

Turbine Operator Network Configuration

1. Implementation Guide

1.1 Turbine Operator Network Configuration

crypto pki certificate chain CA

quit

Certificate ca

Certificate 09

Certificate 01

quit

Certificate chain
Cisco Solution for Renewable Energy – Wind Farm 1.1 Implementation Guide

Turbine Operator Network Configuration

7E606F4B 68ACDE7B 5F55AE4E 7084FA8D C6C44B9A 06445DB7 CD32D8C7 EE37393C
9E3575FD DF3ACCF6 0A8E5C49 0A76466C E6D5F6C3 C7C75F01 0646F6CE 16BF7DB6
OC13A497 D8C1EEFF 3A4A67EE 42922309 9D7E876F F3985091 4AF824C2 E62151F1
B7231AD3 5CA1C579 D79FD49D 30E24DEF DD93905D 8CD1FEFF 56F1111F BE1D0E74
D6E2F32C C864A2ED 327F8F65 6A30DB31 A254182B D4ACC070 DEABFE4C 915FBC9
02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
OF0101FF 04003002 01B6301F 0603551D 23041830 16801413 07525E86 08919689
D8F1F231 40C3D3DA 76D14430 1D0D0535 1D0E0416 0411307 525E8608 9D1968D8
OF123410 C3D3DA6E D144300D 06092A86 4886F70D 01010D05 00382020 01005105
B8AD3E39 A6B19533 3D029858 35FC67B7 CEF78131 AD879855 B2C70C8D 4E907D0A
AE86430A E56F399B B95AA07 C21A0D8 C90ECB5 F5B42F69 028FE47D D551E18B
237357F6 05250D01 4B26A6E1 9C313260 491421E0 A00AAE56 FE196B18 A43E9D54
A754FCE5 B8758B34 80A4B0F0 8015A7C6 09D111CE 5C1A7BE 26447759 FAFC73A6
07F2270F 1768CA0F 90AEB12A 35AF668A 945721B5 ABBB2641 B31B8D88 CE098C19
F6B8B6AB 91046FC9 E37558EE 433BA7FD 19F16F4E 1C4F1A4A 8E06217B 5A3469D0
2419B10F 711AA2C8 BC265E28 F2738D58 F9547857 22C6CBD7 D79C27B0 52E3C6E5
D8F0A10E 33D47C6C D90429B0 BAEB545F EAE8F78E D48662B8 2B67D7B8 4805B1A7
D0790E88 31482F89 410B7A71 3CC376CA 5375D649 AFB76307 C5A8E5E9 5928A7E2
6C705E59 32985A51 F0B10A18 96252952 80DFBBFA BE7A9605 4B8060A6 987908B7
02D1143D 7A81212D 21EFD363 9C340845 4283E29E C21C6D08 8A1452FE 160BCF0D
78BFFC73 6E909872 7AC5939C B593A736 F0031BE3 B428A015 C704911F A1FF4C63
FDA27A33 DE55B66B FB523B64 01818D35 5F54C28 95706297 5D448512 3A88D8C9
8B10A9DF 2CAAC1518 CF24DC21 8182A61A 97166F5F 7555D858 84BCF89F CF62DB88
FF88B0F8 6638D179 62F1FA7E 026FA05E A5633F16 4FB6B154 EB13F55 41CE3E34
A9700577 59F02AF F63DB02F D8309514 F3A812D7 9E76BF4B 2C2C8DA3 DA 92

quit
!

service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template webauth-global-inactive
inactivity-timer 3600
dot1x system-auth-control
memory free low-watermark processor 59462

! diagnostic bootup level minimal
! spanning-tree mode rapid-pvst
spanning-tree extend system-id
! !
!
alarm-profile defaultPort
alarm not-operating
syslog not-operating
notifies not-operating
!
!
mka policy MKA-POLICY
key-server priority 150
sak-rekey interval 65535
mka policy MKAPolicy
macsec-cipher-suite gcm-aes-128 gcm-aes-256
!
!
username dna aaa attribute list MUST-SECURE
username usr-macsec aaa attribute list MUST-SECURE
!
redundancy
mode sso
!
Turbine Operator Network Configuration

vlan 5
  name Multicast_VLAN

vlan 10
  name PrivateVLANvlan
    private-vlan primary
    private-vlan association 101,102

vlan 20
  name IXIA_TrafficTestVLAN

  vlan 101
    name isolated_VLAN
    private-vlan isolated

vlan 111
  name Management_VLAN

lldp timer 5
lldp holdtime 20
lldp run

class-map match-any system-cpp-police-ewlc-control
description EWLC Control
class-map match-any system-cpp-police-topology-control
description Topology control
class-map match-any system-cpp-police-sw-forward
description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any LevelHPD
  match dscp cs3 af31 af32 af33 cs4 af41 af42 af43
class-map match-any system-cpp-default
description EWLC data, Inter FED Traffic
class-map match-any LevelLPD
  match dscp default cs1
class-map match-any LevelMPD
  match dscp cs2 af21 af22 af23
class-map match-any system-cpp-police-sys-data
description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any LevelMCD
  match dscp cs5 ef cs6 cs7

policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
event authentication-failure match-all
  10 class always do-until-failure
  10 terminate dot1x
  20 authentication-restart 10
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE

policy-map system-cpp-policy
Turbine Operator Network Configuration

```plaintext
! interface GigabitEthernet1/0/1
! interface GigabitEthernet1/0/2
! interface GigabitEthernet1/0/3
! interface GigabitEthernet1/0/4
! switchport access vlan 10
! switchport mode access
! spanning-tree portfast
! spanning-tree bpduguard enable
! interface GigabitEthernet1/0/5
! switchport access vlan 5
! switchport mode access
! interface GigabitEthernet1/0/6
! interface GigabitEthernet1/0/7
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
! interface GigabitEthernet1/0/10
! interface GigabitEthernet1/0/11
! switchport voice vlan dot1p
! interface GigabitEthernet1/0/12
! interface GigabitEthernet1/0/13
! interface GigabitEthernet1/0/14
! interface GigabitEthernet1/0/15
! interface GigabitEthernet1/0/16
! interface GigabitEthernet1/0/17
! interface GigabitEthernet1/0/18
! interface GigabitEthernet1/0/19
! interface GigabitEthernet1/0/20
! interface GigabitEthernet1/0/21
! interface GigabitEthernet1/0/22
! interface GigabitEthernet1/0/23
! switchport access vlan 10
! switchport mode access
! interface GigabitEthernet1/0/24
! interface TenGigabitEthernet1/0/25
! switchport mode trunk
! rep segment 100 edge
! macsec network-link
```
Turbine Operator Network Configuration

```plaintext
service-policy type control subscriber DOT1X-MUST-SECURE-UPLINK
!
interface TenGigabitEthernet1/0/26
  switchport private-vlan host-association 10 101
    switchport mode trunk
!
interface TenGigabitEthernet1/0/27
  switchport mode trunk
  rep segment 1
  macsec network-link
  mka policy MKA-POLICY
  mka pre-shared-key key-chain MAC-SEC
!
interface TenGigabitEthernet1/0/28
  switchport mode trunk
  rep segment 1
  macsec network-link
!
interface AppGigabitEthernet1/0/1
  switchport voice vlan dot1p
!
interface Vlan1
  no ip address
!
interface Vlan111
  ip address 10.111.1.4 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip ssh bulk-mode 131072
!
snmp-server community private RW
snmp-server community public RO
!
!
control-plane
  service-policy input system-cpp-policy
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
!
ntp server 10.10.1.10
!
ptp clock transparent domain 0 profile default
!
!
!
!
!
!
end
```
FSN Switch:

hostname WF-SCADA-FSN-Switch
!
!
no logging console
aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK
!
!
aaa authentication dot1x MACSEC-UPLINK local
aaa authorization network MACSEC-UPLINK local
aaa authorization credential-download MACSEC-UPLINK local
!
!
aaa attribute list MUST-SECURE
  attribute type linksec-policy must-secure
!
aaa session-id common
clock timezone UTC 5 30
rep ztp
rep autodisc
iedt refresh-interval 21600
eap profile EAP-PROFILE
  method tls
  pki-trustpoint CA
!
ptp mode e2etransparent
vtp mode transparent
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
access-session mac-move deny
!
key chain MAC-SEC macsec
  key 4000000000000000000000000000000000000000000000000000000000000000
  cryptographic-algorithm aes-128-cmac
  key-string CAFECAFECAFECAFE0CAFE0CAFE0CAFE0CAFE0CAFE0CAFE0
  lifetime local 00:00:00 Jan 1 1993 infinite
!
crypto pki trustpoint CA
  enrollment url http://10.20.200.1:80
  serial-number
  fqdn VOSZ.wf.com
  ip-address none
  subject-name CN=VOSZ
  subject-alt-name VOSZ.wf.com
  revocation-check none
  rsakeypair myrsakeys
  hash sha512
!
crypto pki certificate chain CA
  certificate 02
    3082052F 30820317 A0030201 02020102 300D609 2A864886 F70D0101 0D050030

184
Cisco Solution for Renewable Energy – Wind Farm 1 Implementation Guide

Turbine Operator Network Configuration

| GE103C30 | 0A060355 | 04031303 | 49535230 | 1E170D32 | 33313232 | 32303631 | 3730323A |
| 170D3224 | 31323231 | 30363137 | 30322A30 | 3F301D30 | 0B305030 | 04305034 | 5630535A |
| 31283012 | 06035050 | 05130346 | 4F343224 | 32395360 | 5353A030 | 06092A36 | 486F5F0D |
| 01090216 | 05653053 | 022C3733 | 2B363560 | 30022202 | 300D0609 | 2A864886 | F7D00101 |
| 01050003 | 82008200 | 82002820 | 0098D808 | D8135238 | F8B4617A | D655DA6A |
| FCE973F9 | 1E366D82 | 610BAFFF | 16102218 | A8A1883A | EB19878C | 1A534AA0 | 5ED7058A |
| 1655BB6E | 0C3D3E68 | B5D588AE | B1F6F6DF | E39C388B | 77F59A6E | 891EF289 | 6CCF9FCC |

185
Turbine Operator Network Configuration

AE86430A E5F6399B 8B95A07 C2C1ADC8 AD90ECB5 F5B42F69 028EFE47 D551E18B
237357F6 0525DOE1 4B2CAEE1 9C331260 491421E0 A00AAE96 FE196B18 A43E9D54
A754FC5B B8756B34 082A4B0F 8015A7C6 09DD11CE 5CE1A7BE 26447759 FAF73A6
07F2270F 1768CA0F 90AEB12A 35AF668A 945721B5 ABB264A1 B31B8D88 CE098C19
F6BBAB89 91046FC9 E37558EE 433BA7FD 19F16F4E 1C4FA14A 8E06217B 5A3469D0
0419B1EF 711A2C8E BC25E628 F273B5D8 F954B875 22C6CBDF D79C27B0 5B36EC5
D8F0AE19 33D4B7C6 D90429B0 BAA5455F EABE8F78 E48662B8 2B6FD7B4 8405B1A7
D0790E88 31482F89 410D7A31 3CC376CA 5375D649 ABF76307 C5A6E5E9 59B7A8E
6C705E59 32985A51 F0B10A18 96252952 80DFBBFA BE7A9605 4B8060A6 98790B17
02D143D 7A8121D2 21F7DE23 9C934085 42B35E29 CE11C60B 8A1452F2 160BCFD0
7BBF6763 6E909872 7AC5939C B593A376 F0031BE3 B428A015 C07941FF A1EF4C63
FDA7A33 DE55B66 FB52B3AE 01818D63 5FE54C28 95706297 5D448562 3A380D9C
8B1AD05F 2A1A5181 CF24DC21 8182A63A 97166FF5 7555D85F 84BCF8F9 CF06DBBA
FF88F098 6638D179 62F1FA7E 026FA05E A5633F16 4FB6514 EBF135F5 41CE34C
A9700577 591F02AF FD3DB02F D8390514 F3A812D7 9E76BF4B 2C2C0A3 DA 92
quit
!
!
diagnostic bootup level minimal
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
  linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template webauth-global-inactive
  inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
  username usr-macsec
  pki-trustpoint CA
! license boot level network-advantage
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 64978
!
!
alarm-profile defaultPort
  alarm not-operating
  syslog not-operating
  notifies not-operating
!
!
mka policy MKA-POLICY
  key-server priority 150
  sak-rekey interval 65535
!
username usr-macsec aaa attribute list MUST-SECURE

crypto engine compliance shield disable
!
!
transceiver type all
  monitoring
!
!
_vlan 5
  name Multicast_VLAN
!
_vlan 10
  name PrivateVLANvlan
Cisco Solution for Renewable Energy – Wind Farm 1.1 Implementation Guide

Turbine Operator Network Configuration

```
private-vlan primary
private-vlan association 101,102
!
vlan 20
name IXIA_TrafficTestVLAN
!

vlan 101
name isolated_VLAN
private-vlan isolated
!
vlan 111
name Management_VLAN
!
!
lldp timer 5
lldp holdtime 20
lldp run
!
!
class-map match-any MCD
  match dscp cs5 ef cs6 cs7
class-map match-any LPD
  match dscp default cs1
class-map match-any MPD
  match dscp cs2 af21 af22 af23
class-map match-any HPD
  match dscp cs3 af31 af32 af33 cs4 af41 af42 af43
  match access-group name QoS_ACL
!
class-map match-all HPD_Output
  match dscp cs4
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
      event authentication-failure match-all
        10 class always do-until-failure
        10 terminate dot1x
        20 authentication-restart 10
      event authentication-success match-all
        10 class always do-until-failure
        10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
!
policy-map WF_SCADA_Ingress_Policy
class MCD
  set ip dscp ef
class HPD
  set ip dscp cs4
class MPD
  set ip dscp cs2
class LPD
  set ip dscp cs1
!
policy-map WF_SCADA_Egress_Policy
class MCD
  priority
      queue-limit 48 packets
class MPD
  bandwidth remaining percent 30
      queue-limit 48 packets
class LPD
  bandwidth remaining percent 30
      queue-limit 272 packets
class HPD_Output
  bandwidth remaining percent 40
```
Turbine Operator Network Configuration

queue-limit 48 packets

interface GigabitEthernet1/1
  switchport mode trunk
    rep segment 100
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/2
  switchport mode trunk
    rep segment 100
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/3
  description PNP STARTUP VLAN
  switchport access vlan 5
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/4
  switchport access vlan 9
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/5
  switchport access vlan 59
  switchport mode access
  ip access-group DAUNU_ACL out
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/6
  description ##ConnectedToWindowsCA##
  switchport mode private-vlan host
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/7
  switchport private-vlan mapping 10 101-102
  switchport mode private-vlan promiscuous
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!

interface GigabitEthernet1/8
Turbine Operator Network Configuration

service-policy input WF_SCADA_Ingress_Policy
service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/9
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!
interface GigabitEthernet1/10
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
!
interface AppGigabitEthernet1/1
!
interface Vlan1
  no ip address
  shutdown
!
!
interface Vlan111
  ip address dhcp
!
  ip http server
  ip http authentication local
  ip http secure-server
  ip forward-protocol nd
!
  ip ssh bulk-mode 131072
!
  ip access-list extended QoS_ACL
    10 permit ip 10.1.10.0 0.0.0.255 any
!
  snmp-server community private RW
  snmp-server community public RO
  snmp-server contact Switch
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
!
ntp server 10.10.1.10
!
!
!
!
!
!
!
!
!
!
!
!
!
!
End
Turbine Operator Network Configuration

TSN Switch:

hostname WF-SCADA-TSN

aaa new-model
aaa local authentication MACSEC-UPLINK authorization MACSEC-UPLINK

aaa authentication dot1x MACSEC-UPLINK local
aaa authorization network MACSEC-UPLINK local
aaa authorization credential-download MACSEC-UPLINK local

aaa attribute list MUST-SECURE
  attribute type linksec-policy must-secure

aaa session-id common
clock timezone UTC 5 30
rep ztp
rep autodisc
iedt refresh-interval 21600
eap profile EAP-PROFILE
  method tls
  pki-trustpoint CA

ptp mode e2ettransparent
vtp mode transparent

login on-success log

access-session mac-move deny

crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
  hash sha256

crypto pki trustpoint TP-self-signed-4060431784
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-4060431784
  revocation-check none
  rsakeypair TP-self-signed-4060431784
  hash sha256

crypto pki trustpoint CA
  enrollment url http://10.20.200.1:80
  serial-number
  fqdn Y1SL
  ip-address none
  subject-name CN=Y1SL
  revocation-check none
  rsakeypair my-4096rsa-key
  hash sha512

crypto pki certificate chain SLA-TrustPoint
**Turbine Operator Network Configuration**

certificate ca 01
30820321 30820209 A0030201 02020101 30D0609 2A864886 F70D0101 0B500503
32310E30 0C060355 04A1A05 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63566E73 696E6720 526F6F74 20434310 1E170D31 333C6353 30313934
383437A5 170D3333 30353333 31393438 34375A30 32310E30 0C060355 04A1A05
34697363 6F312030 04031317 43697363 6F204C69 63566E73 696E6720 526F6F74
526F6F74 20434310 1E170D31 333C6353 30313934

diagnostic bootup level minimal
crypto pki certificate chain CA

crypto pki certificate chain Win-CA
quit
5EC534B8 E45FD0A4 BC621619 76F6130F B2D11423
604841B3 6C7EB94C FE913E04 F56A0C9C A0FDD762 72C6EE9E A3C7BF2D 22D5A17E
B7F907FB AE91CBAA 1BF49B7C E32BA7BC 4AB210D6 643BF417 147BDE71 ABA998D6
3BB1783D 1E440857 BB703128 D38BD9C5 45B0BA5A 557F3A49 DEABB46C 97A629F7
9029305F 00E80514
604841B3 6C7EB94C FE913E04 F56A0C9C A0FDD762 72C6EE9E A3C7BF2D 22D5A17E
5EC534B8 E45FD0A4 BC621619 76F6130F B2D11423
Cisco Solution for Renewable Energy – Wind Farm 1.1 Implementation Guide
Cisco Solution for Renewable Energy – Wind Farm 1.1 Implementation Guide

Turbine Operator Network Configuration

```
service-template webauth-global-inactive
  inactivity-timer 3600
dot1x system-auth-control
dot1x credentials DOT1X-CREDS
username usr-macsec
  pki-trustpoint CA
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88360
!
!
alarm-profile defaultPort
  alarm not-operating
  syslog not-operating
  notifies not-operating
!
!
username usr-macsec aaa attribute list MUST-SECURE

crypto engine compliance shield disable
!
!
transceiver type all
  monitoring
vlan internal allocation policy ascending
!
vlan 5
  name Multicast_VLAN
!
vlan 10
  name PrivateVLANvlan
    private-vlan primary
    private-vlan association 101,102
!
vlan 20
  name IXIA_TrafficTestVLAN
!

  vlan 101
    name isolated_VLAN
    private-vlan isolated
!
vlan 111
  name Management_VLAN
!
!
lldp timer 5
lldp holdtime 20
lldp run
!
!
policy-map type control subscriber DOT1X-MUST-SECURE-UPLINK
  event session-started match-all
    10 class always do-untill-failure
  10 authenticate using dot1x aaa authc-list MACSEC-UPLINK authz-list MACSEC-UPLINK both
  event authentication-failure match-all
    10 class always do-untill-failure
    10 terminate dot1x
    20 authentication-restart 10
```
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE

interface GigabitEthernet1/1
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/2
  switchport mode trunk
  rep segment 101
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/3
  switchport mode trunk
  rep segment 101
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/4
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/5
  switchport access vlan 5
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/6
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/7
  description Connected to WF-SCADA-UCS 10_64_66_115 vmnic7
  switchport host-association 10 101
  switchport mode private-vlan host
  speed 1000
duplex full
  spanning-tree portfast
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/8
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/9
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy

interface GigabitEthernet1/10
  service-policy input WF_SCADA_Ingress_Policy
  service-policy output WF_SCADA_Egress_Policy
Turbine Operator Network Configuration

```plaintext
service-policy output WF_SCADA_Egress_Policy

interface AppGigabitEthernet1/1

interface Vlan1
    no ip address

interface Vlan111
    ip address dhcp
    ip http server
    ip http authentication local
    ip http secure-server
    ip forward-protocol nd
    ip ssh bulk-mode 131072

    ip access-list extended QoS_ACL
    10 permit ip 10.1.10.0 0.0.0.255 any

snmp-server community private RW
snmp-server community public RO
snmp-server contact Switch

control-plane

line con 0
    stopbits 1
line aux 0
line vty 0 4
    transport input ssh
line vty 5 15
    transport input ssh

ntp server 10.10.1.10

contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
    destination transport-method http

end
```
CA server sample configuration for auto-enrollment:

```
crypto pki server CA
no database archive
issuer-name CN=ISR
grant auto
hash sha512
!
crypto pki trustpoint CA
revocation-check crl
rsakeypair CARsaKeys
!
```
# Acronyms and Initialisms

The following table summarizes the acronyms and initialisms that apply to a wind farm solution.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>4G LTE</td>
<td>Fourth generation long-term evolution</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, authorization, and accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>Access control list</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>ADM</td>
<td>Axis device manager</td>
</tr>
<tr>
<td>AIS</td>
<td>Automatic identification system</td>
</tr>
<tr>
<td>AMP</td>
<td>Advanced malware protection</td>
</tr>
<tr>
<td>AP</td>
<td>Access point</td>
</tr>
<tr>
<td>ARP</td>
<td>Address resolution protocol</td>
</tr>
<tr>
<td>AVC</td>
<td>Application visibility and control</td>
</tr>
<tr>
<td>BGP</td>
<td>Border gateway protocol</td>
</tr>
<tr>
<td>BS (Turbine)</td>
<td>Base switch</td>
</tr>
<tr>
<td>BW</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate authority</td>
</tr>
<tr>
<td>CBWFQ</td>
<td>Class-based weighted fair queuing</td>
</tr>
<tr>
<td>CC</td>
<td>Control venter</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed circuit television</td>
</tr>
<tr>
<td>CDN</td>
<td>Cisco Developer Network</td>
</tr>
<tr>
<td>CE</td>
<td>Carrier Ethernet</td>
</tr>
<tr>
<td>Cisco Catalyst Center</td>
<td>Cisco Digital Network Architecture Center</td>
</tr>
<tr>
<td>CLI</td>
<td>Command line interface</td>
</tr>
<tr>
<td>CoS</td>
<td>Class of service</td>
</tr>
<tr>
<td>CTS</td>
<td>Cisco Trustsec</td>
</tr>
<tr>
<td>URWB</td>
<td>Cisco Ultra Reliable Wireless Backhaul</td>
</tr>
<tr>
<td>CV</td>
<td>(Cisco) Cyber Vision</td>
</tr>
<tr>
<td>CVC</td>
<td>Cisco Cyber Vision Center</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>DAD</td>
<td>Dual active detection</td>
</tr>
<tr>
<td>DC</td>
<td>Data center</td>
</tr>
</tbody>
</table>
## Acronyms and Initialisms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Dynamic host configuration protocol</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain names system</td>
</tr>
<tr>
<td>DODAG</td>
<td>Destination oriented directed acrylic graph</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of service</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated services code point</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated short-range communications</td>
</tr>
<tr>
<td>EB</td>
<td>Enhanced beacon; external border</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic curve cryptography</td>
</tr>
<tr>
<td>ECMP</td>
<td>Equal-cost multi path</td>
</tr>
<tr>
<td>EEBL</td>
<td>Emergency electronic brake lights</td>
</tr>
<tr>
<td>EID</td>
<td>End point identifier</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced interior gateway routing protocol</td>
</tr>
<tr>
<td>EN</td>
<td>Extended nodes</td>
</tr>
<tr>
<td>EP</td>
<td>Endpoint</td>
</tr>
<tr>
<td>ETS</td>
<td>European teletoll services</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EVA</td>
<td>Emergency vehicle alert</td>
</tr>
<tr>
<td>FAN</td>
<td>Farm area network</td>
</tr>
<tr>
<td>FAR</td>
<td>Field area router</td>
</tr>
<tr>
<td>FC</td>
<td>Fiber channel</td>
</tr>
<tr>
<td>FCAPS</td>
<td>Enhanced fault, configuration, accounting, performance, and security</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FCoE</td>
<td>Fiber channel over Ethernet</td>
</tr>
<tr>
<td>FCW</td>
<td>Forward collision warning</td>
</tr>
<tr>
<td>FE</td>
<td>Fabric edges</td>
</tr>
<tr>
<td>FI</td>
<td>Fabric interconnects</td>
</tr>
<tr>
<td>FiaB</td>
<td>Fabric in a box</td>
</tr>
<tr>
<td>FM</td>
<td>FluidMesh</td>
</tr>
<tr>
<td>FMC</td>
<td>Firepower Management Center</td>
</tr>
<tr>
<td>FND</td>
<td>(Cisco) Field Network Director</td>
</tr>
<tr>
<td>FNF</td>
<td>Flexible NetFlow</td>
</tr>
<tr>
<td>FP</td>
<td>Firepower</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>FW</td>
<td>Firewall</td>
</tr>
<tr>
<td>HA</td>
<td>High availability</td>
</tr>
<tr>
<td>HER</td>
<td>Headend router</td>
</tr>
<tr>
<td>HMI</td>
<td>Human machine interface</td>
</tr>
<tr>
<td>HQ</td>
<td>Headquarter</td>
</tr>
<tr>
<td>HQoS</td>
<td>Hierarchical quality of service</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot standby router protocol</td>
</tr>
<tr>
<td>HTDB</td>
<td>Host Tracking Database</td>
</tr>
<tr>
<td>I/O</td>
<td>Input and output</td>
</tr>
<tr>
<td>IA</td>
<td>Industrial automation</td>
</tr>
<tr>
<td>IB</td>
<td>Internal border</td>
</tr>
<tr>
<td>ICA</td>
<td>Intersection collision avoidance</td>
</tr>
<tr>
<td>IE</td>
<td>(Cisco) Industrial Ethernet</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent end device</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet key exchange</td>
</tr>
<tr>
<td>IMA</td>
<td>Intersection movement assist</td>
</tr>
<tr>
<td>IOT</td>
<td>Internet of things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>IPAM</td>
<td>IP address management</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet protocol security</td>
</tr>
<tr>
<td>IR</td>
<td>Cisco Industrial Router</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet small computer systems interface</td>
</tr>
<tr>
<td>ISE</td>
<td>(Cisco) Identity Services Engine</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 tunneling protocol</td>
</tr>
<tr>
<td>L3VPN</td>
<td>Layer 3 virtual private network</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>LER</td>
<td>Label edge router</td>
</tr>
<tr>
<td>LG</td>
<td>Cimcon LightingGale</td>
</tr>
<tr>
<td>LLG</td>
<td>Least loaded gateway</td>
</tr>
<tr>
<td>LoRa</td>
<td>Long range</td>
</tr>
<tr>
<td>LoRaWAN</td>
<td>Long range WAN</td>
</tr>
</tbody>
</table>
### Acronyms and Initialisms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>Label switched Path</td>
</tr>
<tr>
<td>LSR</td>
<td>Label switched router</td>
</tr>
<tr>
<td>MAC</td>
<td>Media access control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan area network</td>
</tr>
<tr>
<td>ME</td>
<td>Mesh end</td>
</tr>
<tr>
<td>MIC</td>
<td>Message integrity code</td>
</tr>
<tr>
<td>MMS</td>
<td>Manufacturing message specification</td>
</tr>
<tr>
<td>MNT</td>
<td>Monitoring node</td>
</tr>
<tr>
<td>MP</td>
<td>Mesh point</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-protocol label switching</td>
</tr>
<tr>
<td>MQC</td>
<td>Modular QoS CLI</td>
</tr>
<tr>
<td>MRP</td>
<td>Media redundancy protocol</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit</td>
</tr>
<tr>
<td>MUD</td>
<td>Manufacture usage description</td>
</tr>
<tr>
<td>NAN</td>
<td>Neighborhood area network</td>
</tr>
<tr>
<td>NAT</td>
<td>Network address translation</td>
</tr>
<tr>
<td>NBAR2</td>
<td>Cisco Next Generation Network-Based Application Recognition</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next general firewall</td>
</tr>
<tr>
<td>NGIPS</td>
<td>Next-generation intrusion prevention system</td>
</tr>
<tr>
<td>NMS</td>
<td>Network management system</td>
</tr>
<tr>
<td>NOC</td>
<td>Network operations center</td>
</tr>
<tr>
<td>NS</td>
<td>(Turbine) nacelle switch</td>
</tr>
<tr>
<td>NSF/SSO</td>
<td>Non-stop forwarding with stateful switchover</td>
</tr>
<tr>
<td>NTP</td>
<td>Network time protocol</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, administration, and management</td>
</tr>
<tr>
<td>OBU</td>
<td>On-board unit</td>
</tr>
<tr>
<td>OEM</td>
<td>Original equipment manufacturer</td>
</tr>
<tr>
<td>OFTO</td>
<td>Offshore transmission owner</td>
</tr>
<tr>
<td>ONSS</td>
<td>Onshore substation</td>
</tr>
<tr>
<td>OPC UA</td>
<td>Open platform communications unified architecture</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open shortest path first</td>
</tr>
<tr>
<td>OSS</td>
<td>Offshore substation</td>
</tr>
<tr>
<td>OT</td>
<td>Operational technology</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>OTAA</td>
<td>Over the air activation</td>
</tr>
<tr>
<td>PAgP</td>
<td>Port aggregated protocol</td>
</tr>
<tr>
<td>PAN</td>
<td>Policy administration node; personal area network</td>
</tr>
<tr>
<td>PCA</td>
<td>Pedestrian crossing assist</td>
</tr>
<tr>
<td>PEN</td>
<td>Policy extended node</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy enforcement point</td>
</tr>
<tr>
<td>PHB</td>
<td>Per hop behavior</td>
</tr>
<tr>
<td>PIM-ASM</td>
<td>Protocol independent multicast - any source multicast</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Power line communication</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PoP</td>
<td>Point of presence</td>
</tr>
<tr>
<td>PQ</td>
<td>Priority queuing</td>
</tr>
<tr>
<td>PQ</td>
<td>Priority Queuing</td>
</tr>
<tr>
<td>PRP</td>
<td>Parallel redundancy protocol</td>
</tr>
<tr>
<td>PSM</td>
<td>Personal safety message</td>
</tr>
<tr>
<td>PSN</td>
<td>Policy services node</td>
</tr>
<tr>
<td>PVD</td>
<td>Probe vehicle data</td>
</tr>
<tr>
<td>PVM</td>
<td>Probe vehicle management</td>
</tr>
<tr>
<td>PXG</td>
<td>Platform exchange grid node</td>
</tr>
<tr>
<td>pxGrid</td>
<td>Platform exchange grid</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote authentication dial-in user service</td>
</tr>
<tr>
<td>REP</td>
<td>Resilient Ethernet protocol</td>
</tr>
<tr>
<td>RLOC</td>
<td>Routing locator</td>
</tr>
<tr>
<td>RLVW</td>
<td>Red light violation warning</td>
</tr>
<tr>
<td>RPL</td>
<td>Routing protocol for low-power and lossy networks</td>
</tr>
<tr>
<td>RPoPs</td>
<td>Remote points-of-presence</td>
</tr>
<tr>
<td>RSA</td>
<td>Roadside alert</td>
</tr>
<tr>
<td>RSU</td>
<td>Roadside unit</td>
</tr>
<tr>
<td>RSZW</td>
<td>Reduce speed/work zone warning</td>
</tr>
<tr>
<td>RTA</td>
<td>Right turn assist</td>
</tr>
</tbody>
</table>
### Acronyms and Initialisms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTU</td>
<td>Remote terminal unit</td>
</tr>
<tr>
<td>SA</td>
<td>Substation automation</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory control and data acquisition</td>
</tr>
<tr>
<td>SCMS</td>
<td>Security credential management system</td>
</tr>
<tr>
<td>SD-Access</td>
<td>Software-defined Access</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Software defined wide area network</td>
</tr>
<tr>
<td>SFC</td>
<td>Secure network analytics flow collector</td>
</tr>
<tr>
<td>SFC</td>
<td>Secure Network Analytics Flow Collector</td>
</tr>
<tr>
<td>SGACL</td>
<td>Security group-based access control list</td>
</tr>
<tr>
<td>SGT</td>
<td>Security group tag</td>
</tr>
<tr>
<td>SLC</td>
<td>Street light controller</td>
</tr>
<tr>
<td>SOV</td>
<td>Service operations vessel</td>
</tr>
<tr>
<td>SPAT</td>
<td>Signal phase and timing message</td>
</tr>
<tr>
<td>SRM</td>
<td>Signal request message</td>
</tr>
<tr>
<td>SSID</td>
<td>Service set identifier</td>
</tr>
<tr>
<td>SSM</td>
<td>Software security module</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning tree protocol</td>
</tr>
<tr>
<td>SVI</td>
<td>Switched virtual interface</td>
</tr>
<tr>
<td>SVL</td>
<td>StackWise virtual link</td>
</tr>
<tr>
<td>SXP</td>
<td>SGT exchange protocol</td>
</tr>
<tr>
<td>TAN</td>
<td>Turbine area network</td>
</tr>
<tr>
<td>TBN</td>
<td>Turbine base network</td>
</tr>
<tr>
<td>TC</td>
<td>Transit control</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission control protocol</td>
</tr>
<tr>
<td>TFTTP</td>
<td>Trivial file transfer protocol</td>
</tr>
<tr>
<td>TIM</td>
<td>Traveler information message</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport layer security</td>
</tr>
<tr>
<td>TLV</td>
<td>Type length value</td>
</tr>
<tr>
<td>TMC</td>
<td>Traffic monitoring center</td>
</tr>
<tr>
<td>TPE</td>
<td>ThingPark Enterprise</td>
</tr>
<tr>
<td>UCS</td>
<td>Cisco Unified Computing System</td>
</tr>
<tr>
<td>UDP</td>
<td>User datagram protocol</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra high frequency</td>
</tr>
</tbody>
</table>
## Acronyms and Initialisms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPS</td>
<td>Uninterrupted power supply</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to infrastructure</td>
</tr>
<tr>
<td>V2P</td>
<td>Vehicle to pedestrian</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to vehicle</td>
</tr>
<tr>
<td>V2X</td>
<td>Vehicle to infrastructure</td>
</tr>
<tr>
<td>VHF</td>
<td>Very high frequency</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual local area network</td>
</tr>
<tr>
<td>VN</td>
<td>Virtual network</td>
</tr>
<tr>
<td>VNI</td>
<td>VXLAN network identifier</td>
</tr>
<tr>
<td>VoD</td>
<td>Video on demand</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over internet protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual private network</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual routing and forwarding</td>
</tr>
<tr>
<td>VSM</td>
<td>Video Surveillance Manager</td>
</tr>
<tr>
<td>VXLAN</td>
<td>Virtual extensible LAN</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide area network</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless access in vehicular networking</td>
</tr>
<tr>
<td>WF</td>
<td>Wind farm</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless fidelity</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless local area network</td>
</tr>
<tr>
<td>WLC</td>
<td>Wireless LAN controller</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless personal area network</td>
</tr>
<tr>
<td>WRED</td>
<td>Weighted random early detect</td>
</tr>
<tr>
<td>WSMP</td>
<td>WAVE short message protocol</td>
</tr>
<tr>
<td>WTG</td>
<td>Wind turbine generator</td>
</tr>
<tr>
<td>ZTD</td>
<td>Zero touch deployment</td>
</tr>
<tr>
<td>ZTP</td>
<td>Zero touch provisioning</td>
</tr>
</tbody>
</table>