\€

Cisco Solution for Renewable Energy: Offshore Wind Farm 1.0

Design Guide

May 2023

Cisco Validated Design

Cisco Systems, Inc. www.cisco.com

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.

Contents

Introduction to Cisco Solution for Renewable Energy: Offshore Wind Farm

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 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 that are 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, in onshore and offshore wind farms, onshore solar farms, and onshore battery storage facilities. This document focusses on the complexities that offshore wind farms are facing and the solutions that Cisco offers.

Deploying and operating renewable energy 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.

Chapter 1: Solution Overview

As digital technology is increasingly required to operate remote distributed energy resource locations, networking and communication equipment must be installed with close attention paid to ease of operations, management, and security. Cisco validated designs are simple, scalable, and flexible. They focus on operational processes that are field-friendly and don't require a technical wizard. Our centralized network device management (Cisco DNAC) and strong networking asset operation capabilities eliminate the need for manual asset tracking and the inconsistencies in field deployments from one site to another. Integration with operations ensures that field technicians can easily deploy and manage devices without the need for IT support, while IT and OT teams have full visibility and control of the deployed equipment.

Additionally, Cisco provides a wide range of connectivity options, ranging from fiber to cellular or high-speed wireless where hardwired connections are not available.

Cisco has launched a complete validated design for offshore wind farms. This design focusses on an end-to-end architecture for the asset operator's network, including both onshore and offshore locations.

This document refers to the following stakeholders:

- Wind farm operator: The asset operator responsible for the daily operations and administration of a wind farm as a power-producing entity. Many operators are also involved in the development, ownership, and construction of the wind farm. Operators sell power that is produced to public utility companies, typically with long-term fixed price contracts in place.
- Wind farm owner (asset owner): Typically, a consortium of parties such as public utilities or oil and gas companies and financing companies. There are also dedicated renewable energy companies and others who invest in this area. Many wind farm owners also are operators. Many such companies are dedicated renewable companies or renewable energy branches of traditional utilities or oil and gas companies.
- Turbine supplier: Wind turbine suppliers design, test, and manufacture wind turbine equipment, including wind turbine generators (WTGs), and ancillary systems such as supervisory control and data acquisition (SCADA) and power automation. These suppliers also provide ongoing support and maintenance services (O&M) for many wind farm operators. It is typical for the monitoring and maintenance of the wind turbine network to be outsourced to these same suppliers.
- Offshore transmission owner (OFTO): Offshore wind farms are connected to the onshore grid by an export cable system. Regulatory requirements in many countries prohibit power generators from owning transmission assets. Therefore, the export cable often is owned and operated by another third-party, the OFTO. Developers, who often also are the wind farm owners or operators, divest the export cable system to a third-party through a regulated auction. In some regions, the requirement to divest the transmission assets (export cable systems) is not required.
- Grid utility: A traditional power grid operator that provides the connection point for exported power from a wind farm can be either a transmission system operator (TSO), a distribution network operator (DNO), or a distribution system operator (DSO). Public utilities that are also wind farm owners separate the grid and renewable businesses usually due to strict regulatory requirements.

This chapter includes the following topics:

- Cisco Solution for Renewable Energy Offshore Wind Farms
- Offshore Wind Farm Cisco Validated Design
- Scope of Wind Farm Release 1.0 CVD

Cisco Solution for Renewable Energy Offshore Wind Farms

Offshore wind farms are large infrastructure deployments with multiple locations. They include the following:

- Onshore substation
- Offshore substation (platform offshore)
- Offshore wind turbines (ranging from 50 to 300 turbines)
- Onshore operations and maintenance offices
- Offshore service operations vessels (SOV), which provide worker accommodations, offices, and workshops while offshore

Reliable and secure connectivity is key for providing monitoring and control of these offshore and therefore remote assets. Without a reliable and secure communications infrastructure, monitoring and control would be challenging.

From the offshore wind farm operator's viewpoint, the network needs to be easy to deploy, monitor, upgrade, and troubleshoot. The network design also needs to be standardized to enable easy specification and procurement at the early stages of a project. Avoiding both bespoke work and delivering different architectures for each project should enable a speedier project delivery phase.

A standardized solution is required that provides the flexibility to meet these needs while facilitating a clear path forward as complexity and scale evolve (for example, larger wind farms, increased number of devices and applications, and increased reliability).

Offshore Wind Farm Cisco Validated Design

Cisco has developed a complete Cisco Validated Design (CVD) for offshore wind farm projects. It provides a blueprint solution for all phases of a project, from specification and procurement to deployment.

The CVD includes networking infrastructure from offshore wind turbine through offshore platforms to the onshore WAN interface point and connectivity to the wind farm operator's control center.

The CVD is modular to allow for varying wind farm sizes, so it can be adapted for any number of turbines. It provides resilient architectures to allow for fault conditions, and includes cyber security built in from the start.

This CVD offers the following key benefits:

- Flexible deployment options: Support for simple to advanced solutions that cover various deployment options (scalable for small to large wind farms). A modular design that can adjust to the various sizes of wind farms that are deployed. Providing a flexible platform for the deployment of future services and applications.
- Rugged and reliable network equipment: Network equipment designed for harsh offshore environments where required. The ability for network equipment to operate in space-constrained locations and tough environmental conditions.
- Simplified provisioning: Automation and simple onboarding, monitoring, and management of remote networking assets with centralized monitoring and management of multiple wind farm networks.
- Simplified operations: Increased operational visibility, minimized outages, and faster remote issue resolution. Compliance of network device configurations (changes from a known baseline are flagged) and firmware and powerful analytics to provide deep visibility of the network assets.
- Multi-level security: End-to-end robust security capabilities to protect the infrastructure and associated services, monitor traffic flows, and provide control points for interfacing to third-party networks and equipment. Vulnerability information for discovered assets and asset reporting to aid regulatory compliance (for example, NIS 2 and NERC CIP).

The validated design is built on the following functional blocks:

- Wind farm operator data center
- Wind farm wide area network (WAN)
- Onshore DMZ
- Onshore substation
- Offshore DMZ
- Offshore substation
- Turbine SCADA network
- Power control and metering (PCM) network
- Turbine plant IT network (for example, enterprise and plant services)
- Service SOVs
- Operations and maintenance buildings (O&M)

The validated design allows customers or partners to select the parts are applicable to a particular project or deployment or use the complete end-to-end architectures.

Scope of Wind Farm Release 1.0 CVD

This Design Guide provides network architecture and design guidance for the planning and subsequent implementation of a Cisco Renewable Energy Wind Farm solution. In addition to this Design Guide, *Cisco Wind Farm Solution Implementation Guide* provides more specific implementation and configuration guidance with sample configurations.

The scope of this *Wind Farm Release 1.0 CVD* includes:

- End-to-end network infrastructure for offshore and onshore wind farms that leverage Cisco ruggedized Industrial Ethernet (IE) switches for the wind farm turbine networks.
- Cisco IE and Cisco Catalyst switching, firewalls, and routing for offshore and onshore substation networks (integration of customer and third-party networks).
- Several resilient and non-resilient topologies for the turbine network and resilient rings for connecting turbines to an offshore substation aggregation network.

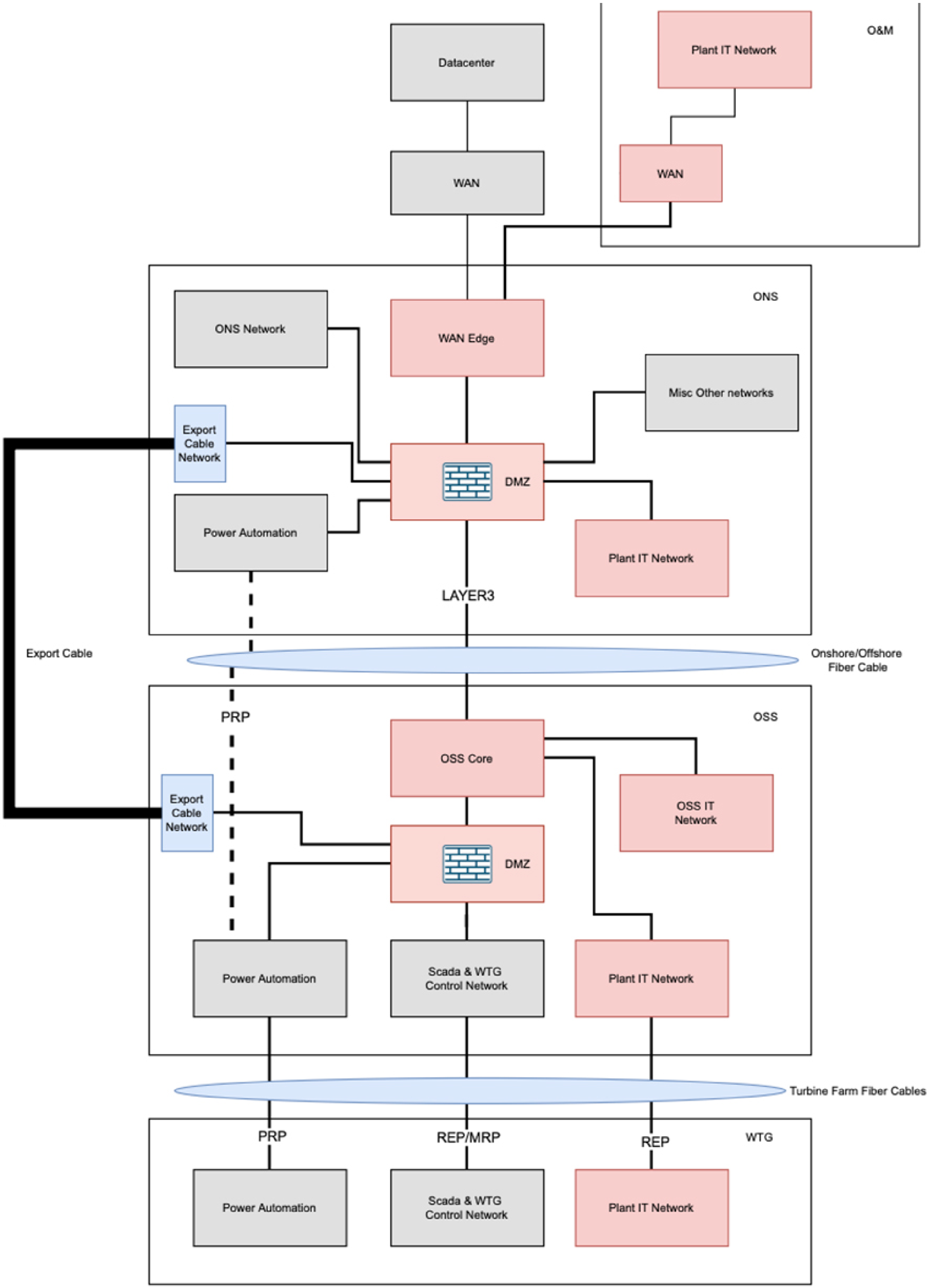
- Corporate IT wired and wireless access to remote sites to enable worker mobility and access to key IT resources. Also enables worker efficiency and the ability to access services such as the corporate intranet, file sharing, and voice and video services.
- Integration of Cisco DNA Center and Identity Services Engine (ISE) to manage wind farm IT network infrastructure, including:
  - Automation of network infrastructure day 0 provisioning, software updates and configuration, and day N lifecycle management
  - Monitoring and management of network health and status with DNA Center assurance
  - Simplified and consistent deployment of network security policies
- Capability to securely interface with third-party networks such as the turbine SCADA network, export cable system, and substation protection and control network.
- A flexible network that allows services to be added as needed while maintaining segregation of traffic.
- WAN handoff interface and new technologies, such as Cisco SD-WAN for automating deployment of overlay networks across multiple underlying WAN technologies.
- Innovation areas, such as solutions for SOVs, which provide high bandwidth connectivity for corporate workers and contractors when operating offshore.

The following architectural blocks are out of the scope of this CVD:

- Backhaul design for WAN handoff routers
- Typical service provider or customer MPLS network or other fixed connectivity options (microwave, fiber, and so on).
- Data center network design
- Turbine OEM SCADA and control network
  - Turbine vendors dictate an off-the-shelf factory design for contract efficiency. Cisco provides support and products to these manufacturers separately and the value to revalidate what they provide is seen as minimal.
  - This network is not managed by turbine operator, not by the wind farm operator.
  - Turbine supplier is awarded a multiyear contract to operate and maintain the turbines.
  - For the purposes of this CVD, treated as a “third-party network block” that connects to the offshore substation DMZ.

Figure 1-1 illustrates the scope of this CVD. Items shown in pink are within the scope of this CVD for wind farm asset operators. Items shown in grey are third-party provided networks that are out of the scope of this CVD.

Figure 1-1 Wind Farm Release 1.0 CVD Scope



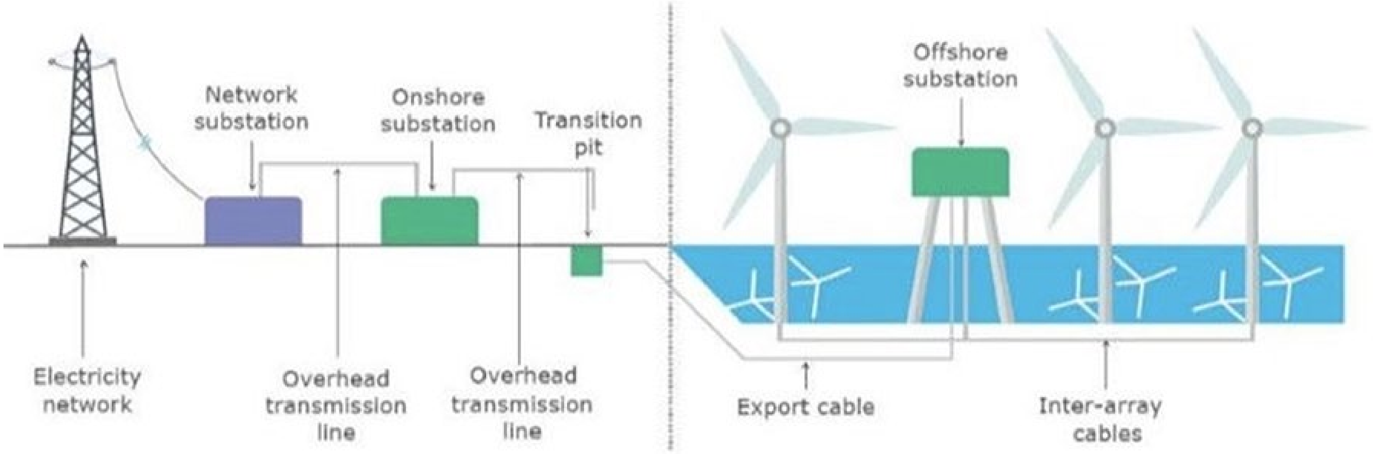
Chapter 2: Wind Farm Use Cases

This chapter includes the following topics:

Offshore Wind Farm Places in the Network

Figure 2-1 shows the places that an offshore wind farm has in a network.

Figure 2-1 Wind Farm Places in a Network



- Wind turbine generator (WTG)
- Offshore substation (OSS)
- Onshore substation (ONSS)
- Service operations vessel (SOV)
- Crew transfer vessel (CTV)

Wind Farm solution architecture network building blocks are defined based on the places in the offshore wind farms.

Use Cases

The communications options that are available at a given site greatly influence the outcomes and capabilities for any use case. The availability of dependable lower latency, high bandwidth connectivity (such as fiber, LTE/5G cellular, and Wi-Fi) allows for more advanced network and data service options, while sites with bandwidth constrains may be limited to simpler use cases such as remote management and monitoring. Table 2-1 lists the key use cases in an offshore wind farm.

Table 2-1 Wind Farm Use Cases

Use Case	Type of Services	Description
WTG SCADA (Not part of this CVD. Design normally defined and provided by the Turbine supplier)	▪ Turbine telemetry ▪ Fire detection ▪ Turbine ancillary systems ▪ Weather systems	▪ Telemetry data collection associated with turbine systems and components. ▪ Detection of smoke and fire within the turbine. ▪ Telemetry data collection associated with ancillary systems (for example, elevator, navigation lights). ▪ Data from weather-related systems such as radar for offshore farms, wind speed anemometers.
Process and control systems (ONSS, OSS, other miscellaneous systems)	▪ Heating and ventilation systems ▪ Public announcement and general alarm (PAGA) systems ▪ Backup generators ▪ Fire detection systems	▪ Heating, ventilation, and air conditioning (HVAC) systems. ▪ Audio systems for announcements and alarms. ▪ Generators for emergency power. ▪ Fire detection systems.
Marine-related Systems	▪ Tetra, VHF, UHF Radio ▪ Automatic identification system (AIS) ▪ Radar systems	▪ Ship and worker radio systems. ▪ Shipping identification system. ▪ Radar for SOV management.
Enterprise services	▪ IP telephony ▪ Corporate network access ▪ Guest network access	▪ Enterprise voice communications for workers. ▪ Fixed and mobile handsets (Wi-Fi). ▪ General network access for enterprise services such as email, file sharing, video, and web. ▪ Basic internet access for subcontractors.
Physical security	▪ Closed circuit television (CCTV) ▪ Access control	▪ Physical security monitoring of turbine assets and areas around turbines for safety and security. ▪ Intrusion detection and entry into areas such as O&M offices and turbine towers.
Miscellaneous systems	▪ Bat and bird monitors ▪ Radar ▪ Lightning detection systems ▪ Lidar (turbine monitoring)	▪ Detection of protected wildlife. ▪ Additional radar equipment as specified by certain bodies (military, Coast Guard, and so on). ▪ Detection of lightning strikes. ▪ Monitoring of turbine performance and blade dynamics.
SOV connectivity	▪ IP telephony ▪ Wireless network access (Wi-Fi)	▪ Enterprise voice communications for workers. ▪ Fixed and mobile handsets. ▪ Wi-Fi access points within SOVs to provide enterprise network access for staff and to provide IP telephony coverage.

Environmental sensors	▪ Heat and humidity ▪ Door open and close ▪ Machine temperature	▪ Turbine nacelle or tower and external measurements. ▪ Turbine tower, external ancillary cabinets. ▪ Machine casing or transformer case temperature.
Location-based services	▪ Personnel location and man down (for lone worker)	▪ Wi-Fi access points providing Bluetooth capability for short-range personnel devices for location and man down worker safety.

Wind Farm Actors in the Network

Various wind farm use cases and places need different endpoints or actors in the network. The following actors are needed in a wind farm network to deliver the features for the use cases that the previous section describes. These actors usually are key to operating a renewable energy site, providing both monitoring and control capabilities.

- CCTV cameras: Physical safety and security IP cameras
- IP phones: Voice over IP (VoIP) telephony devices
- Programmable logic controller (PLC) devices and input and output (I/O) controllers: Power systems protection and control
- Intelligent electronic devices (IED): Power systems protection and control
- Wi-Fi access points: Provide corporate IT Wi-Fi access
- Cisco Ultra Reliable Wireless Backhaul (CURWB) access points: Provide wireless backhaul for SOV connectivity
- Wind turbine monitoring and control: SCADA and monitoring systems
- Fire detection and alarming devices or sensors
- HVAC systems
- Environmental and weather systems: Sensors that are associated with monitoring weather and environmental conditions
- Lightning detection: Sensors that are associated with lightning detection
- Marine systems (radar, radio)

Traffic Types and Flows

Each actor in an offshore wind farm requires network communication with other actors or application servers in the offshore substation (OSS) and control or operations center based on use case requirements. Table 2-2 lists the traffic types and flow in the offshore wind farms places in the network.

Table 2-2 Offshore Wind Farm Traffic Types and Flows

Traffic Type	Traffic Flows in the Network
Video traffic (CCTV cameras)	▪ Turbine nacelle to control center or OSS: CCTV camera in turbine nacelle switch streaming live video to video server in the control center or OSS infrastructure ▪ Turbine base switch to control center: CCTV camera in base switch streaming live video to a video server in the Control Center or OSS Infrastructure

SCADA data for monitoring and control (PLCs and I/O devices that are external to the turbine supplier's dedicated SCADA network))	▪ Traffic within turbine nacelle: PLC and I/O devices communication using SCADA protocols (for examples, DNP3, MODBUS, or T104) ▪ Turbine base switch to nacelle: PLC in turbine base switch to an I/O device in nacelle using SCADA protocols (for example: DNP3, MODBUS, or T104) ▪ Traffic within turbine base switch: Communication between PLC and I/O devices in a turbine base switch ▪ Turbine base switch to base: Communication between PLC in a turbine base switch and I/O device in another turbine base switch
IP telephony voice traffic (IP phones)	▪ Maintenance and operations personnel voice communication between turbine base switch or nacelle and OSS ▪ Maintenance and operations personnel voice communication between turbine base switch networks ▪ Maintenance and operations personnel voice communication between an SOV and turbine base switch or OSS networks
Wi-Fi traffic (Wi-Fi APs)	▪ Turbine nacelle to OSS infrastructure or control center): Workforce AP in nacelle to WLC in the OSS network ▪ Turbine base switch to OSS infrastructure or control center ▪ Workforce AP in a turbine base switch to WLC in the OSS network ▪ Workforce corporate network access from offshore wind farm ▪ Guest internet wireless access from offshore and onshore substation
Offshore and onshore power automation and control SCADA traffic (IEDs, switchgear, other substation OT devices if any)	▪ Turbine nacelle switch to OSS infrastructure ▪ Turbine base switch to OSS infrastructure ▪ Management traffic between IEDs and SCADA systems in the OSS and IEDs and SCADA devices connected turbine nacelle or turbine switches
Cisco Ultra Reliable Wireless Backhaul (CURWB) traffic	▪ SOV wireless connectivity using a CURWB network from turbine nacelle or turbine switch or OSS network
Turbine control network traffic (dedicated turbine SCADA network provided by a turbine manufacturer)	▪ SCADA OPC-UA protocol traffic between OSS DMZ and OSS infrastructure network
SD-WAN and network management traffic (OMP, SSH, SNMP and network control protocols, and so on)	▪ Management traffic from ONSS and OSS via the WAN to the control center ▪ Management traffic related to Cisco SD-WAN and DNA Center network management platform
Auxiliary systems traffic (HVAC, fire, lighting detection, environmental sensors)	▪ Turbine nacelle and switch to OSS infrastructure or control center

Chapter 3: Solution Architecture

This chapter includes the following topics:

- Overall Network Architecture
- Solution Components
- Solution Hardware and Software Compatibility

Overall Network Architecture

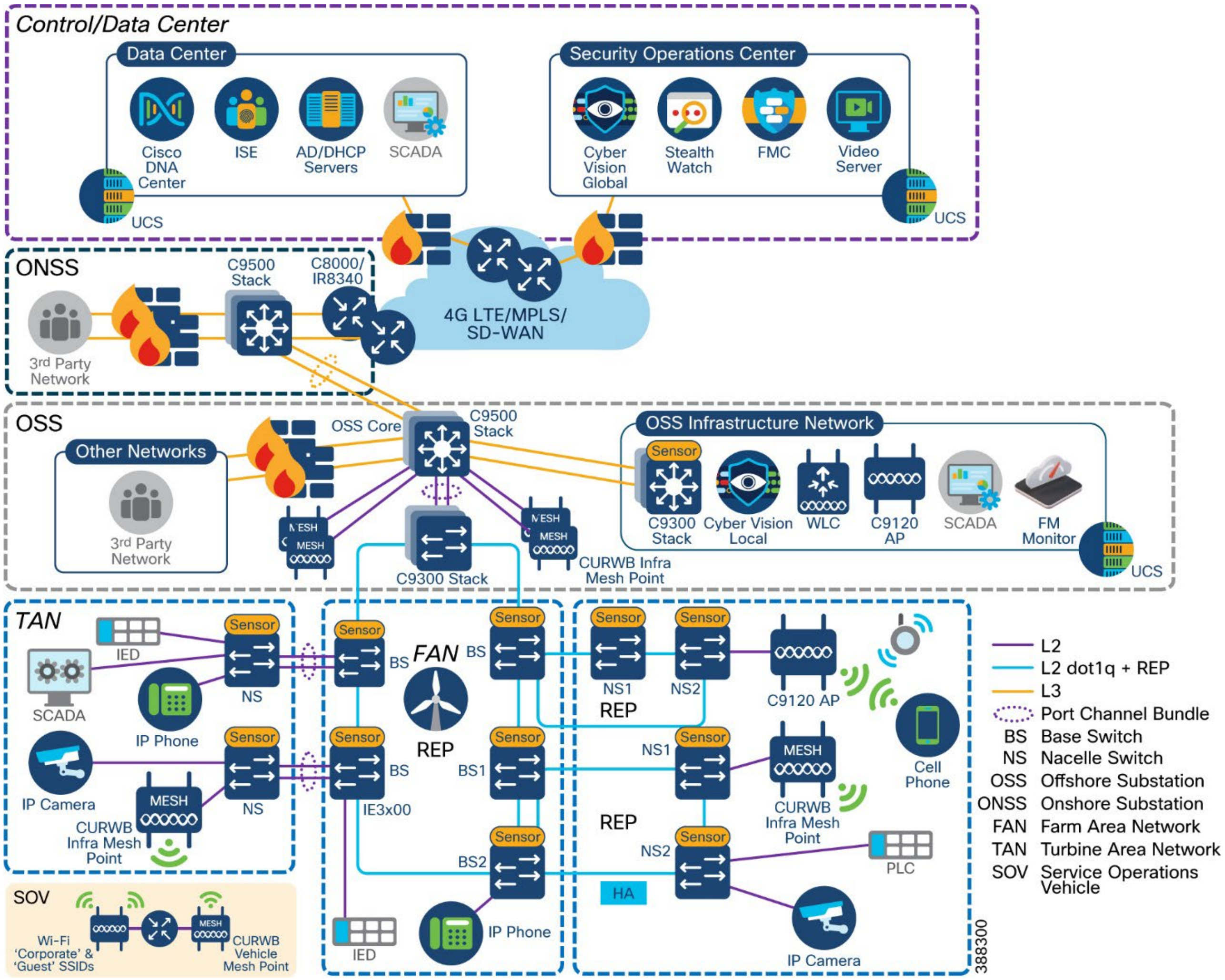
Offshore wind farm solution architecture is built on the following functional blocks:

- Wind farm operator control center (includes data center and security operations center): Hosts wind farm IT and OT data center applications and servers such as Cisco DNA Center, Cisco ISE, AD server, DHCP server, Cisco Cyber Vision Center (CVC), and more.
- Wind farm wide area network (WAN): A backhaul network for interconnecting a wind farm onshore substation with a control center. It can be a privately owned MPLS network, a service provider LTE network, or a Cisco SD-WAN managed network.
- Onshore substation (ONSS): A remote site in a wind farm that interconnects an offshore substation with a control center via a WAN.
- Offshore Substation (OSS): Consists of offshore core network and infrastructure applications to provide network connectivity and application access to wind turbine bases and nacelle switches and their IT and OT endpoints.
- Third-party networks or turbine control network: Turbine vendor’s SCADA control network that runs separately from wind a farm asset operator’s network. This CVD does not cover this third-party SCADA control network architecture. However, this architecture interacts with a wind farm asset operator’s network architecture, which this CVD does focus on.
- Farm area network (FAN): An aggregation network that connects multiple wind turbines base switches and to their aggregation switches.
- Turbine area network (TAN): A switched layer 2 network typically formed by one or more nacelle switches in a wind turbine.
- SOV: Wind farm network operation and maintenance vehicle that moves around offshore wind farms and connects to TAN and OSS or ONSS networks for service operation personnel network communication.

Each of these building blocks and design considerations are discussed in detail in Chapter 4: Solution Design Considerations.

Figure 3-1 shows the end-to-end solution network architecture of a wind farm.

Figure 3-1 Wind Farm Solution Network Architecture



Solution Components

This section describes the components of a wind farm network. Several device models can be used at each layer of the network. The device models that are suitable for each role in the network and the corresponding CVD software versions are described in Solution Hardware and Software Compatibility.

You can choose a device model to suit specific deployment requirements such as network size, cabling and power options, and access requirements. Table 3-1 describes device models that are used for components in the architecture for a wind farm solution.

Table 3-1 Components and Device Models in Wind Farm Architecture

Component Role	Component	Description
Turbine nacelle switch, no HA	Cisco Catalyst Industrial Ethernet (IE) 3400 Series Switch	1G fiber ring with port channel connectivity to base switch.
Turbine nacelle switch, with HA	Cisco Catalyst Industrial Ethernet (IE) 3400 Series Switch	1G fiber ring for nacelle switch redundancy.
Turbine base switch	Cisco Catalyst Industrial Ethernet (IE) 3400 Series Switch	1G fiber ring for base switches in FAN. Up to 20 switches can be in the ring. 8, 9, or 10 switches in the ring are common in a deployment.
Farm area aggregation	Cisco Catalyst 9300 Series switch Stack	REP ring aggregation switch. Stack for HA.

OSS and ONSS core switch, with HA	Cisco Catalyst 9500 Series switches with Stackwise Virtual (SVL)	Offshore IT network core. Deployed with SVL for HA.
OSS IT network access switch	Cisco Catalyst 9300 Series switch stack	Consists of two switches for HA to provide access connectivity to OSS network infrastructure devices.
OSS firewall	Firepower 2100 or 4100 Series	OSS network firewall.
ONSS WAN router	Cisco Catalyst IR8300 Rugged Series Router or Cisco Catalyst 8000 Series Edge Platform	Onshore substation WAN router.
OT network sensor	Cisco Cyber Vision network sensor on IE3400 Series Switches	CV network sensors on all IE switches in the ring and FAN.
OT security dashboard	Cisco Cyber Vision Center global and local virtual appliances	CVC deployed globally and locally in control center and OSS network infrastructures, respectively.
Wireless LAN controller	Cisco Catalyst 9800 Wireless Controller (WLC)	Catalyst Wi-Fi network controller in OSS network infrastructure.
SCADA application server	SCADA application server	SCADA application server in OSS network infrastructure.
CURWB gateway	CURWB FM1000 Gateway	CURWB wireless network mesh end.
Network management	Cisco DNA Center	Wind farm network management application in control center and DC.
Authentication, authorization, and accounting (AAA)	Cisco ISE	AAA and network policy administration.
IT and OT security management	Cisco Secure Network Analytics (Stealthwatch) Manager and Flow Collector Virtual Edition	Network flow analytics and security dashboard in control center.
Physical safety video server	Cisco or third-party video server for IP cameras	Cisco or third-party video server for IP cameras in control center
4G-LTE or 5G connectivity for SOV	Cisco Industrial Router 1101 with 4G-LTE or 5G SIM	4G-LTE or 5G connectivity for SOV when in range of cellular connectivity close to shore.
OSS, FAN, or TAN wireless backhaul	CURWB FM3500	CURWB infrastructure AP on OSS, FAN, or TAN for SOV wireless backhaul connectivity.
OSS vessel wireless backhaul	CURWB FM4500	OSS vessel mesh point for connectivity into OSS or TAN.
Wi-Fi network access point	C9120 AP	Catalyst Wi-Fi network AP in TAN and OSS.
Hardened Wi-Fi access point	Cisco IW6300	Catalyst Wi-Fi network AP in TAN and OSS.

Solution Hardware and Software Compatibility

Table 3-2 lists the Cisco products and software versions that are validated in this CVD. Table 3-3 lists the third-party products that are used in the validation.

Table 3-2 Cisco Hardware and Software Versions Validated in this CVD

Component Role	Hardware Model	Version
Turbine nacelle switch, no HA	IE3400-8P2S IE3400-8T2S	17.11.1
Turbine nacelle switch, with HA	IE3400-8P2S IE3400-8T2S	17.11.1
Turbine base switch	IE3400-8P2S, IE3400-8T2S	17.11.1
Farm area aggregation	C9300-24UX	17.11.1
OSS core switch, with HA	C9500-16X	17.11.1
OSS IT network access switch	C9300-24UX	17.11.1
ONSS core switch	C9300-24UX	17.11.1
OSS and ONSS DMZ firewall	Firepower 2140	7.0.1
Firewall management application	Firepower Management Center (FMC) Virtual Appliance	7.0.1
ONSS WAN edge router	Cisco Catalyst IR8340 Rugged Series Router	17.11.1
Network management application	Cisco DNA Center Appliance DN2-HW-APL	2.3.6.0
Unified Computing System (UCS)	UCS-C240-M5S	3.1.3c
Authentication, authorization, and accounting (AAA) server	Cisco ISE Virtual Appliance	3.2
CV network sensors	IoX Sensor App	4.1.2
OT security dashboard	Cisco Cyber Vision Center global and local virtual appliance	4.1.2
Wireless LAN controller	C9800-L-C-K9	17.11.1
Cisco IW6300 ruggedized AP for Wi-Fi access	IW6300-AP	17.11.1
Cisco AP for Wi-Fi access	AIR-AP9120	17.11.1
CURWB mesh point	CURWB FM3500 and FM4500	9.4
CURWB mesh gateway	CURWB FM1000 Gateway	1.6.0
CURWB FM-Monitor	CURWB FM-Monitor VM	1.0.1
IT and OT security management	Cisco Secure Network Analytics (Stealthwatch) Manager and Flow Collector Virtual Edition	7.4.1
Control center headend router	ASR-1002-HX	17.3.4a

WAN management	Cisco SD-WAN vManage, vSmart, vBond virtual appliances	20.8.1

Table 3-3 Third-party Hardware and Software Versions Validated in this CVD

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

Note: Enable appropriate licenses for each of the wind farm network components. See the component's data sheets for information about enabling the features and functions that you need.

Chapter 4: Solution Design Considerations

This chapter includes the following topics:

Turbine Area Network Design

In offshore wind farms, each wind turbine has a Cisco IE3400 switch deployed at the turbine nacelle to provide offshore substation (OSS) network connectivity to various endpoints in the turbine. These endpoints include SCADA devices, PLC, I/O devices, CCTV cameras, and so on. The IE switch deployed in the turbine nacelle is also called a nacelle switch (NS). The NS with its OT and IT endpoints forms a turbine area network TAN in the wind farm solution architecture, as shown in Figure 4-1.

Figure 4-1 TAN Design

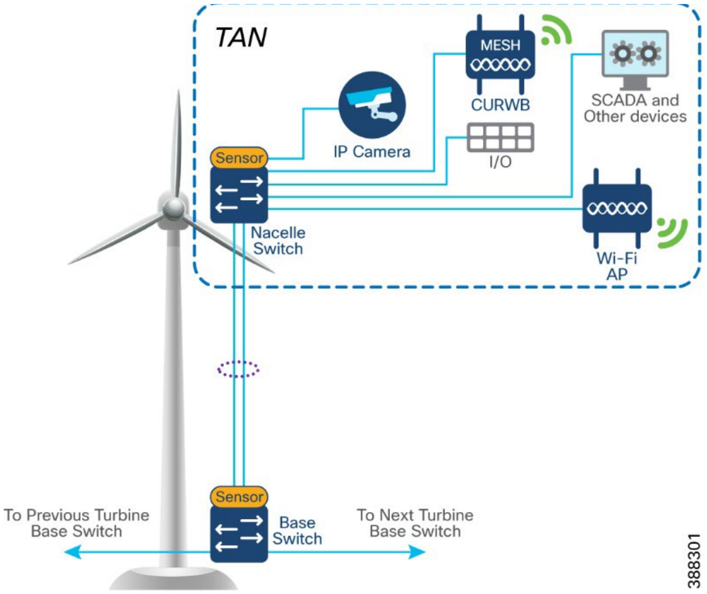


Table 4-1 lists the actors and traffic types in a TAN.

Table 4-1 TAN Actors and Traffic Types

Actors	Traffic Type
CCTV camera	TAN to control center. CCTV camera in nacelle switch streaming live video to video server in OSS infrastructure or control center.
PLC and IO	Traffic within the TAN. OT Traffic between PLC and I/O in nacelle. TAN to base. PLC in base of turbine to I/O in nacelle.
Wi-Fi access point	TAN to OSS infrastructure and CC. Workforce AP in Nacelle to WLC in OSS network. Provides corporate network access and guest internet access.
SCADA	TAN to OSS infrastructure. management traffic between SCADA endpoints in OSS.
CURWB	Offshore vessel wireless connectivity using CURWB network from the TAN.

TAN Non-HA Design Considerations

- Single Cisco IE3400 switch deployed in each turbine nacelle, as shown in Figure 4-1 for the TAN non-HA design option turbine nacelle Ethernet switch.
- Layer 2 Star Topology (non-HA) of nacelle switches connecting to turbine base switch (shown in Figure 4-1).
- An LACP port-channel with two member links to a base switch provides link-level redundancy to TAN.
- Multiple VLANs for segmenting TAN devices are configured in the NS. Examples include CCTV camera VLAN, OT VLAN for SCADA endpoints, Wi-Fi AP management VLAN, management VLAN (FTP/SSH), CURWB VLAN for vessel connectivity, voice VLAN for VOIP phones, and marine systems VLAN.
- First hop security protocols with device authentication using MAB or Dot1x are configured for securing TAN endpoints.
- Layer 3 gateway for all VLANs in the NS is configured in OSS Core switch (C9500 switch)

TAN High Availability Design with REP

An IE3400 nacelle switch in the TAN provides a single point of failure for TAN endpoints. To provide a highly available TAN, two nacelle switches are deployed for TAN endpoints network connectivity. In addition, a redundancy protocol is configured.

Resilient Ethernet Protocol Ring

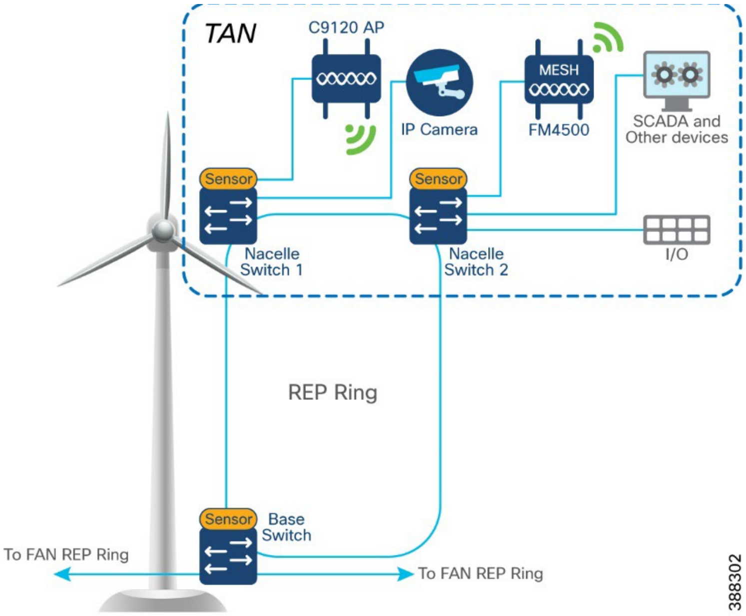
Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) for controlling network loops, handling link failures, and improving convergence time. REP controls a group of ports that are connected in a segment, ensures that the segment does not create bridging loops, and responds to link failures within the segment. REP provides a basis for constructing complex networks and supports VLAN load balancing. It is the preferred resiliency protocol for IoT applications.

A REP segment is a chain of ports that are connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. The preferred alternate port selected by REP is blocked during normal operation of the ring. If a REP segment fails, the preferred alternate port is automatically enabled by REP, which provides an alternate path for the failed segment. When the failed REP segment recovers, the recovered segment is made the preferred alternate port and blocked by REP. In this way, recovery happens with minimal convergence time.

Two uplink ports from two nacelle switches deployed for HA in TAN are connected to a turbine base switch.

There are two options for TAN high availability design. In the first option, shown in Figure 4-2, a closed ring topology of two nacelle switches connects to a single turbine base switch. This arrangement forms a subtended REP ring to the FAN main ring.

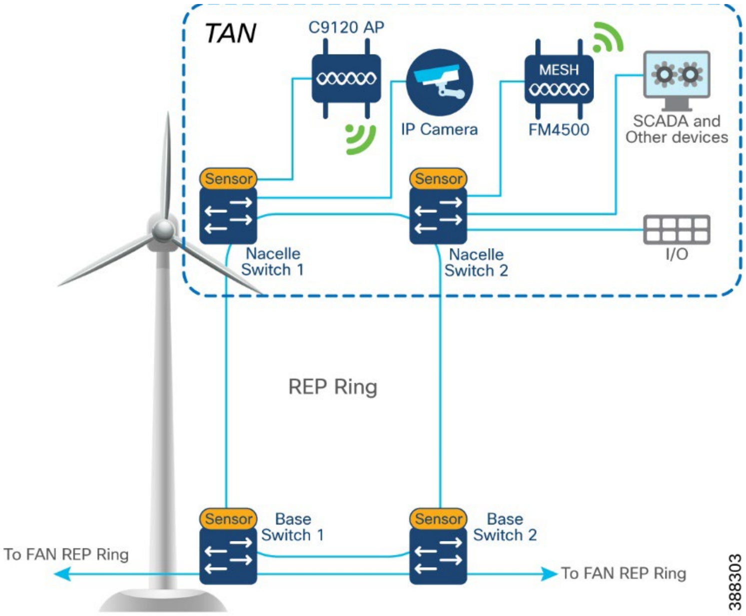
Figure 4-2 TAN HA Design, Option 1



In the second option, shown in Figure 4-3, the uplinks form two nacelle switches are connected to two different base switches in a TAN, which provides redundancy for the turbine base switch network and the TAN. In this option:

- An open ring topology of two nacelle switches connects to two turbine base switches.
- A subtended RIP ring of FAN main REP ring of base switches is formed.

Figure 4-3 TAN HA Design, Option 2



Turbine Base Network Design

In offshore wind farms, each wind turbine has an IE3400 switch that is deployed at the turbine base to provide OSS network connectivity to various endpoints in the turbine base. These endpoints include SCADA devices, PLC, I/O devices, CCTV cameras. the TAN, and so on. The IE switch that is deployed in the turbine base is also called the base switch (BS). The BS, with its OT and IT endpoints, forms a Turbine Base Network (TBN) in the wind farm solution architecture, as shown in Figure 4-4.

Figure 4-4 Turbine Base Network Design

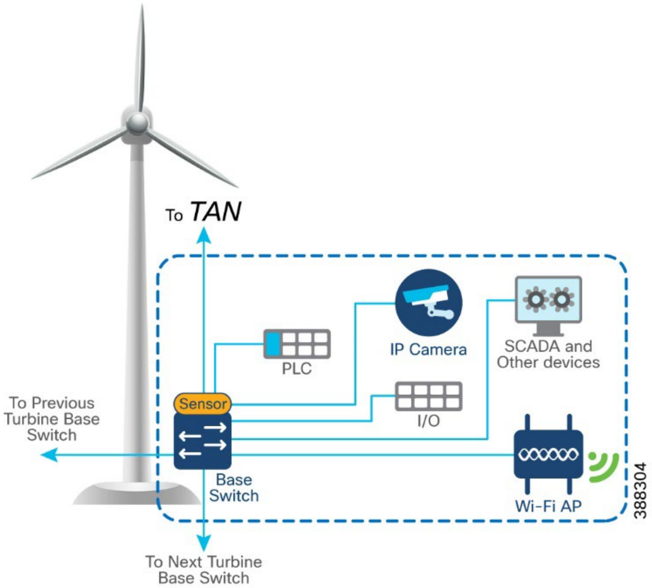


Table 4-2 lists the actors and traffic type in a turbine base switch network.

Table 4-2 Turbine Base Network Actors and Traffic Types

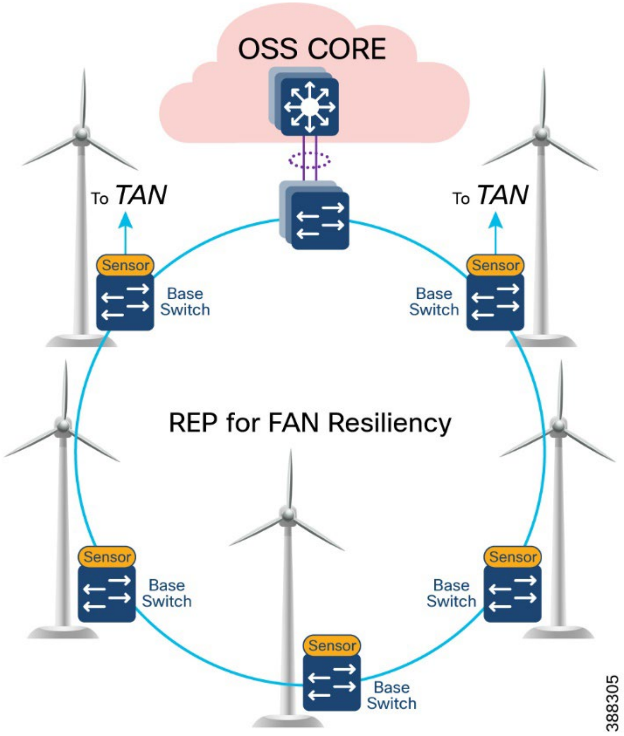
Actors	Traffic Type
CCTV camera	▪ Base to control center. CCTV camera in base switch streaming live video to video server in OSS infrastructure or control center.
PLC and I/O controller	▪ Traffic within base. OT traffic between PLC and I/O in base. ▪ Base to base. PLC in base of turbine to I/O in base.
Wi-Fi access point	• Base to OSS infrastructure or control center. Workforce AP in base switch communicating with the WLC in the OSS infrastructure. Provides connectivity to the OSS and DC network based on needs and provides guest internet access.
SCADA	• Base to OSS Infrastructure. Management traffic between SCADA endpoints in OSS.

Farm Area Network Design

In offshore wind farms, the base switch from each wind turbine is connected in a ring topology using a 1G fiber cable with Catalyst 9300 stack switches to form a farm area network (FAN) ring. A REP is configured in the FAN ring to provide FAN resiliency for faster network convergence if a REP segment fails.

Figure 4-5 shows a FAN ring aggregating to a pair of Cisco Catalyst 9300 switches in a stack configuration. A Catalyst 9300 stack aggregates all FAN rings in an offshore wind farm.

Figure 4-5 FAN Design



Design Considerations

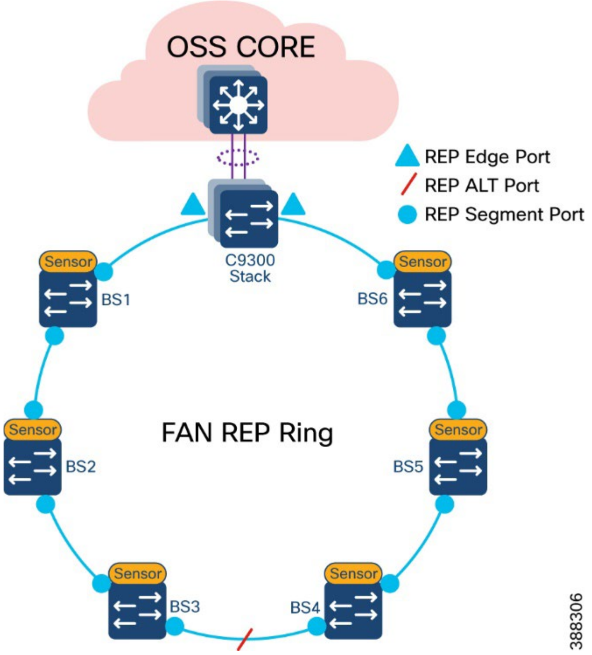
- Cisco Industrial Ethernet 3400 Switches as turbine base ethernet switches.
- A layer 2 closed ring of turbine base switches connected via 1G fiber forms a FAN.
- FAN base switches aggregates subtended REP ring for HA traffic from the TAN with HA.
- A FAN ring consists of a maximum of 18 base switches. A Catalyst 9300 stack aggregates up to 10 FAN rings, depending on the Catalyst9300 model and port density.
- REP protocol is used for base switches and FAN resiliency; REP edge ports are configured on a Catalyst 9300 stack in OSS aggregation.
- Multiple VLANs are configured for network segmentation of TAN and FAN devices. Examples include CCTV camera VLAN, OT VLAN for SCADA endpoints, management VLAN (FTP and SSH), CURWB VLAN for vessel connectivity, Wi-Fi AP management VLAN, voice VLAN for VoIP Phones, and marine systems VLAN.

FAN REP Ring Design

A closed REP ring of FAN forms a main REP segment to forward all VLAN traffic in an offshore wind farm network. Primary and secondary REP edge ports are configured on an OSS aggregation switch stack (Catalyst9300) and an alternate port is configured in the middle of the ring. See Figure 4-6.

A FAN REP ring can be provisioned by using the Cisco DNA Center REP workflow, which automates the REP configuration from daisy-chained IE switches. For more detailed information about FAN REP ring and subtended REP ring provisioning using Cisco DNA Center, see Chapter 5: Network Management and Automation.

Figure 4-6 FAN REP Design

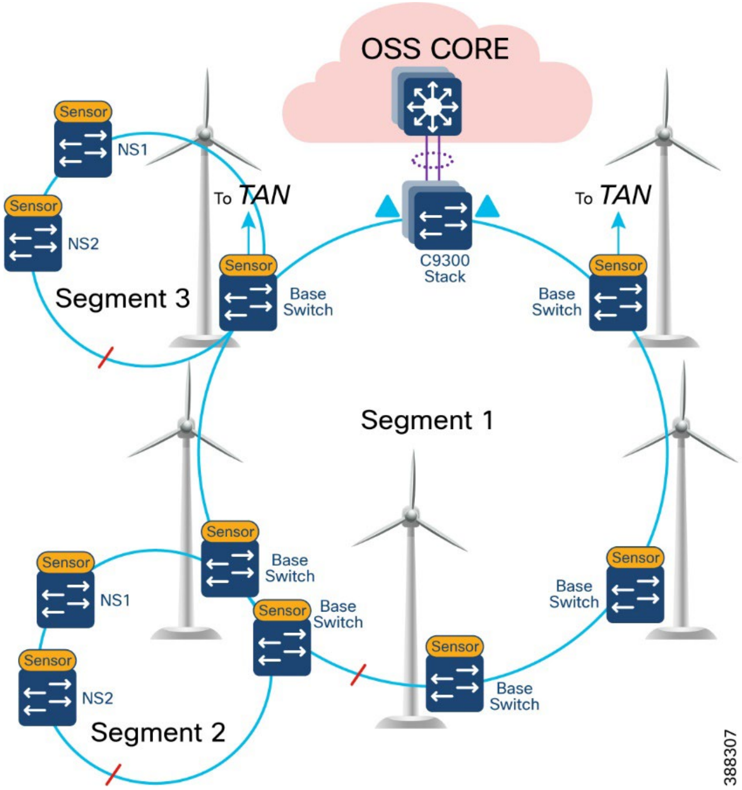


FAN Subtended REP Ring Design

A TAN REP ring aggregating to a turbine base switch or a pair of base switches, as discussed in TAN High Availability Design with REP, creates a subtended REP ring or ring of REP rings in an offshore wind farm network. A closed or open REP ring configured with REP Topology Change Notification (TCN) within a REP segment notifies REP neighbors of any topology changes. At the edge, REP can propagate the TCN to other REP segments.

Figure 4-7 shows the FAN main REP ring and subtended REP rings design in the wind farm solution architecture.

Figure 4-7 FAN main REP Ring and Subtended REP Rings Design



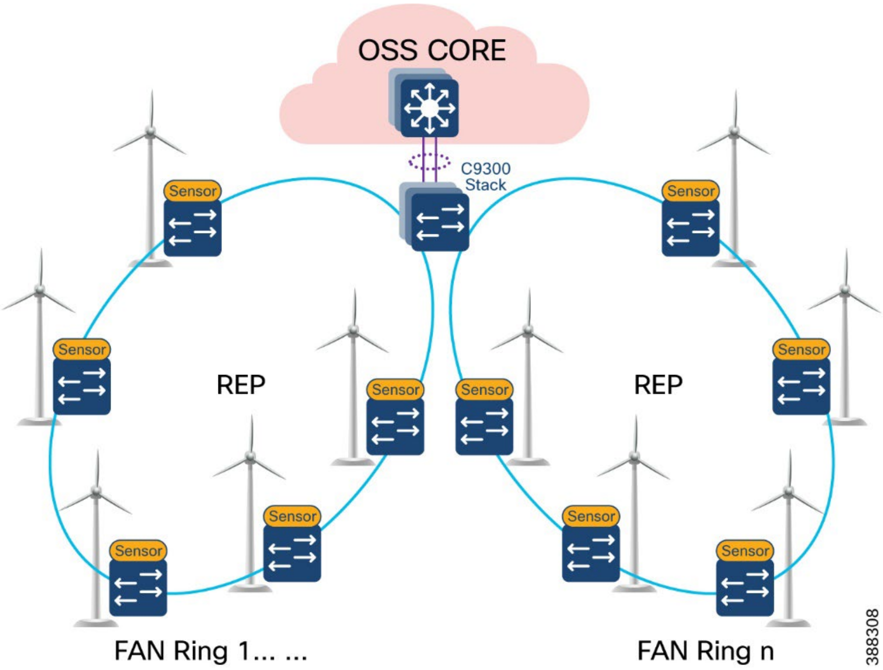
FAN Aggregation

An offshore wind farm can have more than 200 turbines, and each turbine can have more than 2 base switches that connect to the OSS network. We recommend that a deployment have a FAN ring size of more than 20 IE switches. Multiple such FAN rings should be aggregated to access offshore substation (OSS) and onshore substation (ONSS) IT networks.

The FAN aggregation infrastructure is composed of Cisco Catalyst 9300 Series switches, typically with two of these switches in a physical stack, that are capable of providing 10G uplinks to OSS and ONSS networks. A stack of two Catalyst 9300 switches physically located in an OSS network connects turbine base switches in a ring via fiber cables (turbine string cables) and aggregates layer 2 traffic from each ring to upper layers of the wind farm network infrastructure, for or example, to an OSS core switch.

Figure 4-8 shows the FAN aggregation design using a stack of Catalyst 9300 Series switches to aggregate FAN rings and their traffic from and to offshore wind turbines.

Figure 4-8 FAN Aggregation Design



We recommend that between one and nine FAN rings be aggregated to a stack of Catalyst 9300 switches for optimal network performance. If there are more than 200 turbines or base switches in a wind farm, another stack of two Catalyst 9300 switches can be added to the FAN aggregation network in the offshore substation OSS.

Offshore Substation Network and Building Blocks

This section discusses the design for a wind farm OSS network. The OSS network has following building blocks:

- OSS core network: Provides network layer 3 routing across offshore and onshore substations
- OSS DMZ and third-party or other networks: Provides secure remote access for corporate employees and third-party vendors to OSS assets
- OSS infrastructure network: Hosts OSS infrastructure services and application servers

OSS Core Network Design

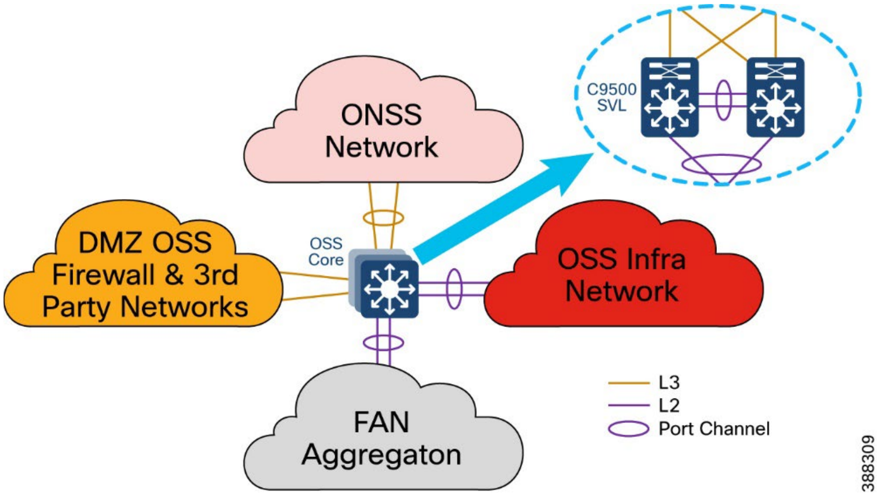
An offshore substation core network is composed of a pair of suitably sized layer 3 devices that provide resilient core networking and routing capabilities. Multilayer switches may be used as core switches, even though they are intended for routing. In the wind farm solution architecture, Cisco Catalyst 9500 Stackwise Virtual (SVL) switches are used as OSS core network switches.

The OSS core connects to multiple components, and this connection should be resilient, providing higher bandwidth (10Gbps) layer 3 links. The OSS core network connects the following building blocks in an OSS network and provides connectivity through fiber uplinks to the onshore substation network (ONSS), as shown in Figure 4-9.

- ONSS network: Connects to ONSS core switches.
- OSS infrastructure network: Provides layer 2 access switch connectivity to infrastructure applications such as CVC, SCADA servers, WLC, and so on.

- FAN aggregation: Aggregates FAN rings in a wind farm
- OSS DMZ and firewall: Connects to third-party networks (for example, turbine vendor SCADA networks such as GE, VESTAS, and others, and substation automation networks export cable HVDC and AC systems).

Figure 4-9 OSS Core Network Design



In Figure 4-9, a pair of Cisco Catalyst 9500 switches in Stackwise Virtual (SVL) configuration provides core network high availability across OSS networks with layer 3 links to the OSS DMZ firewall and ONSS core. These layer 3 links can be configured as Equal-Cost Multi Pathing (ECMP) routing links or links bundled in a layer 3 port channel.

The C9500 SVL switch connects to the OSS infrastructure and FAN aggregation switches using layer 2 port channels with each port channel bundling two 10 Gb ethernet interfaces.

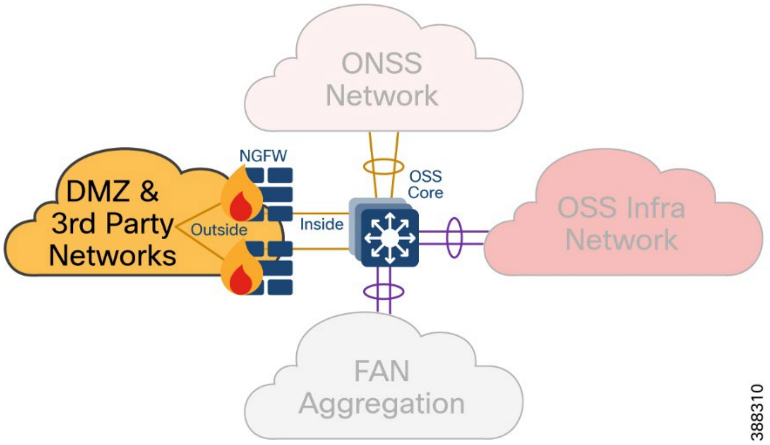
OSS DMZ and Third-Party Network

A DMZ in a wind farm OSS network provides a layer of security for the internal network by terminating externally connected services at the DMZ and allowing only permitted services to reach the internal network nodes.

Any network service that runs as a server that communicates with an external network or the Internet is a candidate for placement in the DMZ. Alternatively, these servers can be placed in a data center and be reachable only from the external network after being quarantined at the DMZ.

Cisco Next-Generation Firewall (NGFW) is deployed with outside interface connectivity to third-party turbine vendor networks and inside interface connectivity to the OSS core network, as shown in Figure 4-10. A Firepower Management Center (FMC) in the control center centrally manages all Firepower instances in the OSS and ONSS networks.

Figure 4-10 OSS DMZ Network



The OSS DMZ is composed of a resilient pair of Cisco NGFW Firepower 2100 or 4100 Series appliances. The Firepower in OSS DMZ provides OSS network security protection from outside vendor networks.

OSS Infrastructure Network

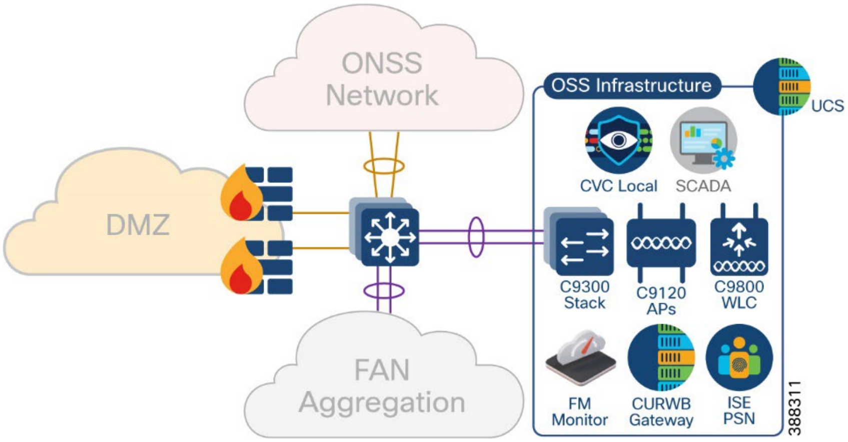
This section covers various infrastructure components and application servers in a wind farm network. The OSS infrastructure is composed of a set of resources that are accessible by devices or endpoints across the FAN and TAN. The OSS infrastructure is deployed with a pair of Cisco Catalyst 9300 Series switches in a stack to extend access to various applications and servers, as shown in Figure 4-11 as Option 1.

You also can deploy the OSS infrastructure with a separate access switch stack and UCS server for wind farm OSS IT and OT applications respectively, as shown in Figure 4-12 as Option 2. The OSS infrastructure includes of:

- One or more Cisco Unified Computing System (UCS) servers for hosting virtual machines for the applications
- On Cisco Cyber Vision Center (CVC) Local
- Two wireless controllers for Wi-Fi network management
- One or more ISE PSNs*
- Two CURWB gateways (FM1000)
- Two Catalyst 9800 WLCs
- Four FM3500 or FM4500 devices with 90-degree horn antennas
- One URWB FM monitor
- IW6300 or C9120 APs for Wi-Fi access
- One CURWB FM monitor
- SCADA server application

Figure 4 11 shows the wind farm OSS infrastructure network and its components.

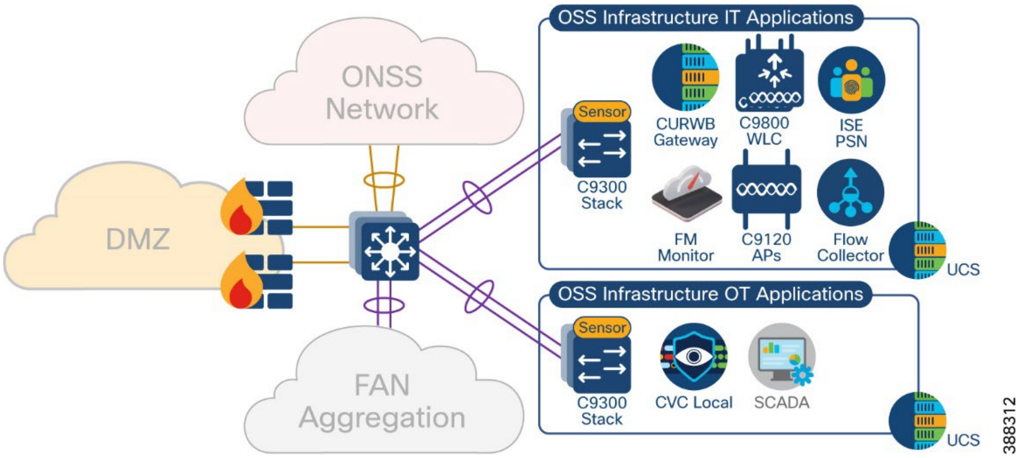
Figure 4-11 OSS Infrastructure Network Deployment Option 1



*ISE PSN may optionally be deployed at the OSS infrastructure network for the distributed deployment of ISE with PAN at the control center. You also may choose to decentralize PSNs if there is a latency concern.

Figure 4-12 shows the wind Farm OSS Infrastructure network option for IT and OT applications separated into two access switch stacks and UCS servers.

Figure 4-12 OSS Infrastructure Network Deployment Option 2



Onshore Substation Network

In a wind farm network, an onshore substation (ONSS) is a renewable energy site that is normally in remote areas where communication network is not readily available.

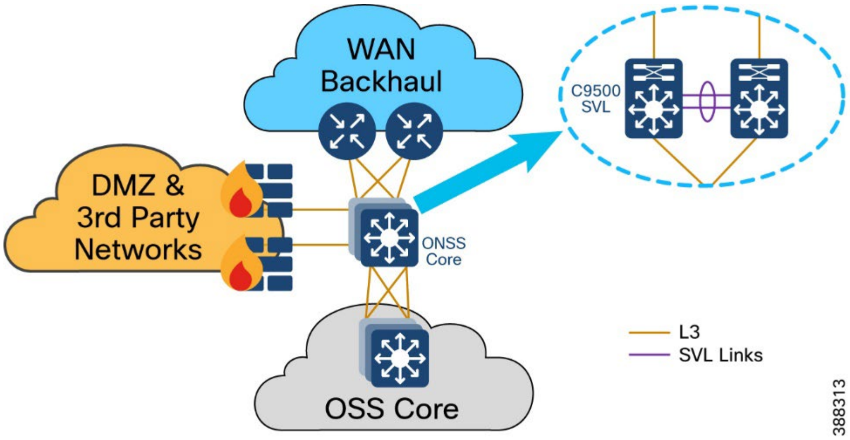
Generally, offshore substations connect to ONSSs in rural locations where access to backhaul technologies is limited. While offshore to onshore connectivity is served by fiber optic cable, the backhaul from the onshore location is more challenging and often relies on service provider network availability for services such as fiber, MPLS, metro Ethernet, and so on.

ONSS Network Design

In the wind farm solution architecture, Cisco Catalyst 9500 Stackwise Virtual (SVL) switches are used as ONSS core network switches. The ONSS core connects to multiple components. The connections should be resilient and provide higher bandwidth (10Gbps) and layer 3 links for scalable L3 routing.

Figure 4-13 shows the building blocks in an ONSS network that the ONSS core network connects to.

Figure 4-13 ONSS Network and its Building Blocks



OSS network building blocks include:

- OSS network: Connects to an OSS core switch via 10 Gb fiber links
- ONSS DMZ and firewall: Connects to third-party networks (for example, turbine vendor SCADA network, power control and metering network, export cable HVAC and DC system)
- WAN backhaul: Connects wind farm data center and control center to the ONSS via service provider MPLS, 4G LTE, and so on.

The ONSS DMZ is similar to the OSS DMZ that is discussed in OSS DMZ and Third-Party Network. WAN backhaul and control center are discussed in detail in the following section.

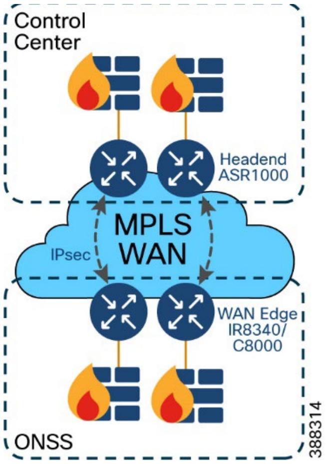
WAN Network Design

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

ONSS WAN router can provide inline firewall (zone-based firewall) functionality, or a dedicated firewall can be placed beyond the substation router to protect wind farm assets. This approach results in a unique design in which a DMZ is required at the substation edge. All communications into and out of the substations network must pass through the DMZ firewall. The zone traffic egressing the substation edge should be encrypted using IPsec and put into separate logical networks using Layer 3 virtual private network (L3VPN) technology, as shown in Figure 4-14.

A WAN tier aggregates the wind farm operator’s control center and onshore and offshore substations. A Cisco IR8340 or C8000 Series Router deployed as an ONSS WAN edge router serves as an interface between the onshore substation and the control center.

Figure 4-14 Example Wind farm WAN Backhaul



WAN circuits and backhaul failure options are efficiently designed, provisioned, and managed using Cisco SD-WAN. For more information, see *Cisco SD-WAN Design Guide*:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

The wind farm WAN backhaul design is similar to the Cisco Substation Automation Solution WAN backhaul design. For more information about WAN backhaul design, see *Substation Automation Design Guide – The New Digital Substation*:

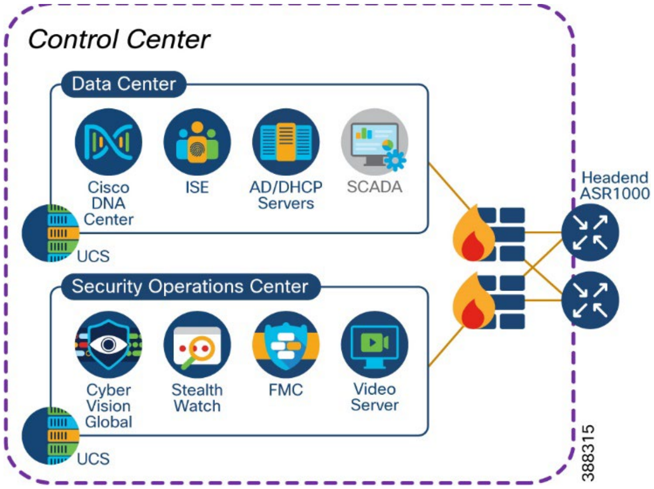
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/3-0/CU-3-0-DIG.pdf

Control Center Design

A wind farm asset operator’s control center hosts multiple IT and OT applications with other network infrastructure servers. All communications to the control center are secured by using a pair of firewalls in HA deployment and a pair of Cisco ASR1000 series routers acting as headend or hub routers. Cisco ASR1000 Series routers terminate all IPSec tunnels from remote substations WAN edge routers.

Figure 4-15 shows a wind farm control center with its IT and OT applications and servers.

Figure 4-15 Wind farm Control Center



The control center network consists of:

- One or more Cisco ASR1000 Series routers for WAN headend
- One or more Cisco Firepower 2100 or 4100 Series firewalls
- One or more Cisco Unified Computing System (UCS) servers for hosting virtual machines for applications
- One Cisco DNA Center for network management
- One or more Cisco ISE policy administration node (PAN)*
- One centralized Active Directory
- One centralized DHCP server
- One network time protocol (NTP) server
- One SCADA server application for wind farm turbine control
- One video server for CCTV
- One Cyber Vision Global
- One Cisco Centralized Firepower Management Center
- One Cisco Secure Networks Analytics Manager (SMC)

* PSN may optionally be deployed at the OSS Infrastructure network for the distributed deployment of ISE with the PAN located at the control center. You may also choose to decentralize the PSN whenever there is a concern about latency.

Network VLANs and Routing Design

This section covers the different VLANs in a wind farm network and virtual routing and forwarding (VRF) for layer 3 routing between OSS and ONSS core networks. The wind farm network is segmented by using VLANs for various endpoints and applications traffic. There is a dedicated VLAN and VRF for each service, endpoint, or application traffic in the network. Table 4-3 summarizes the design guidance for creating multiple VRFs and VLANs in the network.

Table 4-3 VLANs and VRFs in the Wind Farm Network Design

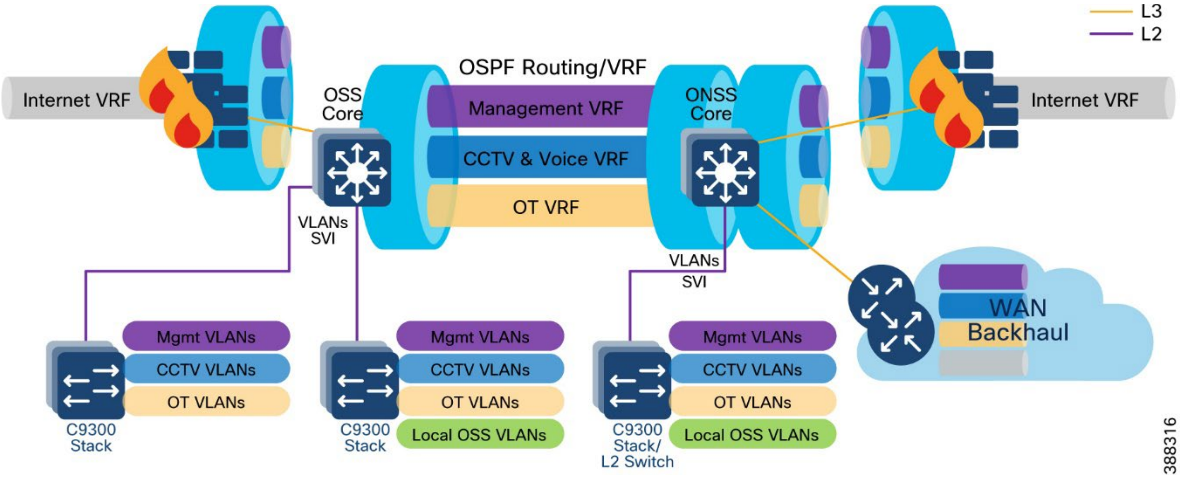
VRF	VLAN Description
Management VRF (VRF for network management traffic)	• Network device management VLAN(s) • Wi-Fi and CURWB aps management VLAN(s) • FAN and TAN REP ring administrative VLAN(s) • Cyber Vision (CV) collection network VLAN(s)
Video and voice VRF (VRF for CCTV cameras and IP telephony voice traffic)	• VLANs for CCTV Cameras in FAN and TAN • IP telephony devices voice VLAN

Wi-Fi access VRF	• Employee and contractor Wi-Fi access VLAN • Guest Wi-Fi access VLAN
CURWB traffic VRF	• CURWB traffic VLAN
Operational technology (OT) (VRF for all renewables and OT traffic in the network)	• VLANs for SCADA traffic such as weather systems, HVAC, fire detection, lightning detection, and other systems such as wildlife monitoring • VLANs for automation systems such as I/O controllers, PLCs, and so on
Internet VRF (VRF for device Internet access from the wind farm network)	• DMZ VLANs for Internet traffic routing in OSS and ONSS networks
Global routing table (GRT)	• VLANs local to OSS network (not to be routed) • VLANs local to ONSS network (not to be routed)

A VRF creates a separate routing and forwarding table in the network for IP routing, which is used instead of a default global routing table (GRT). A VRF provides high-level network segmentation across multiple services or traffic in the network. Each VLAN layer 3 interface (SVI) is created and assigned to a VRF for layer 3 routing in the OSS and OSS core switches. The VRF-lite feature is used for layer 3 routing with a separate IGP (OSPF) routing protocol instance per VRF for routing between the OSS and ONSS core networks.

Figure 4-16 illustrates the layer 3 IP routing design in the wind farm architecture.

Figure 4-16 Wind Farm Network IP Routing Design



For more information about the VRF-lite feature, see “Information about VRF-lite” in *IP Routing Configuration Guide, Cisco IOS XE Dublin 17.10.x (Catalyst 9500 Switches)*:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-10/configuration_guide/rtng/b_1710_rtng_9500_cg/configuring_vrf_lite.html#concept_uk1_s24_ngb

OSPF is an interior gateway protocol (IGP) that is designed for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF per VRF is configured for routing between the OSS and ONSS core networks.

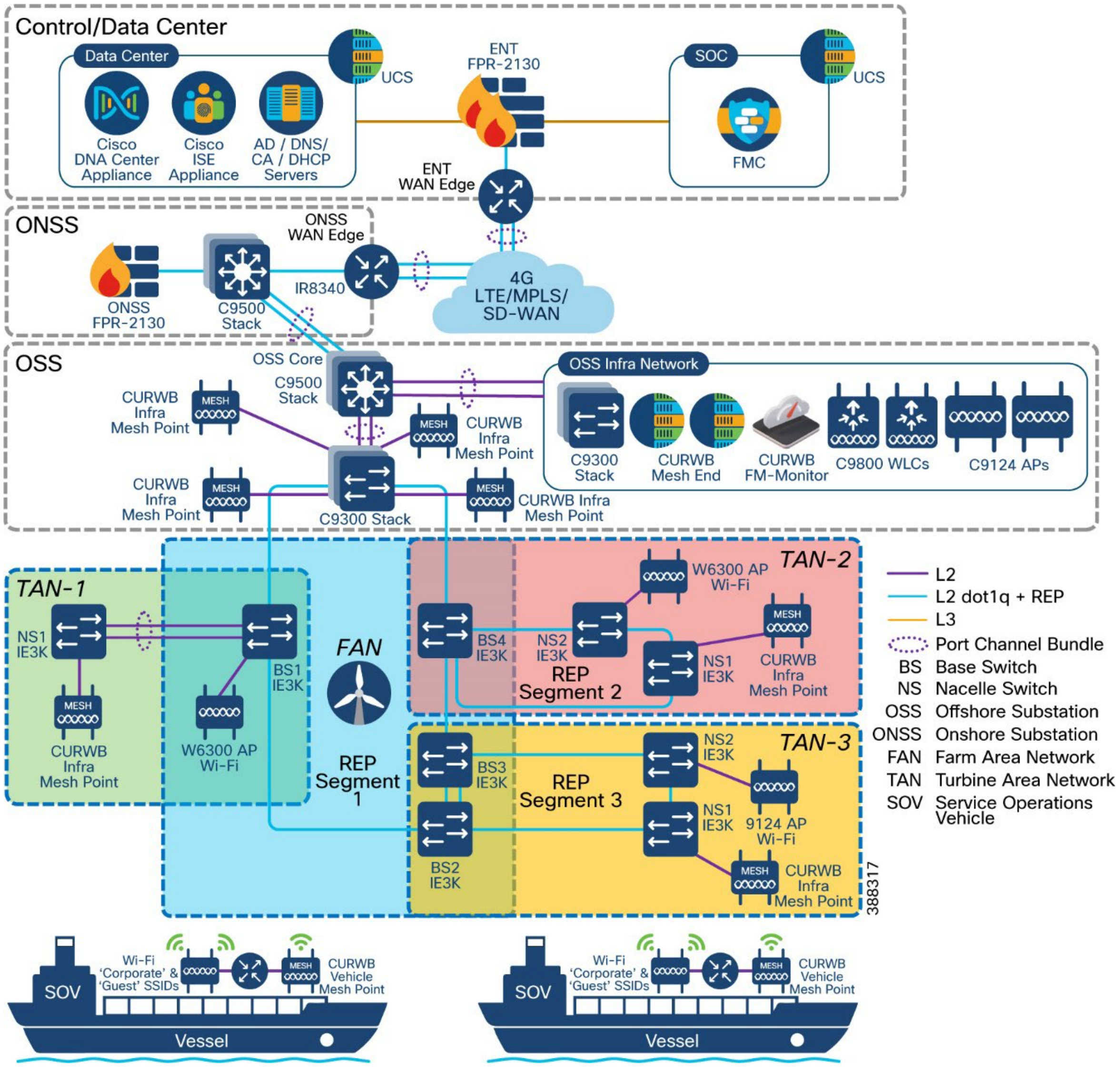
For more information about the OSPF protocol, see “Information About OSPF” in *IP Routing Configuration Guide, Cisco IOS XE Dublin 17.10.x (Catalyst 9500 Switches)*:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-10/configuration_guide/rtng/b_1710_rtng_9500_cg/configuring_ospf.html#concept_h1g_rkz_kgb

Wireless Network Design

Figure 4-17 shows the offshore wind farm wireless architecture. This architecture includes URWB on the OSS and TAN for SOV connectivity and enterprise Wi-Fi on the OSS, TAN, FAN, and vessel. The following sections provide details about the URWB architecture.

Figure 4-17 Offshore Wind Farm Wireless Architecture (Wi-Fi and URB)



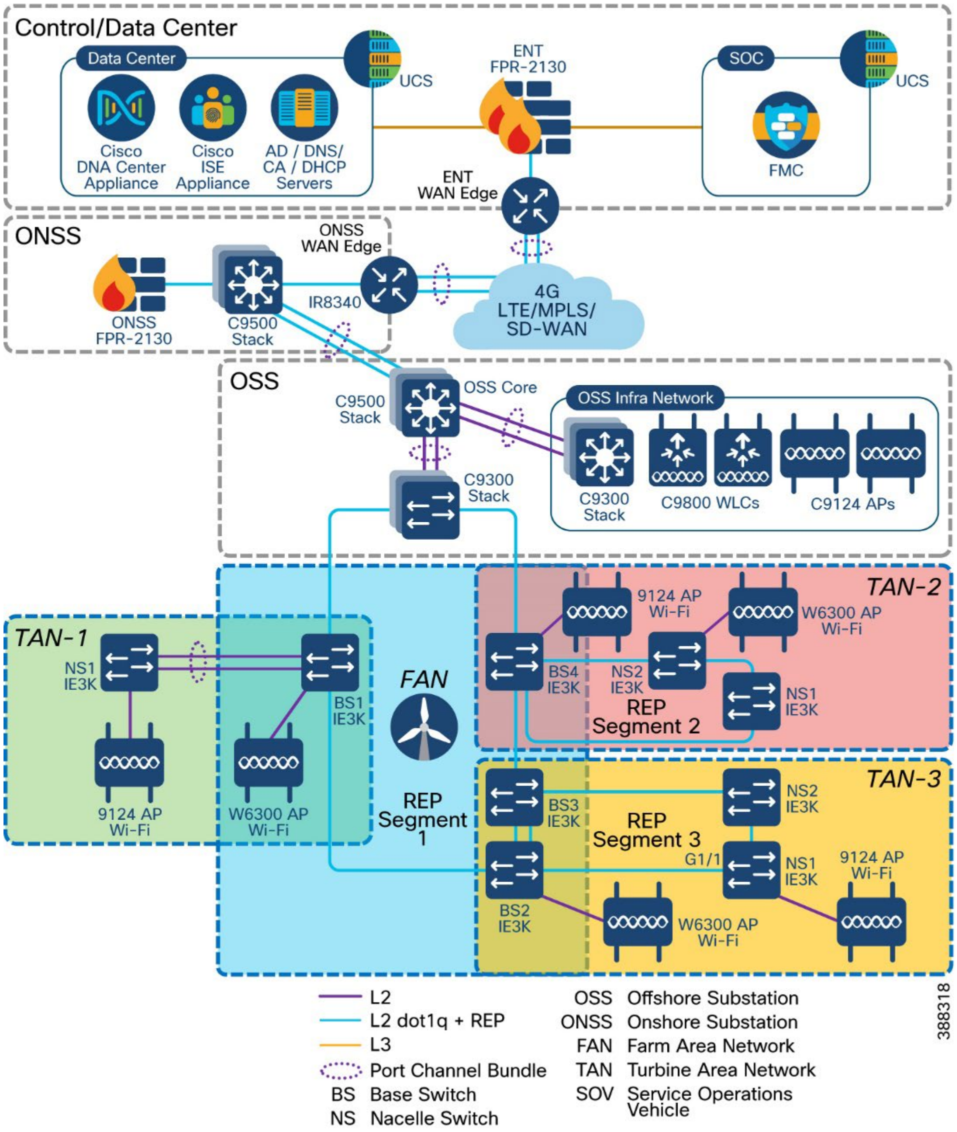
Enterprise Wi-Fi Network

This section provides an overview of the Cisco Wi-Fi deployment at an offshore windfarm for employee, contractor, and guest access on the OSS, FAN, and TAN. The wireless deployment leverages Cisco's next-generation wireless controller, the Cisco Catalyst 9800 WLC deployed within the OSS infra network, and is managed centrally via the Cisco DNA Center that is located at the control center. Microsegmentation is provided by Cisco ISE and TrustSec.

Cisco Wi-Fi Architecture for Off-Shore Windfarm

Figure 4-18 shows the Wi-Fi architecture for an offshore wind farm deployment, which enables Wi-Fi access for employees, contractors, and guests on the OSS network, FAN, and TAN.

Figure 4-18 Offshore Windfarm Wi-Fi Access Architecture



The Cisco DNA Center is located onshore within the control center. It has connectivity to the Cisco Catalyst 9800 WLC over a WAN connection. The DNA Center is used to centrally manage and configure the WLCs and APs. It can be used to view the health metrics of the wired and wireless networks that are located within the offshore windfarm network. The DNA Center also is used to configure the TrustSec matrix that Is used for segmentation of user traffic.

A Microsoft Windows servers is located within the control center and provides the following functionality:

- Employees user identity store (group, username, password)
- Contractor user identity store (group, username, password)
- Certificate authority (CA)
- DNS server
- DHCP server (DHCP scopes for employee and guest wireless access)

The ISE server is collocated in the control center. The ISE server acts as the central identity and policy management server used for wireless IEEE 802.1X authentication and authorization. It assigns security group tags (SGTs) to clients. These tags are used for microsegmentation. The ISE server is integrated with the Cisco DNA Center and the Catalyst 9800 WLC.

ISE also hosts the wireless guest portal for guest wireless access.

The appropriate firewall ports need to be opened on the enterprise firewall at the boundary of the control center for DNA Center to WLC communications (configuration and telemetry), ISE to WLC communication (IEEE 802.1X, TrustSec), and WLC to AD connectivity (DHCP, DNS ports).

The Cisco Catalyst 9800 WLCs are deployed as a redundant SSO high-availability pair with the OSS infra network connected to the Cisco Catalyst 9300 switches. The We-Fi deployment is managed using Cisco DNA Center and use Cisco ISE for IEEE802.1X wireless and guest access. A good practice is to use different WLC interfaces for wireless management (access port), wireless client traffic (trunk port) and guest user traffic (access port).

Cisco IW6300s (ruggedized APs) or 9124s (enterprise APs) are deployed in local mode on the OSS, FAN BS, or TAN NS to provide wireless access where needed. The wireless traffic is carried over the CAPWAP tunnel from the APs to the WLC and dropped off in the appropriate client VLAN on the Catalyst 9300 switch that is located within the OSS infra network.

A dedicated VLAN and subnet needs to be assigned for wireless AP management. One or more VLANs and subnets need to be assigned for wireless client traffic. A dedicated VLAN and subnet needs to be assigned for guest wireless traffic. The AP management subnet needs to be trunked to whichever switch has APs connected to it. It also needs to exist on the switches to which the WLCs are connected. The AP switch port can be configured as an access port in the AP management VLAN with spanning-tree portfast enabled.

The SVIs for the VLANs and subnets need to exist on the Cisco 9500 stack.

Different User groups need to be created for employee users and contractors within Microsoft Active Directory (AD) or another LDAP server of your choice. Employee and contractor users need to be created in Microsoft AD or LDAP server and assigned to the appropriate groups. Unique scalable group tags (SGTs) need to be assigned for the employee, contractor, and guest user groups within ISE.

The employee SGT usually is configured to provide full access to all the required enterprise services so that it can accomplish its job functions. The contractor SGT usually provides limited access only to the services that it needs to access for its function, or only internet access if that is all it requires. The guest SGT is provided only with internet access. These policies can be defined and configured on the Cisco DNA Center and pushed to the ISE. The ISE then pushes these policies to the WLC.

When a wireless client is connected and is authenticated by ISE, the IP-SGT binding is generated on the controller.

CURWB Wireless Backhaul

Use case for Service Operations Vessel Wireless Backhaul within a Wind Farm

There is a need for a reliable, high-bandwidth wireless backhaul solution that connects to the large SOVs (SOVs) and smaller crew transfer vessels (CTVs), both of which move staff around an offshore wind farm estate. During periods near shore, a vessel should use public cellular connectivity.

This section provides an overview of CURWB technology, the wireless network components needed to build out the wind farm solution, and the high-level and low-level architecture to support connectivity SOVs and CTVs to the OSS network.

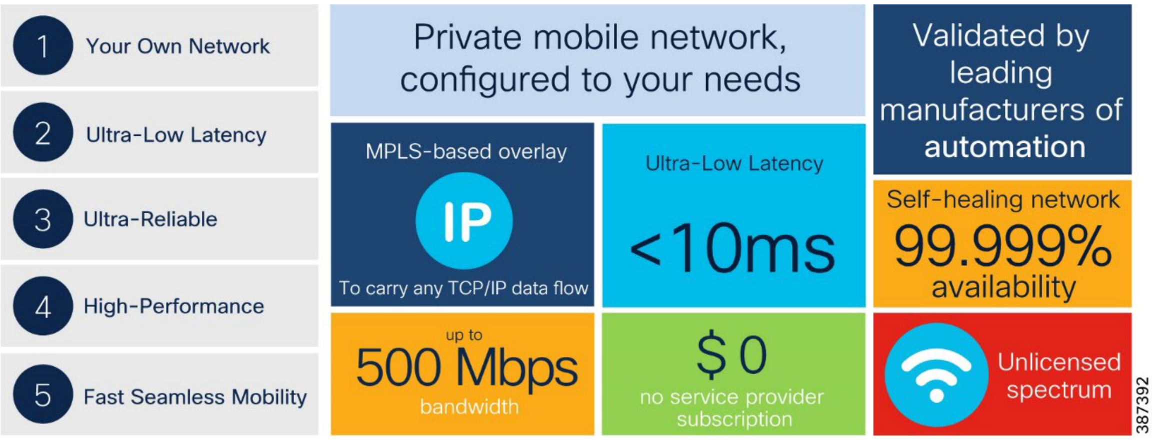
The following high-level requirements are met by this CVD:

- Reliable wireless backhaul connectivity to vessels that are within a 10 km radius of an OSS platform using CURWB radios.
- The head end or wayside is on the OSS.
- Vessels can switch to cellular connectivity when in range of onshore cellular networks.
- Vessels have specialist antennas with appropriate radios and modems.
- Antennas on vessels automatically adjust their direction to optimize the radio signals for best performance by using a GPS feed to dynamically change the beam direction.
- Antennas on vessels are combination antennas that support 5 GHz CURWB wireless and public LTE.
- Target throughput: 30 to 50 Mbps for vessels that are within a 10 km radius of an OSS.
- Support for connectivity to a public LTE network when a vessel is going to or from a harbor, extending to a few miles offshore.
- IP telephony extended to a vessel, with Cisco Survivable Remote Site Telephony (SRST) preferred onboard for periods when no OSS connectivity is available.
- Corporate and guest user networks to be extended to the SOV using fixed and Wi-Fi connections.

CURWB Overview

Figure 4-19 highlights some key features and capabilities of CURWB that are related to performance, ultra low latency, 0 ms seamless handovers, and reliability.

Figure 4-19 Key CURWB Capabilities



CURWB: Key Technology Pillars

The following key technologies underlay the foundation for the CURWB solution:

- Prodigy 2.0: MPLS-based transmission protocol built to overcome the limits of standard wireless protocols.
- Fluidity: Proprietary fast-roaming algorithm for vehicle-to-wayside communication with a 0 ms roam delay and no roam loss for speeds up to 200 Mph (360 kph).
- TITAN: Proprietary fast-failover high-availability mechanism that provides hardware redundancy and carrier-grade availability.

Prodigy 2.0: MPLS Overlay

CURWB uses the proprietary wireless-based MPLS transmission protocol Prodigy to discover and create label-switched paths (LSPs) between mesh-point radios and mesh end(s). Prodigy helps make the wireless mesh networks resilient. It also helps making fixed and mobility networks resilient. MPLS provides an end-to-end packet delivery service operating between layer 2 and layer 3 of the OSI network stack. It relies on label identifiers, rather than on the network destination address as in traditional IP routing, to determine the sequence of nodes to be traversed to reach the end of the path.

Fluidity

Fluidity enables a vehicle that is moving between multiple infrastructure APs to maintain end-to-end connectivity with seamless handoffs between APs. Vehicle radios negotiate with the infrastructure APs and form a new wireless connection to a more favorable infrastructure AP with better signal quality before breaking or losing their currently active wireless connections.

TITAN: Hardware Redundancy and High-Availability

TITAN is a proprietary fast-failover feature that provides high-availability and protection against hardware failures. This feature virtually guarantees uninterrupted service for mission-critical applications where safety and or operations would otherwise be compromised by failure of a single radio or gateway device. Leveraging an MPLS-based protocol, TITAN achieve device failovers within 500 ms within layer 2 and layer 3 networks.

CURWB Network Components

CURWB Mesh End Gateway

All fluidity and fixed infrastructure deployments need a mesh end. The mesh end functions as a gateway between wireless and wired networks. We recommend that all systems using Fluidity use a redundant pair of mesh end gateways to terminate the MPLS tunnels, aggregate traffic, and act as an interface between the wired and wireless network. Mesh end gateways can also be thought of as MPLS label edge routers (LERs) on the infrastructure network. The mesh end gateway is responsible for encapsulating the traffic that comes from the wired network to the fluidity overlay network using MPLS, decapsulating MPLS, and delivering standard datagrams onto the wired network.

CURWB gateways are rugged, industrial grade network appliances that make setup and management of medium and large-scale CURWB fluidity and fixed infrastructure deployments fast and easy.

CURWB mesh end gateways are deployed as a redundant pair within an OSS infrastructure network.

Figure 4-20 CURWB Gateway Models Comparison

Feature	FM1000	FM10000
Scalability	Up to 1 Gbps	Up to 10 Gbps
Core	Dual core or quad core SOC	Intel Core i7
Ports: RJ45	2 x Gbit	4 x GE RJ45 Intel i210
Ports: fiber	–	4 x 10 Gbe SFP Intel i350-AM4
Power supply	Single	Redundant

CURWB FM3500 Endo Radio Unit

Figure 4-21 FM3500 Endo Radio Unit

The Cisco FM3500 Endo is used to create point-to-point, point-to-multipoint, mesh, and mobility networks with a throughput of up to 500 Mbps. It is especially suitable for wayside-to-vehicle communication in industries where reliable, stable, and low-latency communications are essential for safe operations and optimal productivity.

For the offshore windfarm deployment, the FM3500 Endo can be used as an infrastructure radio on the OSS, turbines, and vessels.

For more information, see the Cisco FM3500 Endo data sheet:

https://www.cisco.com/c/en/us/products/collateral/wireless/ultra-reliable-wireless-backhaul/datasheet-c78-744549.html

CURWB FM4500 Radio Unit

Figure 4-22 Cisco FM4500 Mobi and Cisco FM4500 Fiber

The Cisco FM4500 is a high-performance mobility-communications radio transceiver designed to deliver fast, stable connectivity from any slow-moving or fast-moving vehicle to a wayside network, particularly in mission-critical market sectors and extreme environments.

The FM4500 MOBI comes in a rugged die cast aluminum housing that has been built for harsh outdoor environments. It consists of industrial-grade anti-vibration M12 ports and a QMA connector. Optionally, you can order the fiber-enabled FM4500 Fiber, which provides a fiber port with an XCO connector.

The Ethernet model (FM4500 Mobi) has two 10/100/1000 M12 ports. The fiber model (FM4500 Fiber) has one dual LC ruggedized SFP XCO connector (transceiver not included) and one 10/100/1000 M12 port. The radio can either be powered by using PoE+ output from a switch or 48 VDC input from an onboard power source.

Note: The FM4500 Mobi radio can also be powered using both DC power and PoE at the same time, which provides a redundant power capability.

We recommend that the FM4500 MOBI be deployed on board vessels because it is vibration resistant. The FM4500 MOBI can also be used as an infrastructure access radio within an offshore wind farm deployment.

For more information, see:

- Cisco FM4500 MOBI data sheet:

  https://www.cisco.com/c/en/us/products/collateral/wireless/ultra-reliable-wireless-backhaul/datasheet-c78-744552.html
- Cisco FM4500 FIBER data sheet:

  https://www.cisco.com/c/en/us/products/collateral/wireless/ultra-reliable-wireless-backhaul/datasheet-c78-744551.html
- Cisco Optics-to-Device Compatibility Matrix:

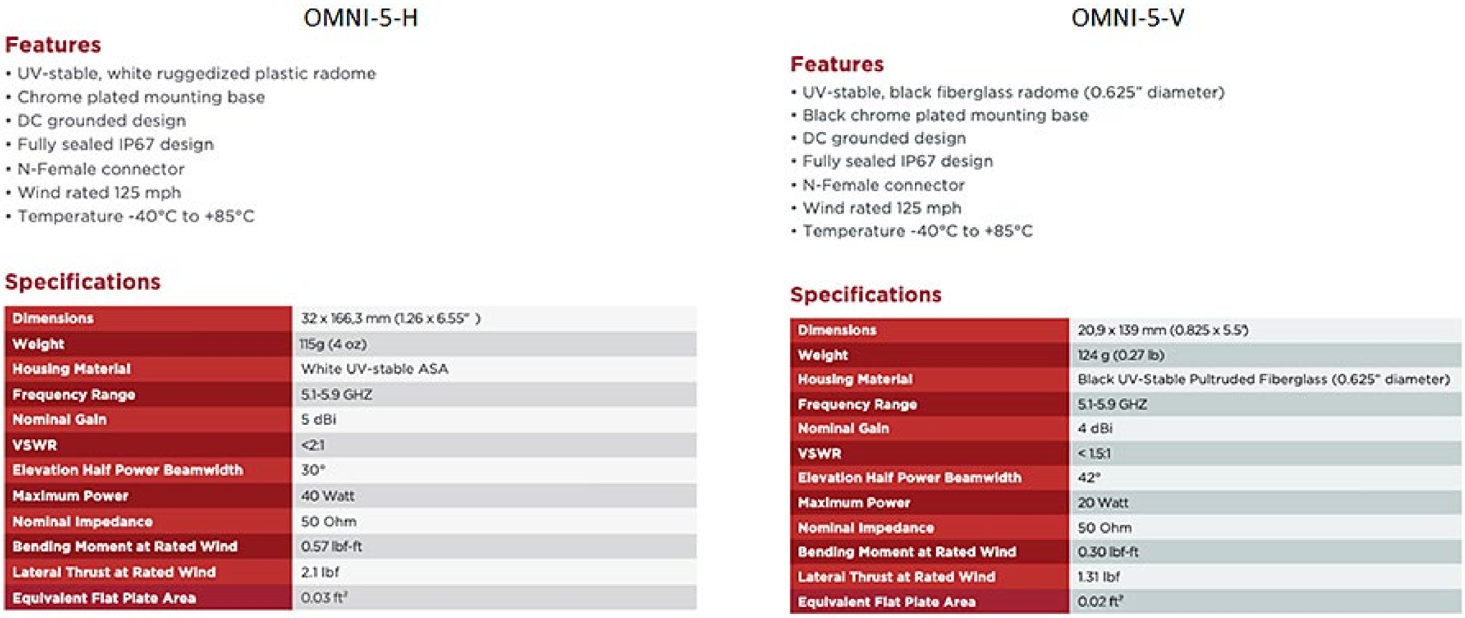
  https://tmgmatrix.cisco.com/?npid=4601&npid=4602&npid=5001

FM-OMNI-5-KIT Antenna

The FM-OMNI-5-KIT antenna consists of two antennas: an FM-OMNI-5-H, which is a horizontally polarized antenna, and an FM-OMNI-5-V, which is a vertically polarized antenna. FM-OMNI-5-H horizontally polarized omnidirectional antennas are designed for long-lasting operation with outdoor access points. The FM-OMNI-5-V vertically polarized omnidirectional design utilizes a linear array, encapsulated in a heavy-duty fiberglass radome with a thick-walled mounting base for reliable, long-term use.

The rugged design of these antennas allows them to withstand harsh environments, making the antennas ideal for industrial wireless applications. The antennas are DC grounded for ESD protection of radio components.

Figure 4-23 FM-OMNI-5-KIT Antenna Specifications



OMNI-5-H

Features

- UV-stable, white ruggedized plastic radome
- Chrome plated mounting base
- DC grounded design
- Fully sealed IP67 design
- N-Female connector
- Wind rated 125 mph
- Temperature -40°C to +85°C

Specifications

Dimensions	32 x 166.3 mm (1.26 x 6.55")
Weight	115g (4 oz)
Housing Material	White UV-stable ASA
Frequency Range	5.1-5.9 GHZ
Nominal Gain	5 dBi
VSWR	<2:1
Elevation Half Power Beamwidth	30°
Maximum Power	40 Watt
Nominal Impedance	50 Ohm
Bending Moment at Rated Wind	0.57 lbf-ft
Lateral Thrust at Rated Wind	2.1 lbf
Equivalent Flat Plate Area	0.03 ft²

OMNI-5-V

Features

- UV-stable, black fiberglass radome (0.625" diameter)
- Black chrome plated mounting base
- DC grounded design
- Fully sealed IP67 design
- N-Female connector
- Wind rated 125 mph
- Temperature -40°C to +85°C

Specifications

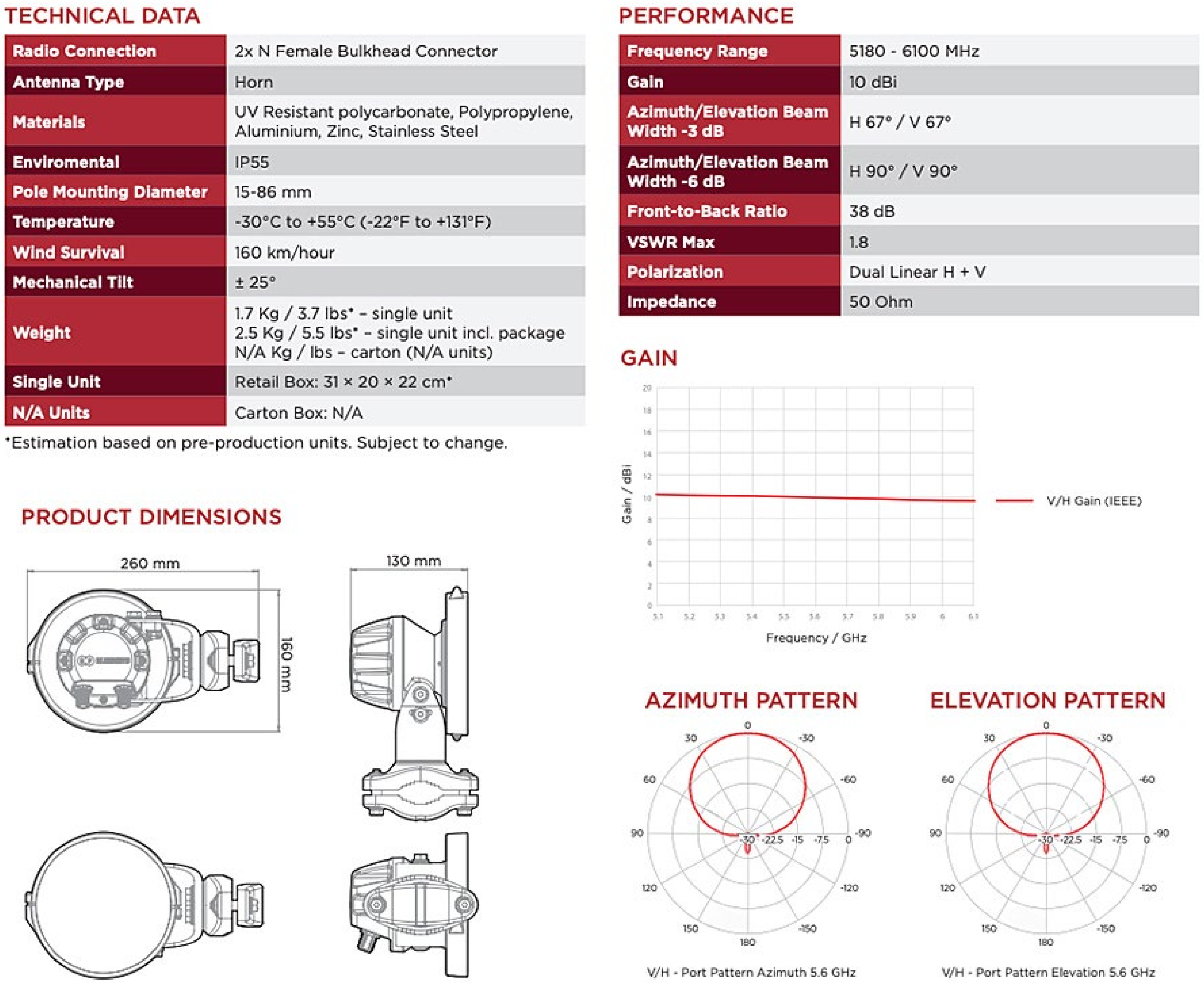
Dimensions	20.9 x 139 mm (0.825 x 5.5")
Weight	124 g (0.27 lb)
Housing Material	Black UV-Stable Pultruded Fiberglass (0.625" diameter)
Frequency Range	5.1-5.9 GHZ
Nominal Gain	4 dBi
VSWR	< 1.5:1
Elevation Half Power Beamwidth	42°
Maximum Power	20 Watt
Nominal Impedance	50 Ohm
Bending Moment at Rated Wind	0.30 lbf-ft
Lateral Thrust at Rated Wind	1.31 lbf
Equivalent Flat Plate Area	0.02 ft²

Note: If a wind farm deployment does not use BATS antennas on SOVs, the OMNI-5-KIT antenna can be used for each of the CURWB radios instead.

FM-Horn-90 Antenna

The FM-Horn-90 is a connectorized symmetrical horn antenna with carrier class performance. It offers unique RF performance in a compact package. Scalar horn antennas have symmetrical beams with identical patterns in the vertical and horizontal planes. Extremely small side lobes result in greatly decreased interference. FM-Horn-90 antennas are ideal for covering areas with close-in clients where null zone issues occur. This antenna makes high density AP clusters and radio colocation practical due to its radiation pattern and compact size. The FM-Horn-90 antenna is equipped with N-female connectors.

Figure 4-24 FM-Horn-90 Specifications



TECHNICAL DATA

Radio Connection	2x N Female Bulkhead Connector
Antenna Type	Horn
Materials	UV Resistant polycarbonate, Polypropylene, Aluminium, Zinc, Stainless Steel
Enviromental	IP55
Pole Mounting Diameter	15-86 mm
Temperature	-30°C to +55°C (-22°F to +131°F)
Wind Survival	160 km/hour
Mechanical Tilt	± 25°
Weight	1.7 Kg / 3.7 lbs* - single unit 2.5 Kg / 5.5 lbs* - single unit incl. package N/A Kg / lbs - carton (N/A units)
Single Unit	Retail Box: 31 × 20 × 22 cm*
N/A Units	Carton Box: N/A

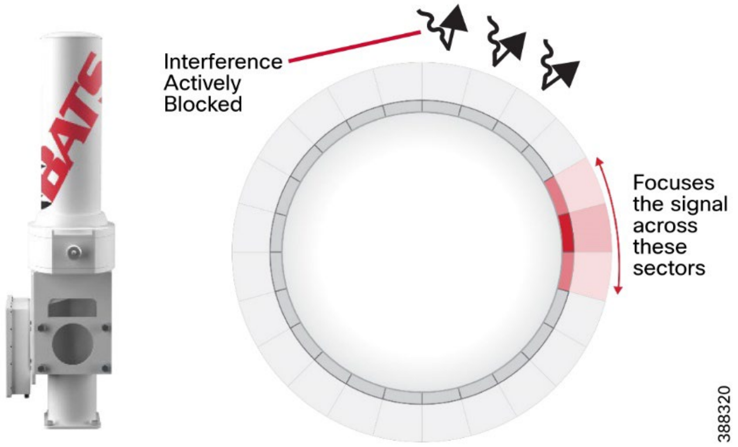
*Estimation based on pre-production units. Subject to change.

PERFORMANCE

Frequency Range	5180 - 6100 MHz
Gain	10 dBi
Azimuth/Elevation Beam Width -3 dB	H 67° / V 67°
Azimuth/Elevation Beam Width -6 dB	H 90° / V 90°
Front-to-Back Ratio	38 dB
VSWR Max	1.8
Polarization	Dual Linear H + V
Impedance	50 Ohm

BATS FAST 5.8 Intelligent Antenna System

Figure 4-25 BATS FAST 5.8 Intelligent Antenna System



BATS Wireless is a Cisco design-in partner. When integrated with Cisco industrial wireless products, including the CURWB backhaul and cellular gateway solutions, the BATS systems, deliver ultra high capacity connectivity for mobile and vehicles and SOVs.

Ideal for the unique demands of onshore and offshore operators in the energy, shipping, public transport, and defense markets, the integrated solutions provide the flexibility that is needed for dynamic and adaptive networks. They deliver a wealth of cutting-edge wireless communications and data opportunities for IoT sensing and monitoring applications, autonomous and augmented control applications, and intelligent multi-network roaming solutions.

The BATS FAST 5.8 high performance antenna is an ultra-fast (sub-500 ns) antenna array with 24 micro sectors. The solid-state and compact FAST antenna proves ideal for highly mobile environments where only minimal space is available, such as on a vehicle or small vessel.

A typical omnidirectional antenna is a passive antenna that radiates the signal in all directions equally. The BATS wireless FAST antenna is an active antenna made up of a cylindrical antenna array that sends a signal to a specific point, when required. Unlike a traditional omni or sector antenna, the FAST deploys active interference mitigation to block out unwanted signals while transmitting.

For the offshore windfarm deployment, we recommend that the BATS FAST 5.8 antenna be installed on the SOVs.

For more information, see the BATS website.

Note: It is not mandatory to utilize the BATS Antenna on SOVs. The OMNI-5-KIT antennas can be used for the CURWB radios on-board an SOV and the appropriate LTE antennas can be used for Cisco IR-1101 routers.

FM-Shield Ruggedized Enclosure

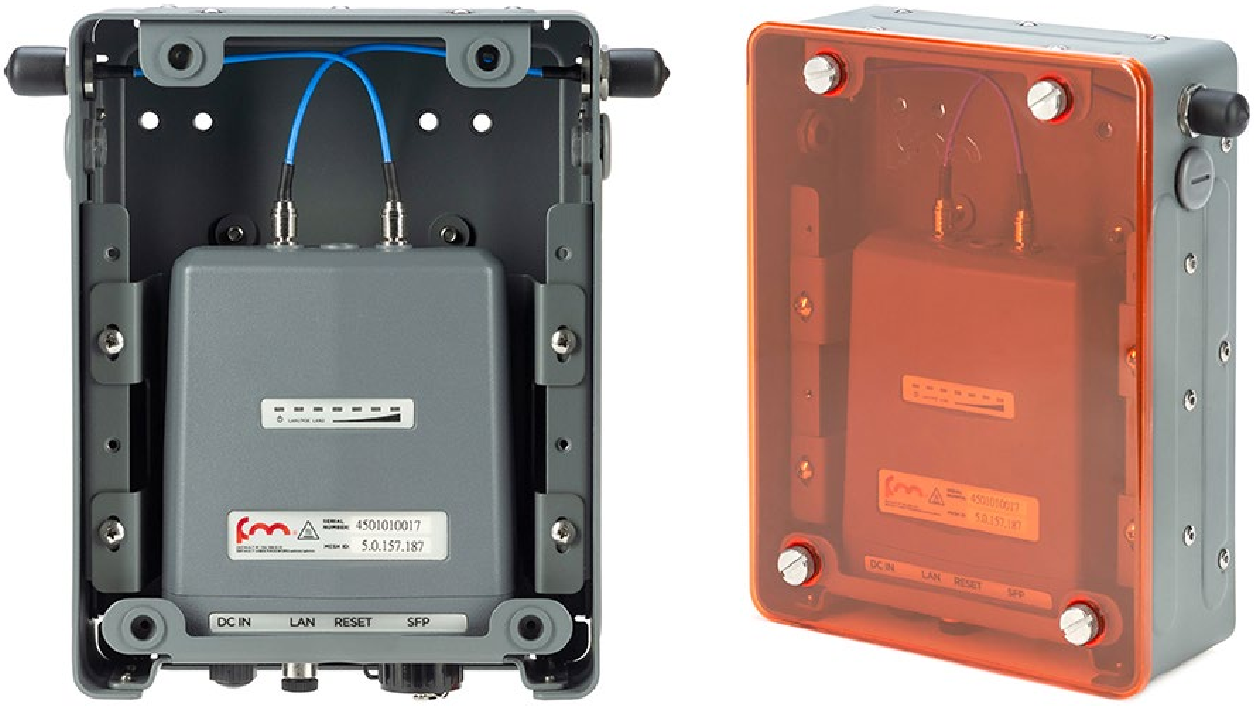
The FM-SHIELD is a proprietary ruggedized enclosure designed to ensure long-term durability and reliability of radios that are installed in outdoor environments.

If a 3200-series, 3500 ENDO, 4200-series, or 4500-series radio is installed outdoors, install the radio inside an FM-SHIELD. The FM-SHIELD provides additional protection from impact, salt, air, and water.

FM-Shield features include the following:

- Steel protective enclosure with polycarbonate cover, designed to protect against high-pressure water spray and impacts from heavy, fast-moving objects.
- Proven in high-vibration environments, including in all vehicles that are operated in a terminal environment.
- N-female antenna connectors for easy integration and minimal RF signal loss.
- Designed for installation within automation cabinets, and on vehicle hand railings and antenna poles. Also can be installed in a horizontal or vertical position while maintaining a vertical position of the radio.
- Semitransparent front panel with self-retaining screws for easy inspection.

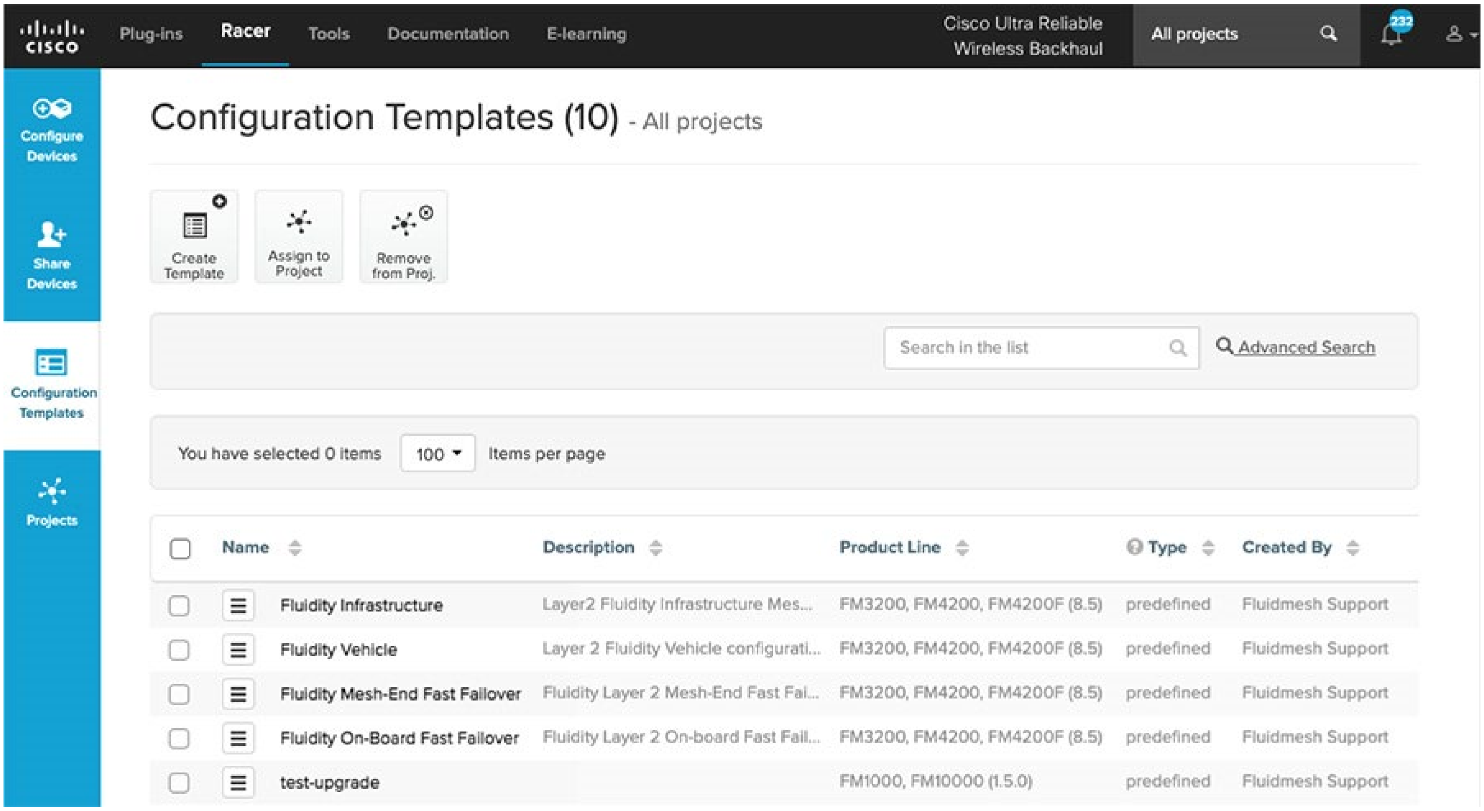
Figure 4-26 FM-Shield Ruggedized Enclosure



RACER

CURWB RACER is a centralized cloud-hosted server that can be used for provisioning of an entire CURWB 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. RACER supports almost all CURWB configuration options (basic and advanced). RACER can be used to create configuration templates and apply them to multiple CURWB devices of the same type. RACER templates can be applied in either online mode (if the CURWB devices have internet access) or offline mode (if the CURWB devices have no internet access). The advantage of using RACER is that, in addition to the device configuration, it upgrades firmware to the latest version that is available and applies the configured plug-ins. We recommend RACER for configuring CURWB devices in deployments of any size.

Figure 4-27 RACER Cloud-Hosted CURWB Configuration Tool



☐	Name	Description	Product Line	Type	Created By
☐	Fluidity Infrastructure	Layer2 Fluidity Infrastructure Mes...	FM3200, FM4200, FM4200F (8.5)	predefined	Fluidmesh Support
☐	Fluidity Vehicle	Layer 2 Fluidity Vehicle configurati...	FM3200, FM4200, FM4200F (8.5)	predefined	Fluidmesh Support
☐	Fluidity Mesh-End Fast Failover	Fluidity Layer 2 Mesh-End Fast Fai...	FM3200, FM4200, FM4200F (8.5)	predefined	Fluidmesh Support
☐	Fluidity On-Board Fast Failover	Fluidity Layer 2 On-board Fast Fail...	FM3200, FM4200, FM4200F (8.5)	predefined	Fluidmesh Support
☐	test-upgrade		FM1000, FM10000 (1.5.0)	predefined	Fluidmesh Support

Note: See the “RACER” section within the Implementation Guide for step-by-step instructions on how to use RACER to create the appropriate CURWB radio configuration templates and configuring CURWB radio devices.

FM Monitor: Centralized Management of CURWB Infrastructure

FM Monitor is a network-wide, on-premises monitoring dashboard that allows any CURWB customer to proactively maintain and monitor one or more wireless OT networks. FM-Monitor displays data and situational alerts from every CURWB device in a network in real time.

FM Monitor supports fixed and roaming network architectures and allows easy end-to-end troubleshooting. It can be operated as a standalone system or in parallel with a sitewide simple network management protocol (SNMP) monitoring tool. It is designed to support network installations used in wind farms, smart cities, rail, mining, renewables, ports and terminals, entertainment, smart factories, and military applications.

Note: This document does not provide setup or configuration instructions for FM Monitor. For this information, see *Cisco Ultra-Reliable Wireless Backhaul FM Monitor Configuration Manual*:

https://www.cisco.com/c/dam/en/us/td/docs/wireless/ultra-reliable-wireless-backhaul/device-software/cisco-urwb-fm-monitor-datasheet.pdf

FM Monitor provides the following features and benefits:

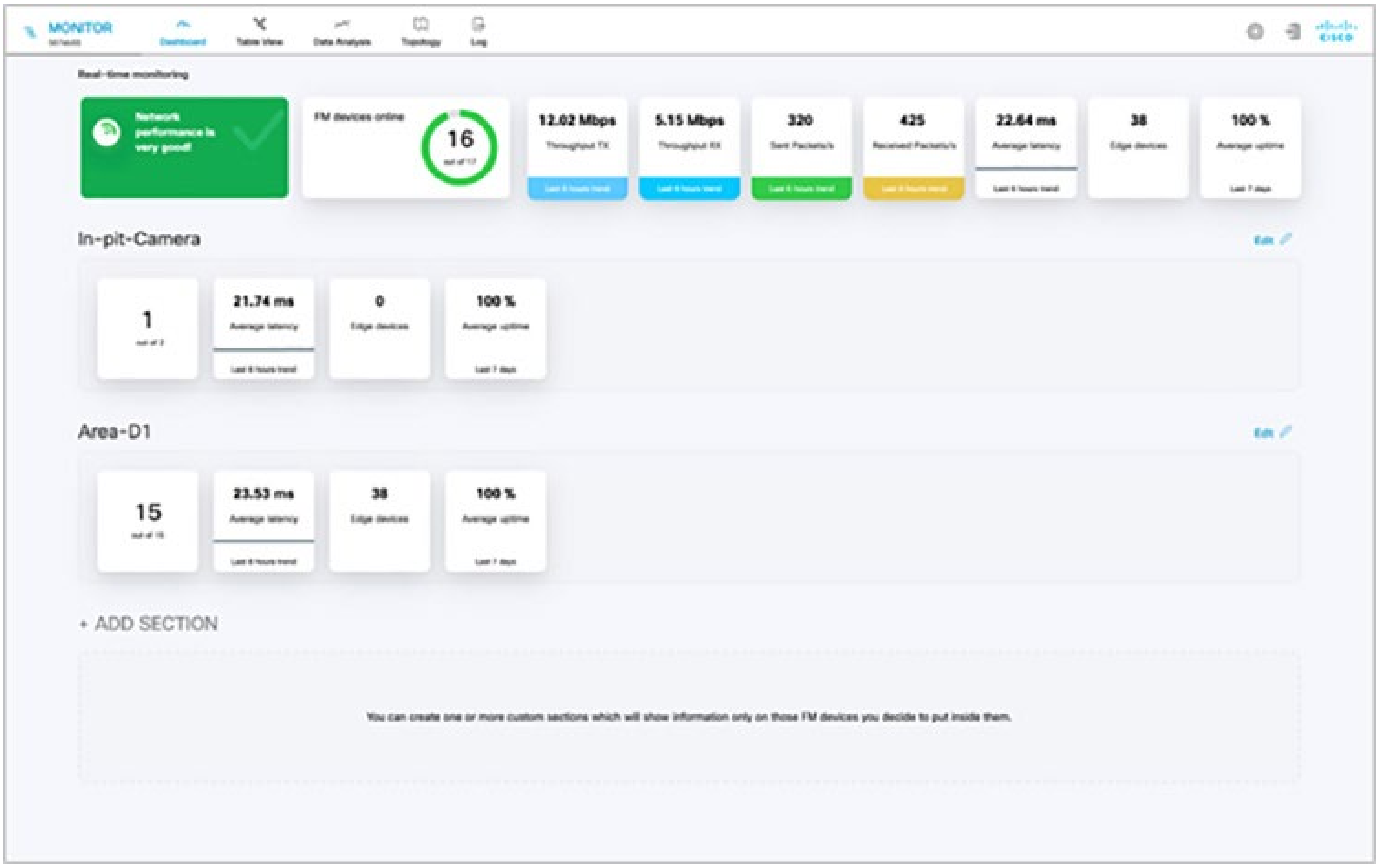
- On-premises monitoring for CURWB networks
- Wizard setup for quick and easy installation and deployment
- Real-time dashboard displaying uptime, throughput, latency, jitter, and other network KPIs
- Customizable section view to easily check groups of radios
- Customizable monitoring alerts for prompt response
- Radio-by-radio data logging with a minimum sampling interval of 300 ms
- Real-time radio configuration display for quick and accurate troubleshooting
- Side-by-side comparison of radio KPIs over time and over vehicle position
- Data logging export to a syslog server

One of the biggest advantages of FM 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.

FM Monitor Dashboard

The FM Monitor dashboard shows overall network performance and allows customizable segmentation of the network into clusters. This segmentation provides easy monitoring of network sections or parts of a fleet of vehicles, maximizing network usage and performance. Clusters can include backhaul point-to-point links, point-to-multipoint distribution networks, vehicle access networks, wayside networks, and vehicle-mounted radios. FM Monitor displays and tracks real-time KPIs within each cluster, including the number of active radios, number of connected IP edge devices, end-to-end latency, jitter, upload and download throughput in real time, and system uptime.

Figure 4-28 FM Monitor Dashboard

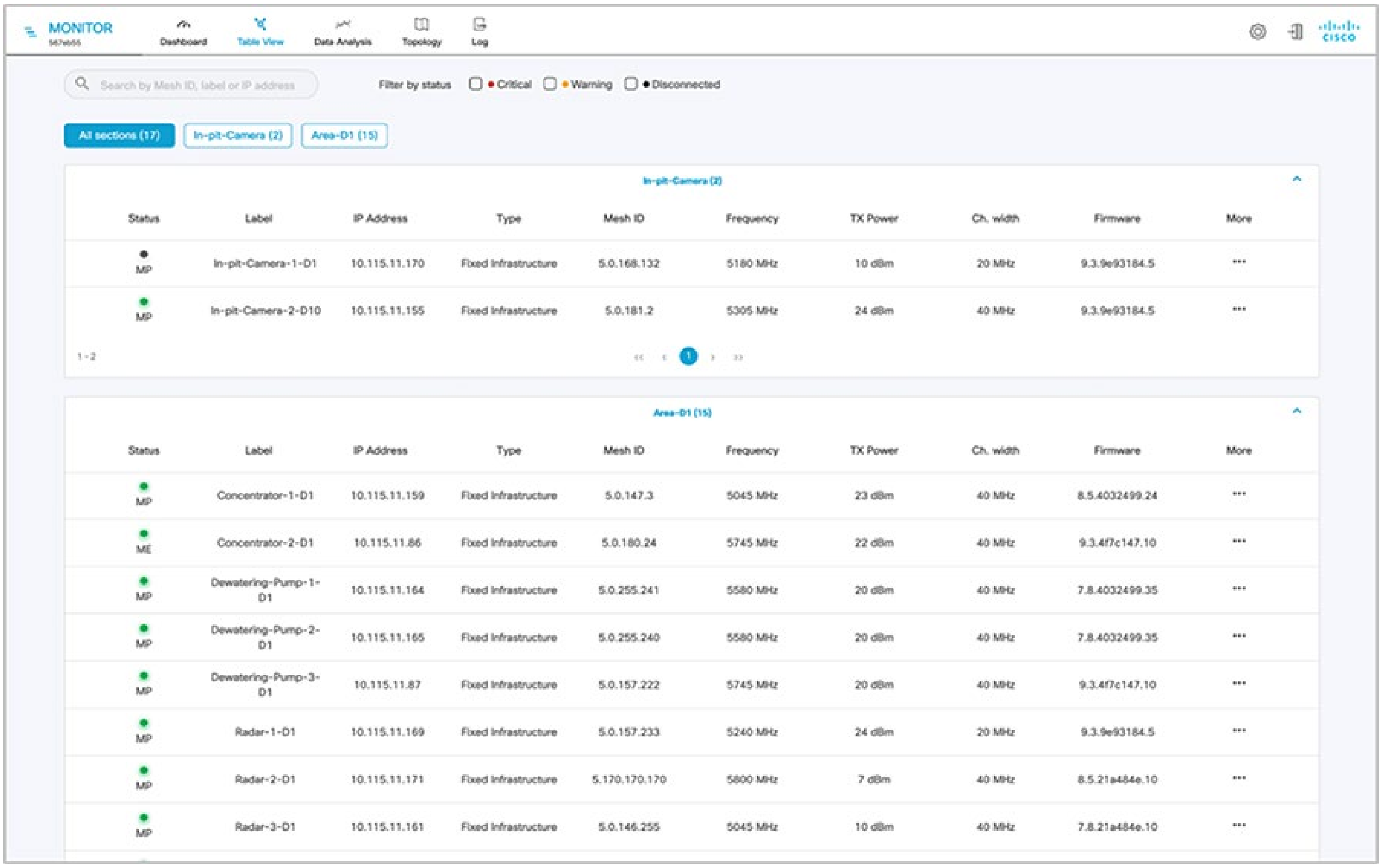


You can create one or more custom sections which will show information only on those FM devices you decide to put inside them.

FM Monitor Table View

The FM Monitor table view allows you to condense sections of the network into a tabular view, isolating specific radio configurations and performance statistics. During troubleshooting, this approach significantly reduces the time needed to understand system performance on a radio-by-radio basis.

Figure 4-29 FM Monitor Table View



In-pit-Camera (2)

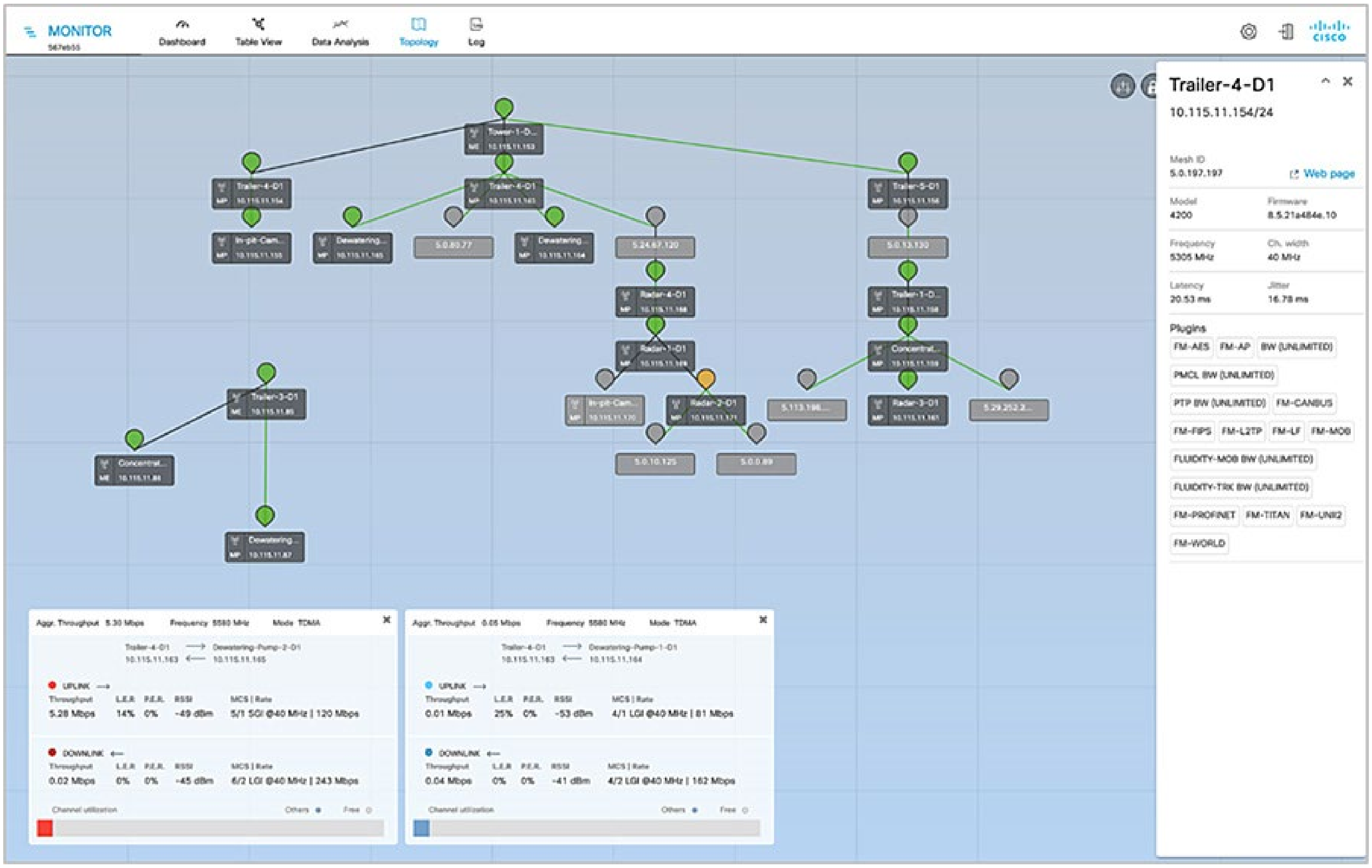
Status	Label	IP Address	Type	Mesh ID	Frequency	TX Power	Ch. width	Firmware	More
● MP	In-pit-Camera-1-D1	10.115.11.170	Fixed Infrastructure	5.0.168.132	5180 MHz	10 dBm	20 MHz	9.3.9e93184.5	•••
● MP	In-pit-Camera-2-D10	10.115.11.155	Fixed Infrastructure	5.0.181.2	5305 MHz	24 dBm	40 MHz	9.3.9e93184.5	•••

1 - 2

Area-D1 (15)

Status	Label	IP Address	Type	Mesh ID	Frequency	TX Power	Ch. width	Firmware	More
● MP	Concentrator-1-D1	10.115.11.159	Fixed Infrastructure	5.0.147.3	5045 MHz	23 dBm	40 MHz	8.5.4032499.24	•••
● ME	Concentrator-2-D1	10.115.11.86	Fixed Infrastructure	5.0.180.24	5745 MHz	22 dBm	40 MHz	9.3.4f7c147.10	•••
● MP	Dewatering-Pump-1-D1	10.115.11.164	Fixed Infrastructure	5.0.255.241	5580 MHz	20 dBm	40 MHz	7.8.4032499.35	•••
● MP	Dewatering-Pump-2-D1	10.115.11.165	Fixed Infrastructure	5.0.255.240	5580 MHz	20 dBm	40 MHz	7.8.4032499.35	•••
● MP	Dewatering-Pump-3-D1	10.115.11.87	Fixed Infrastructure	5.0.157.222	5745 MHz	20 dBm	40 MHz	9.3.4f7c147.10	•••
● MP	Radar-1-D1	10.115.11.169	Fixed Infrastructure	5.0.157.233	5240 MHz	24 dBm	20 MHz	9.3.9e93184.5	•••
● MP	Radar-2-D1	10.115.11.171	Fixed Infrastructure	5.170.170.170	5800 MHz	7 dBm	40 MHz	8.5.21a484e.10	•••
● MP	Radar-3-D1	10.115.11.161	Fixed Infrastructure	5.0.146.255	5045 MHz	10 dBm	40 MHz	7.8.21a484e.10	•••

Figure 4-30 FM-Monitor Topology View



Trailer-4-D1

10.115.11.154/24

Mesh ID
5.0.197.197

Web page

Model	Firmware
4200	8.5.21a484e.10

Frequency	Ch. width
5305 MHz	40 MHz

Latency	Jitter
20.53 ms	16.78 ms

Plugins

FM-AES FM-AP BW (UNLIMITED) PMCL BW (UNLIMITED) PTP BW (UNLIMITED) FM-CANBUS FM-FIPS FM-L2TP FM-LF FM-MOB FLUIDITY-MOB BW (UNLIMITED) FLUIDITY-TRK BW (UNLIMITED) FM-PROFINET FM-TITAN FM-UNI2 FM-WORLD

Aggr. Throughput 5.30 Mbps Frequency 5580 MHz Mode TDMA

Trailer-4-D1 ⟶ Dewatering-Pump-2-D1
10.115.11.163 ⟵ 10.115.11.165

● UPLINK ⟶

Throughput	L.E.R.	P.E.R.	RSSI	MCS | Rate
5.28 Mbps	14%	0%	-49 dBm	5/1 SGI @40 MHz | 120 Mbps

● DOWNLINK ⟵

Throughput	L.E.R.	P.E.R.	RSSI	MCS | Rate
0.02 Mbps	0%	0%	-45 dBm	6/2 LGI @40 MHz | 243 Mbps

Channel utilization Others ● Free ○

Aggr. Throughput 0.05 Mbps Frequency 5580 MHz Mode TDMA

Trailer-4-D1 ⟶ Dewatering-Pump-1-D1
10.115.11.163 ⟵ 10.115.11.164

● UPLINK ⟶

Throughput	L.E.R.	P.E.R.	RSSI	MCS | Rate
0.01 Mbps	25%	0%	-53 dBm	4/1 LGI @40 MHz | 81 Mbps

● DOWNLINK ⟵

Throughput	L.E.R.	P.E.R.	RSSI	MCS | Rate
0.04 Mbps	0%	0%	-41 dBm	4/2 LGI @40 MHz | 162 Mbps

Channel utilization Others ● Free ○

CURWB: Terminology and Miscellaneous Configurations

This section covers some concepts that are needed to understand the CURWB architecture and deployment.

Mesh ID

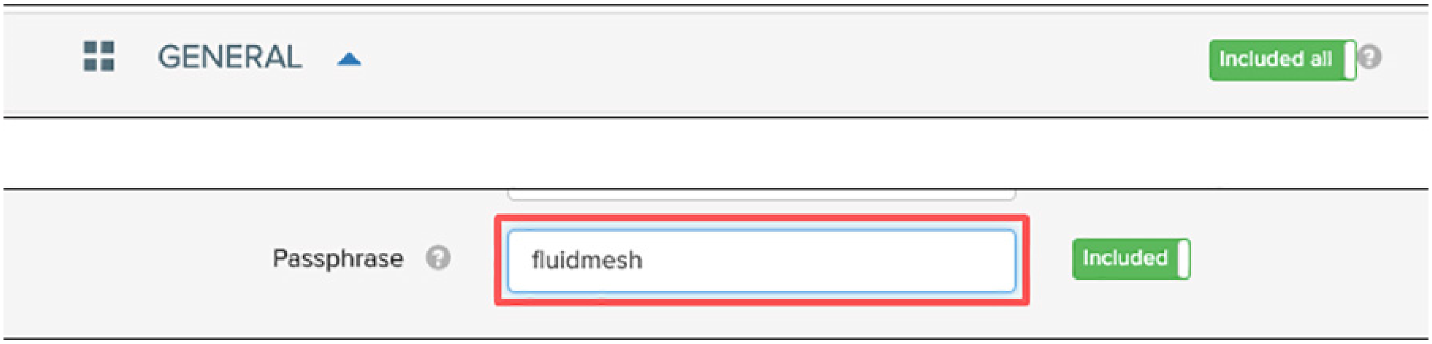
Figure 4-31 Mesh ID

The mesh ID is a hardware identifier for CURWB gateways and radios. It is preprogrammed at the factory with a hard-coded value that cannot be modified. The mesh ID is in the format of 5.x.x.x.

Note that a mesh ID is not an IP address. The mesh ID is relevant within the constructs of network design. A gateway or radio with a lower mesh ID becomes the “primary.” In addition, the gateway or radio with the lowest mesh ID becomes the mesh end (if a mesh end is not explicitly configured).

Passphrases

Figure 4-32 Passphrases



GENERAL

Included all

Passphrase: fluidmesh

Included

CURWB gateways and radios are configured with shared passphrases. CURWB control plane traffic is encrypted using this passphrase. The passphrase can also be used to segment a particular network so that radios with the same shared passphrase form a cluster and are kept separate from other mesh networks which use a different passphrase.

Note: Data plane and user traffic is not encrypted using the passphrase. To encrypt data-plan and user traffic, AES encryption must be enabled on gateways and radios.

Note: If a shared passphrase is defined, the same passphrase must be used for all Fluidmesh units in the same network. As a deployment best practice, configure the passphrase to be something other than the default value of “Fluidmesh.” The shared passphrase can be composed of any ASCII characters except the following: ' ` " \ $ =

MTU Considerations

- Similar considerations as for normal MPLS
- MTU at endpoint 1500
- The minimum required MTU on switches is 1544
- Radios don't have to be configured manually with MTU, this configuration is done automatically

Spanning Tree Protocol

Spanning tree protocol (STP) is a layer 2 protocol that runs on switches to prevent loops in the network when there are redundant paths in the network. Switches run the STP algorithm when they are first connected to a network or whenever there is a topology change. CURWB radios do not participate in the STP alongside the switches. The radios simply forward or block BPDU messages, depending on how the radios are configured. CURWB radios have an equivalent process to STP, called AutoTap, which helps avoid any loops within the wireless network.

BPDU snooping can be enabled or disabled on a radio. According to the configuration the radio acts or does not act on the contents of the BPDU.

BPDU forwarding, when configured as **Pass**, forwards all the BPDUs. BPDU forwarding, when configured as **Auto**, forwards the BPDUs within the wayside space and does not forward BPDUs to the vehicle space. Similarly in the **Auto** mode, BPDUs are not forwarded from the vehicle space to the wayside space. When BPDU forwarding is configured as **Stop**, no BPDUs are forwarded.

AutoTap

AutoTap is a network loop prevention mechanism that allows CURWB radios to detect connections and allow only a dedicated ingress or egress route to and from the mesh end or network core.

When AutoTap is enabled, only one radio in the physically connected redundant radio group advertises MAC address information. This radio is known as the primary radio, and is the radio with the lowest mesh ID. In this way, radios can detect each other over a wired connection and forward traffic to other connected radios utilizing the wired connection. Routes to the core and end devices are built automatically. The result is like having a single radio with multiple wireless interfaces.

Network Time Protocol

As a best practice, network time protocol (NTP) should be configured on CURWB radios. A primary and secondary NTP server IP address can be configured. When NTP is enabled on a radio, the radio synchronizes its time with the NTP server, usually within an hour. However you can force this synchronization to happen sooner. The radio's network connectivity goes down for milliseconds when you force it to connect to the NTP server.

VLAN Design

Table 4-3 lists the VLANs and their purposes in a typical CURWB deployment.

Figure 4-3 VLAN Segmentation

VLAN	Purpose
VLAN-X	CURWB management VLAN. Used to connect, configure, and manage the CURWB devices. Also used for control plane communication between the radio units. Every CURWB device needs to have an IP address in this subnet for management reachability.
VLAN-Y	Client traffic VLAN. Each client device, for example on board cameras, sensors, VCUs, and so on, have an IP address within this subnet. Multiple client VLANs can be used based on segmentation requirements.
VLAN-Z	CURWB native VLAN. This VLAN should not be used on the wired network. For example, a dummy value such as '999' can be used. Note that when the CURWB native VLAN is configured with a value of '0' all untagged traffic will be dropped.
VLAN-A	Switch management VLAN. Each LAN switch should have an IP address from this subnet for management reachability. Used to connect, configure, and manage the switches within the deployment.

On CURWB radios, VLAN support is not enabled by default and can be enabled by installing an optional plugin. We recommend that you Install and enable the VLAN plugin to control how tagged and untagged traffic is propagated through the network. When the plugin is enabled, two VLANs are configurable, one for management of radio units and one for the CURWB native VLAN. The CURWB management VLAN is used for control plane communication between the radios and to connect, configure, and manage CURWB devices. The native VLAN determines how untagged traffic is handled as it passes through a radio. Setting the native VLAN to 0 is a special case that causes all untagged traffic to be dropped and allows only tagged traffic to pass through the radio.

The switch interface that is connected to a CURWB radio should be configured as a trunk port carrying the CURWB management VLAN and the client traffic VLAN or VLANs. Note that the CURWB radio does not have the capability to tag VLANs, so VLAN tagging should be done on the directly connected switch.

CURWB Mesh End

A logical mesh end can be redundant and consist of two physical mesh end gateways or radios with the TITAN high-availability plug-in. The mesh end typically is configured within the core network. The purpose of an ME radio is to terminate all MPLS label switched paths (LPSs) and to act as a gateway between the CURWB network and the wired network. The mesh end stores all LSPs to all the other radios in its database.

Note: Even though the CURWB solution has the capability to automatically select a gateway or radio with the lowest mesh ID to become the ME, as a best practice we recommend that you configure the role of ME and mesh points manually within the deployment to have more deterministic convergence in case of a failure within the network.

Note: By default, a full mesh of LSPs is created. However, within an offshore wind farm deployment, a full mesh of LSPs from each radio to each of the other radios within the network is not needed. LSPs are needed only from each mesh point to the mesh ends. This configuration is made with the **Pseudo wires set** parameter within RACER. Change this parameter from the default setting of **All** to **Mesh-Ends only**.

CURWB Mobility Architecture: Layer 2 Fluidity

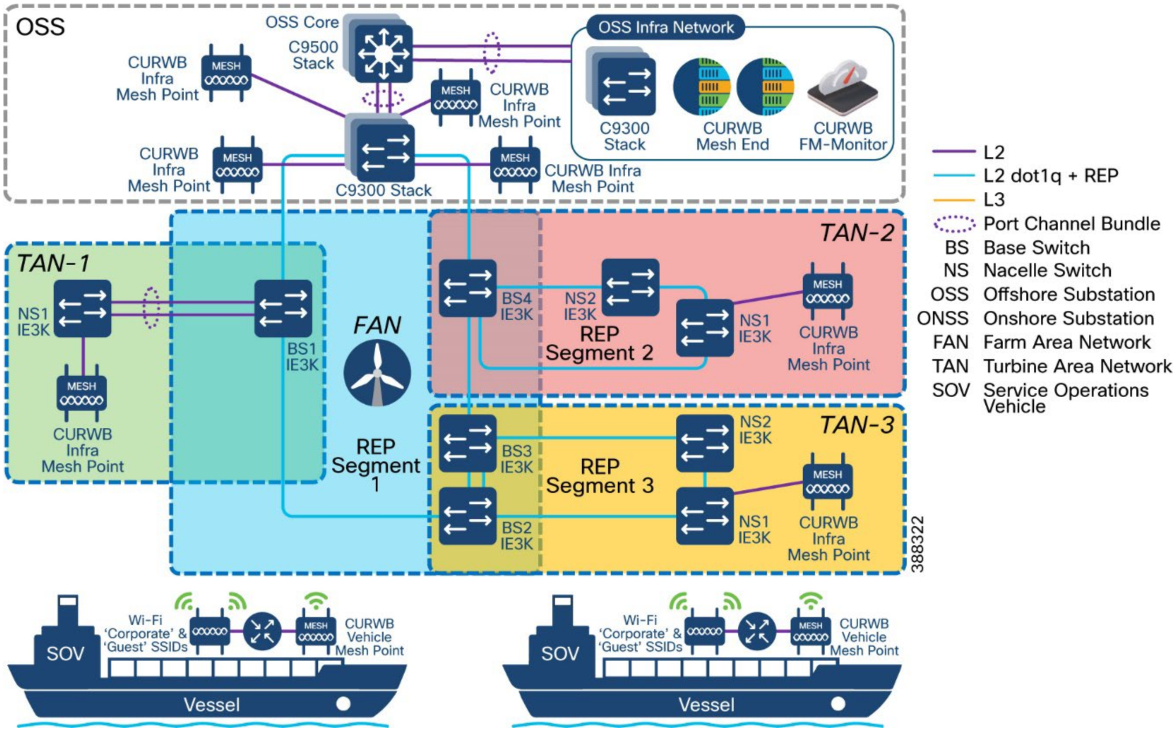
Figure 4-33 depicts a typical CURWB layer 2 fluidity mobility architecture for offshore wind farm SOV to OSS connectivity. A prerequisite for layer 2 fluidity is that all the CURWB devices (mesh end gateways, access radios and mobile radios) must be within the same VLAN, IP subnet, and layer 2 broadcast domain and configured with the same passphrase.

The OSS infrastructure network consists of a redundant pair of mesh end gateways. The role of the mesh ends is to terminate the MPLS tunnels from each of the SOV radios and act as demarcation points between the wired and the wireless domains. The mesh ends are responsible for de-encapsulating the MPLS header and then forwarding the traffic to the distribution or core switch. For the traffic originating from the wired network and going toward the mobility domain, mesh ends act as default gateways and are responsible for the MPLS encapsulation and forwarding traffic to the appropriate SOV radio.

Access radios are configured as mesh points in the layer 2 fluidity mode with same passphrase that is configured on the mesh ends. The role of the access radios is to provide RF coverage for the mobility domain. Access radios are distributed across the area where wireless coverage is required while the SOVs roam. For small to medium offshore wind farms, the four URWB radios on the OSS might provide sufficient RF coverage for the SOVs. For larger offshore wind farms, URWB radios might need to be deployed on some of the turbines to address any RF coverage gaps. In this design, all access radios are configured to operate on the same frequency, which is known as a single frequency design.

Radios on the SOVs are configured in **Vehicle** mode and are statically configured to use the same frequency that is used on infrastructure radios.

Figure 4-33 CURWB L2 Fluidity Deployment for SOV to OSS Connectivity



The network architecture is based on Prodigy 2.0, an MPLS-based technology, which is used to deliver IP-encapsulated data. MPLS provides an end-to-end packet delivery service that operates between levels 2 and 3 of the OSI network stack. It relies on label identifiers, rather than on the network destination address as with traditional IP routing, to determine the sequence of nodes to be traversed to reach the end of the path. An MPLS-enabled device is also called a label switched router (LSR). A sequence of LSR nodes configured to deliver packets from the ingress to the egress using label switching is called a label switched path (LSP), or tunnel. LSRs that are situated on the border of an MPLS-enabled network and other traditional IP-based devices are called label edge routers (LER).

The ingress node of the path classifies incoming packet according to a set of forwarding equivalence classes (FEC). When a packet matches a class, the packet is marked with the label that is associated with a particular class and then forwarded to the next node of the sequence, according to information that is configured in the forwarding information table (FIB) of the node. Subsequently, each intermediate node manipulates the MPLS labels that are stored in the packet and then forwards the data to the next node. The egress node finally removes the label and handles the packet using normal IP routing functions.

The FIBs on the different nodes of a network are managed by the label distribution protocol (LDP). which is the primary component of the network control plane. Fluidity relies on a custom LDP that provides automated installation of LSPs in the different nodes of the network. This approach ensures that each node can be reached from any other node.

In traditional MPLS networks, whenever the network topology changes, the FIBs of the nodes that are involved must be reconfigured to adapt to the new paths. This reconfiguration usually is performed using the standard LDP signaling that is available.

In a mobility network, the handoff process can be assimilated into a network topology change, where a link is broken and a new one created, as with Wi-Fi. However, the standard mechanisms to detect a change and reconfigure the nodes are too slow and data-intensive to provide adequate performance in a real-time constrained scenario, such as high-speed mobility. In particular, the reconfiguration latency and the number of messages exchanged should be minimized to reduce the chances that some data packets are lost in the process.

To mitigate these issues, fluidity implements a fast handoff solution that is able to provide very fast path reconfiguration with latency in the order of one millisecond. The fast handoff mechanism is an extension to the existing control plane of the network and is based on a specific manipulation technique concerning the MPLS FIB tables of the nodes.

The scheme proposed allows mobile nodes, and client devices that are attached to them to maintain their IP addresses throughout the mobility process. All nodes are part of a single layer 2 mesh network. The layer 3 handoff process is seamless in the sense that, because of a make-before-break strategy, the availability of at least one valid LSP is ensured during the transitory handoff as the network is reconfigured.

LSPs connecting to the static backbone are installed and updated whenever a vehicle performs the handoff procedure using dedicated signaling. LSPs are always present as long as a mobile radio is communicating with a fixed infrastructure radio, although labels change as a vehicle roams.

Fluidity Rate Adaptation

The fluidity rate adaptation setting controls a unit's choice of modulation coding and speed of packet transmission. Fluidity supports the following rate adaptation modes:

- Standard: Applies a standard reactive rate selection as used by Wi-Fi access points
- Advanced: Applies the CURWB proprietary predictive rate selection algorithm

For offshore wind farm SOV to OSS connectivity, we recommend the advanced rate adaptation. The CURWB predictive rate selection algorithm is proactive. When the link error rate (LER) increases, there is no packet drop because the LER is kept low by predictively adjusting the data rate. The predictive algorithm tries to keep the LER and packet loss low by selecting a more conservative data rate. The standard rate selection algorithm would need higher LER and packet drops to adjust to a lower data rate. Rate selection also is important for obtaining good performance and maximizing the throughput of a radio communication system.

The RSSI prediction is performed by the transmitting radio using explicit feedback that it receives from the destination radios. This prediction provides a good estimate of the upstream channel condition. For further accuracy, the system also filters out instantaneous variations that may have a detrimental effect on the choice of the transmission rate.

The transmission rate is then selected according to the prediction of the estimated RSSI, drawing from a small set of optimal rates that are computed by a heuristic channel estimation algorithm. Within high-speed mobility environments, the channel state changes quickly. Therefore, it is important that the rate sampling algorithm finds the optimal rates in the shortest time possible while keeping accuracy. Failure to meet either condition typically results in low throughput, high latency, and a high packet error rate (PER).

When the rate adaptation is set to Advanced, a vehicle radio bases the selection of MCS based on the RSSI that it receives from a wayside infrastructure radio. The RSSI scale is divided into a number of non-overlapping bins, and each bin corresponds to a subset of MCS values to be sampled by the rate selection algorithm. The RSSI bin definitions and their associated MCS subsets can be determined according to several criteria, which may include, for example, the sensitivity thresholds of the underlying wireless hardware. Table 4-4 shows the default values for the RSSI bins and the corresponding MCS rate that is selected.

Table 4-4 MICS Rate Selection Based on RSSI Bins Default Values

Default RSSI Bins	MCS Rate (20 MHz Wide Channel)	
	Minimum	Maximum
–95 through –77	0	2
–77 through –71	1	3
–71 through –67	2	4
–67 through –59	3	5
–59 through –49	4	7
–49 or above	5	7

Fluidity Handoff Logic

Within standard Wi-Fi based communication, a handoff is triggered by the Wi-Fi client based on preconfigured static thresholds such as RSSI and SNR. For example, a Wi-Fi client might be configured to trigger a handoff when its RSSI value drops below –75 dBm. CURWB, on the other hand, uses a dynamic handoff decision algorithm.

As shown in Figure 4-34, a vehicle radio always operates on the top line (RSSI envelope), handing over from the currently connected radio to the next available radio as soon as the difference in RSSI meets the configured hysteresis threshold. Figure 4-35 shows the fluidity predictive rate selection and the location where the fluidity handoff occurs.

Figure 4-34 Fluidity Dynamic Handoff Decision

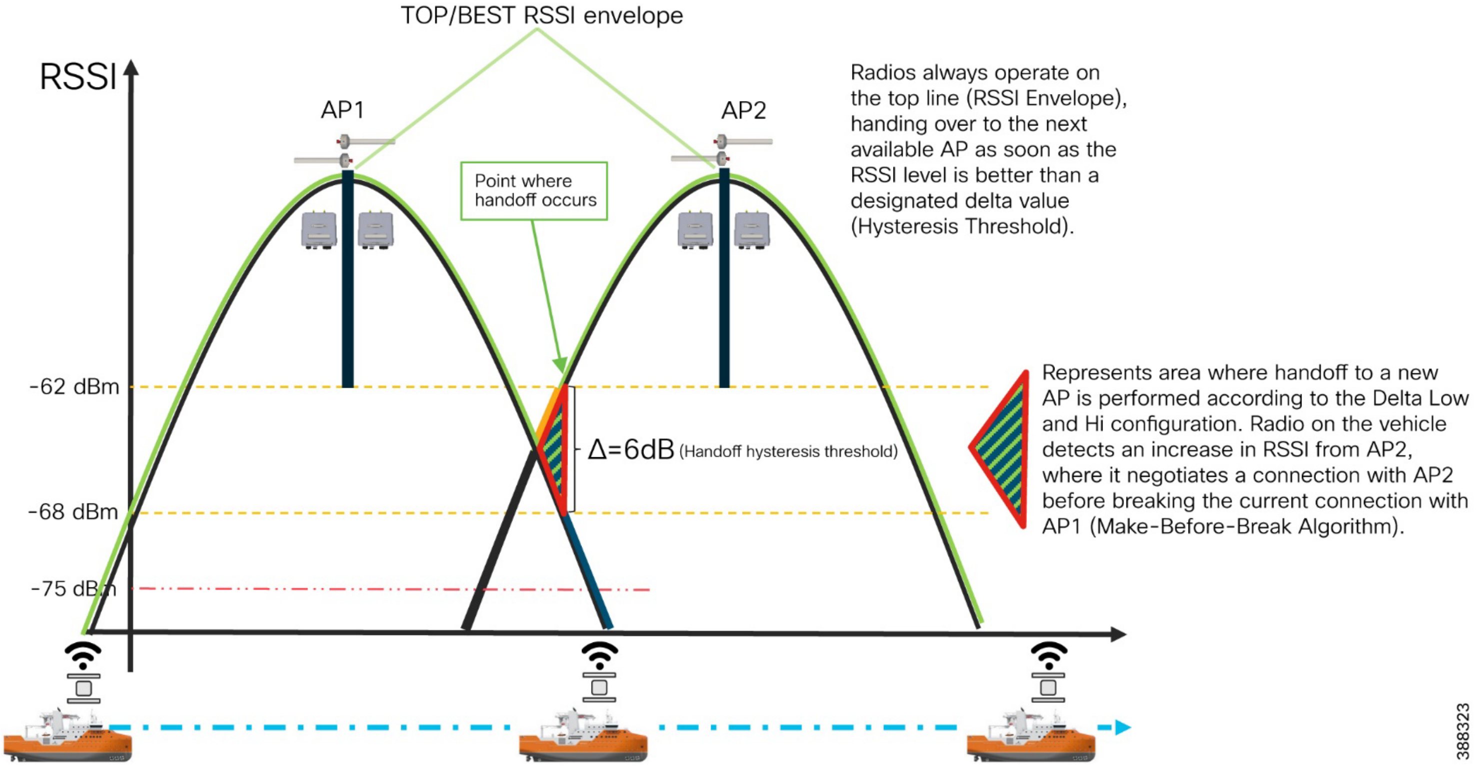
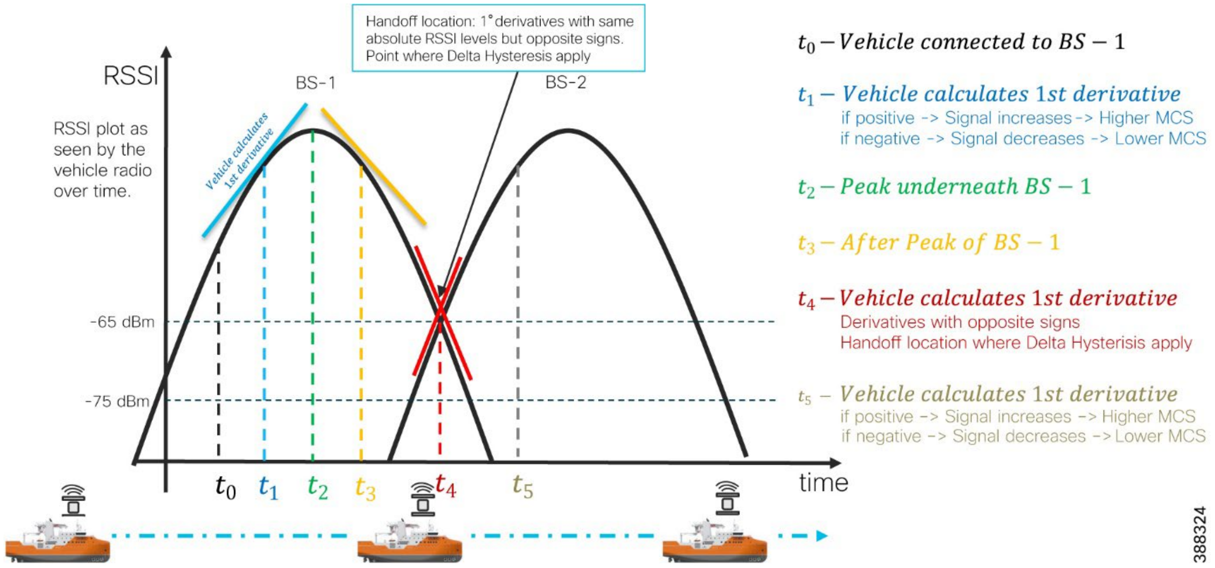


Figure 4-35 Fluidity Predictive Rate Selection and Handoff Location



Fluidity Advanced Handoff Tuning for SOV Radios

The CURWB solution provides certain advanced handoff parameters for vehicle radios that can be tuned depending on the RF environment to achieve optimal handoffs.

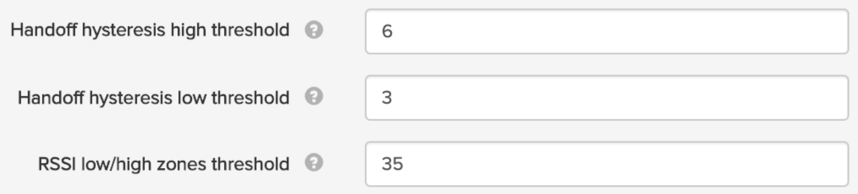
The RSSI zone threshold and handoff hysteresis threshold features provide safeguards against unwanted handoffs, that is, against unreasonably long periods between the received signal strength from a connected radio falling too low and a handoff request from a relief unit.

The relationship between the three settings that are shown in Figure 4-36 governs whether a handoff takes place from one unit to another, based on a difference in comparative signal amplitude values over a period.

The RSSI low/high zone threshold sets the border between the low and high RSSI zones. In this case, as represented by the two graphs that are shown in Figure 4-37 and Figure 4-38, the –60 dB level marks the border between the low and high RSSI zones.

The threshold value is always expressed as SNR, with –95 dBm as the reference value, and is always expressed as a value greater than 0. The default value is 35. This value equates to –60 dBm.

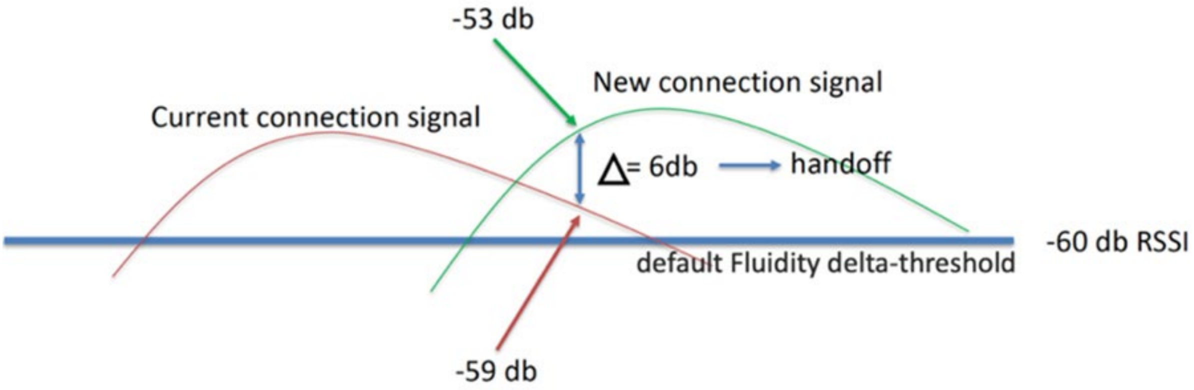
Figure 4-36 RACER Fluidity Advanced Handoff Parameters



Handoff hysteresis high threshold	6
Handoff hysteresis low threshold	3
RSSI low/high zones threshold	35

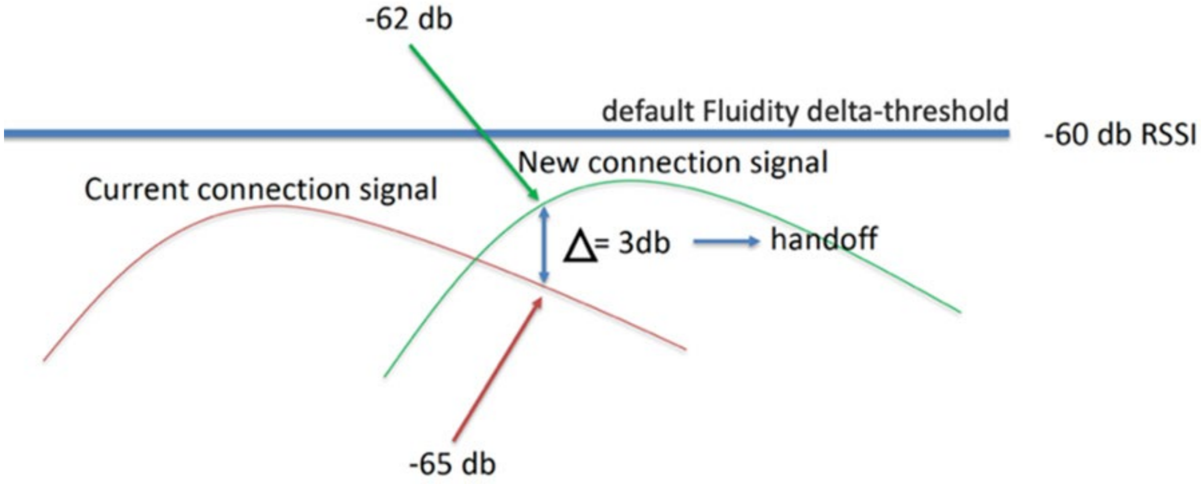
As shown in Figure 4-37, the default fluidity delta-threshold is –60 dBm. The default delta-high threshold is 6 dBm. With these settings, in good RF environments where the signal strength is higher than –60 dBm, the vehicle radio attempts a handoff to another wayside infrastructure radio only if the wayside radio provides a signal that is at least 6 dBm higher than what the vehicle is receiving from its currently connected wayside infrastructure radio. If the delta value is lower than 6, no handoff occurs at that time.

Figure 4-37 Fluidity Delta-High Example



As shown in Figure 4-38, the default delta-low threshold is 3 dBm. With this setting, in poor RF environments where the signal strength is lower than –60 dBm, the vehicle radio attempts a handoff to another wayside infrastructure radio if the wayside radio provides a signal that is at least 3 dBm higher than what it is receiving from its currently connected wayside infrastructure radio. If the delta value is lower than 3, no handoff occurs at that time.

Figure 4-38 Fluidity Delta-Low Example



Note: The Fluidity delta-threshold, the delta-high value, and the delta-low value are all configurable by using either RACER or the radio CLI, if needed for your RF environment tuning.

CURWB Fluidity Advanced: Large Network Optimization

Large network optimization (LNO) is useful in large network environments of more than 50 infrastructure radios. LNO helps optimize the MPLS forwarding table by establishing LSPs only toward the mesh end units.

The mesh end is the ingress or egress point of the MPLS domain. Spanning tree protocol (STP) also is affected because BPDU forwarding is disabled.

If LNO is enabled, the mesh points establish LSPs only with other mesh end devices. Enabling LNO also disables STP packet and BPDU forwarding.

If LNO is disabled, LSPs are created between all mesh points, and between mesh points and mesh ends. STP packets and BPDU forwarding are set to Automatic.

For an offshore wind farm deployment, we recommended that the LNO feature be disabled.

Note: If enabled, the LNO feature overrides the pseudo-wires configuration within MPLS settings.

SOV Mobility Network

Figure 4-39 SOV Mobility Network

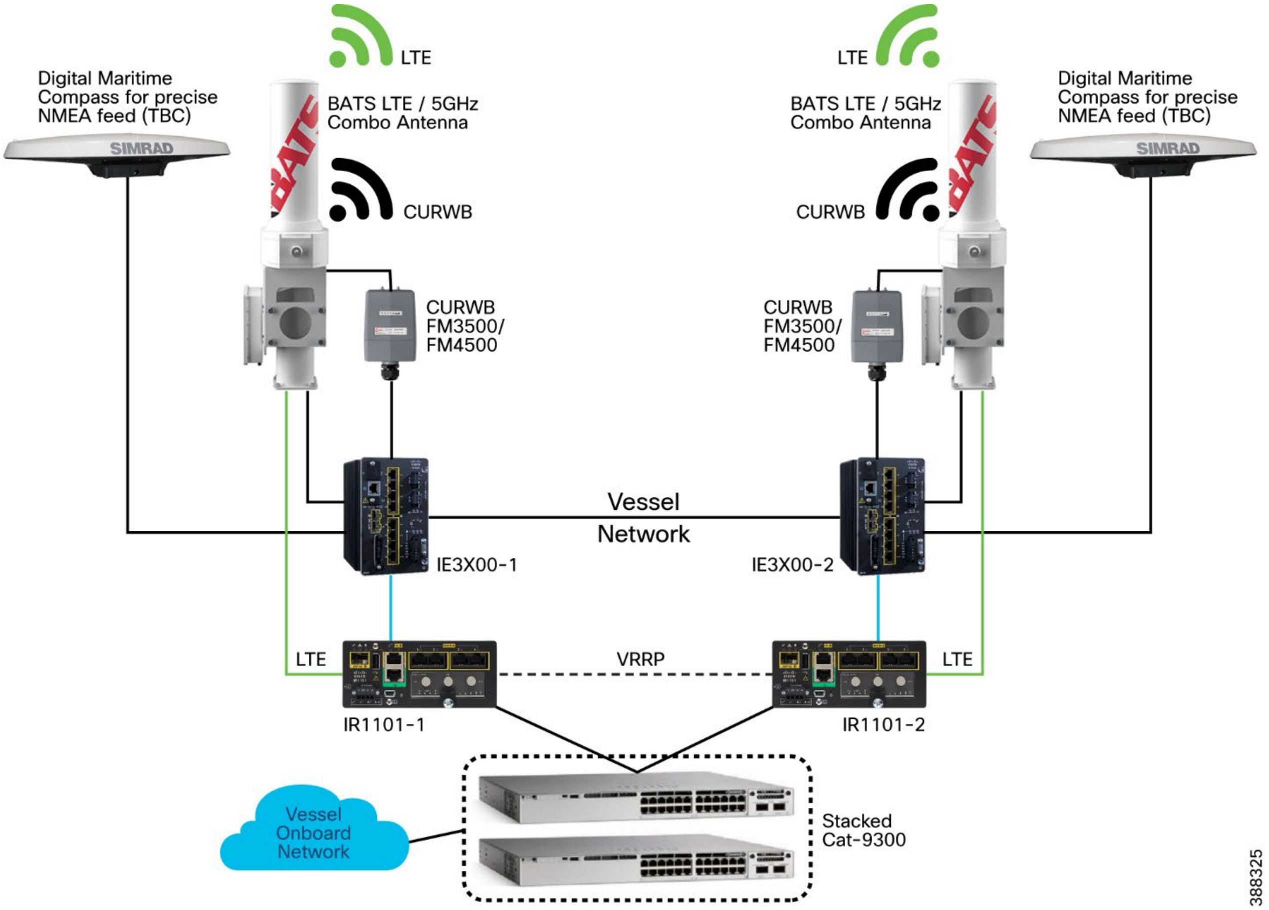


Figure 4-39 shows the SOV onboard network. The onboard Wi-Fi network (WLC and APs), wired ports, servers, and IP phones are connected to a stacked pair of Cisco Catalyst 9300 switches. The Cisco Catalyst 9300 stack is then connected to a pair of Cisco IR1101 routers with 5G and 4G-LTE SIMs that provide cellular connectivity when an SOV is close to shore and within range of a cellular tower.

When the SOV is farther out in the ocean, it uses satellite connectivity, which is out of scope of this CVD.

When an SOV is in range of the CURWB network on the OSSs and turbines, the SOV switches to using dual FM4500 radios that are connected to BATS antennas to communicate with the OSS network, which has connectivity back to the control room and internet.

A BATS antenna that is deployed on an SOV serves two purposes. One port of the antenna is connected to a Cisco IR1101 router to provide 5G and 4G-LTE connectivity via a cellular network. The second port is connected to a CURWB FM4500 radio to provide connectivity to the OSS CURWB network.

VRRP is configured between two Cisco IR1101 routers to provide layer 3 redundancy.

The two CURWB radios on an SOV are configured with the same passphrase and configured to operate in the **Vehicle** mode. Assign the unit a vehicle identity by using either of the following methods. For more information about performing this configuration, see the Implementation Guide.

- Allow the unit to automatically generate a unique vehicle identity by checking the **Enable** check box to the right of the **Automatic Vehicle ID**: heading.
- Assign a vehicle identity manually by unchecking the **Enable** check box to the right of the **Automatic Vehicle ID:** heading, and manually enter an identification string in the **Vehicle ID:** field.

Note: If vehicle identities have been manually assigned, the **Vehicle ID** string must be unique for each Fluidmesh unit that operates on the same network, even if more than one Fluidmesh unit is installed on the same vehicle.

The CURWB network type must be configured as **Flat**' because it uses the layer 2 fluidity deployment model. The SOV CURWB radios must have a management IP address in the same subnet as the CURWB infrastructure APs on the OSS and TAN.

The **Handoff Logic** setting controls the unit's choice of the infrastructure point with which to connect. For the SOV radios, configure this setting to the **Standard** handoff, which entails the SOV CURWB radio unit connects to the infrastructure CURWB radio that provides the strongest signal.

The **Rate Adaptation** setting controls the unit's choice of modulation coding and speed of packet transmission. For the SOV CURWB radios, configure this setting to **Advanced Rate Adaptation**, which uses the CURWB proprietary predictive rate selection algorithm.

The SOV network should be in a layer 2 ring to maximize traffic efficiency and minimize outages.

- CURWB management VLAN should be present on all nodes.
- The Cisco IE3X00 should be designated as the STP root to minimize traffic hairpinning.
- Layer 3 SVIs should be configured on the Cisco IR1101 for the client gateway.
- VRRP should be configured on the Cisco IR1101s to load-balance different client subnets.
- Dynamic routing protocol should be used between SOVs and OSS to automatically choose the WAN interface.
- BATS specific (applicable only if using BATS antennas on the SOV):
- Configure the BATS antennas for GPS only tracking mode (dummy radio).
- RSSI mode requires constant telemetry from the attached radio. CURWB radios send only telemetry when they are in the in **primary** role. In the **secondary** role, the radios send no telemetry. Therefore, the RSSI mode cannot be used effectively.

High-Availability

This section covers the high availability design for the CURWB deployment.

TITAN High Availability Plug-in

For faster convergence, we recommend that the Titan high availability plugin be installed on all radios in a wind farm deployment.

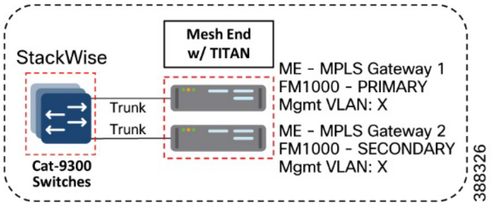
Gratuitous ARP

Enable gratuitous APR (GARP) when enabling the Titan HA plugin to advertise the secondary radios MAC address if the primary radio fails.

CURWB Mesh End Redundancy

This section covers the URWB FM1000 Mesh-End redundancy and high-availability design.

Figure 4-40 Redundancy and High-Availability at the OSS Infra Layer



FM1000 Mesh End Redundancy and Titan High Availability

We recommend that you apply the TITAN high availability plugins for a pair of redundant FM-1000 mesh ends in the wind farm deployment.

After Titan is configured, it is completely autonomous and ensures stable and reliable connectivity without the need for any human intervention. If data exchange ceases because of the failure of the primary mesh end device, Titan detects the failure and reroutes traffic through the designated secondary device, reestablishing connectivity within a maximum of 500 ms. When the failed primary mesh end device comes back online, the secondary mesh end device automatically reverts to its standby role.

We recommend that you connect the FM1000 gateways to separate power sources and to different switches within the 9500 StackWise pair. This arrangement provides protection against power outages and switch hardware failure.

Primary Election

All CURWB units that are connected to the same wired broadcast domain and configured with the same passphrase perform a distributed primary election process every few seconds. The primary unit is an edge point of the Fluidmesh MPLS network, that is, a device where user traffic may enter or leave the mesh. Secondary units act as MPLS relay points.

For each neighbor, the algorithm computes a precedence value based on the role of the unit (mesh end or mesh point) and its mesh ID. Mesh ends are assigned a higher priority than mesh points and, among the same priority, the unit with the lowest mesh ID is preferred. The election mechanism relies on a dedicated signaling protocol that constantly runs in the network and guarantees that all units elect the same primary unit.

Mesh End Failover

During normal operation, the primary and secondary mesh ends constantly communicate to inform each other about their statuses and to exchange network reachability information. In particular, the primary mesh end periodically sends updates to the secondary mesh end regarding its internal forwarding table and multicast routes.

Primary Mesh End Failure

If the primary mesh end fails for any reason, the secondary mesh end times out after not receiving keepalive messages for a configurable interval, which typically is from 50 through 200 ms. At that point, the secondary mesh end becomes the new active mesh- end, taking over the role of primary mesh end, and it executes the following actions:

- Issues a primary change command to inform all other units on the same wired network that the primary has changed. The message also is propagated to mobile units by using an efficient distribution protocol.
- Updates the internal MAC and MPLS forwarding tables. This step is performed using a proprietary fast rerouting technique that provides seamless performance.
- Sends gratuitous ARPs for the onboard devices on its ethernet or fiber port. This action forces the network switch to update its MAC forwarding table (CAM table) so that it sends traffic for onboard destinations through the port that is connected to the new primary.

When the other units receive the primary change command from the secondary, they perform the internal seamless fast-rerouting procedure so that the traffic can immediately be forwarded with no additional delay or signaling required. This approach provides fast network reconvergence, with an effective end-to-end service disruption below 500 ms.

Primary Mesh-End Recovery

When the primary mesh end is recovered, it scans the network for the presence of an active secondary mesh end. If the detection is positive, the unit enters an inhibition mode wherein the secondary mesh end remains the current edge point of the infrastructure for a certain amount of time (70 seconds, by default). During this grace period, the primary unit receives updates from the currently active secondary mesh end and acquires full knowledge about the state of the network. Then, the secondary unit switches to being the primary unit, using the same procedure that is described above for failure.

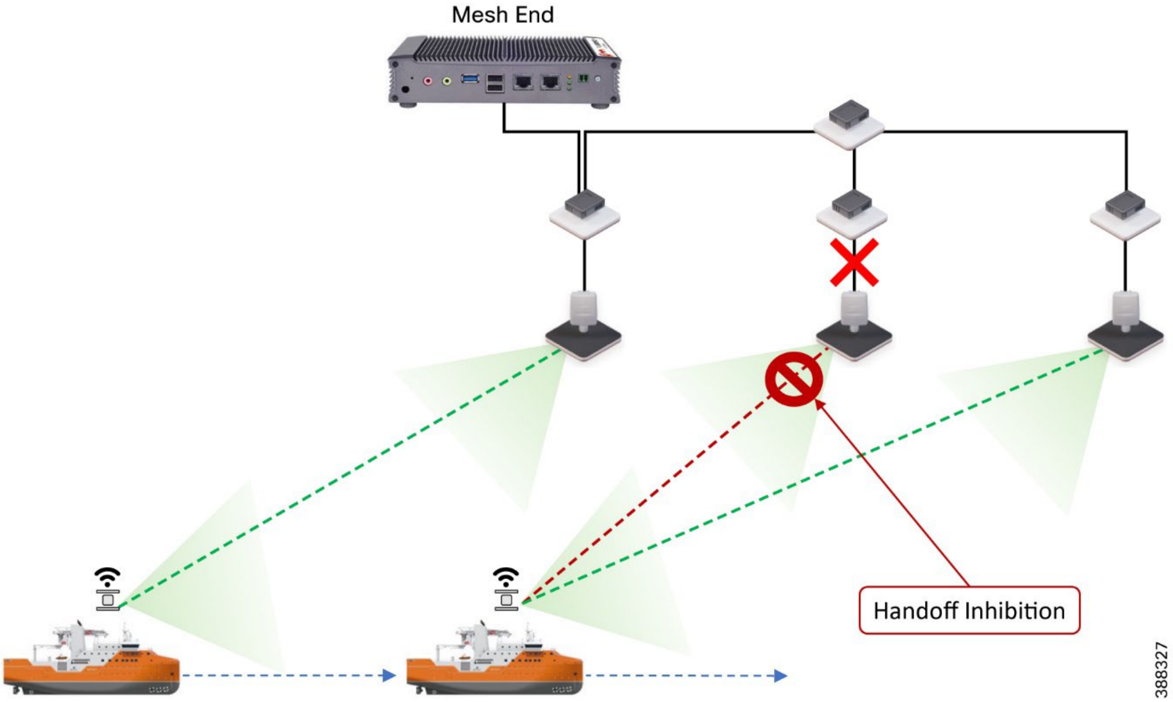
CURWB Access Layer: Fast Convergence on Failure

Link Backhaul Check: Handoff Inhibition

Using the link backhaul check feature, an access radio detects a carrier loss on its Ethernet or fiber port. With a carrier loss, an access radio unit loses its ability to deliver mobility traffic to the mesh end. The radio immediately advertises its status as Unavailable by transmitting a **handoff inhibition** message over the wireless channel. Upon receiving the **handoff inhibition** message, any existing mobile radio that is connected to the affected radio searches for another access radio to connect to. All mobile radios that are currently connected to affected access radio find and connect to an alternative access radio within a few hundred milliseconds, typically within less than 400 ms. In addition, handoff attempts from any other mobile radios to the affected access radio are rejected. We recommend that you enable the link backhaul check feature on access radios in a wind farm deployment.

Figure 4-41 shows a link between the access radio and its switch is down. Assuming that the radio is powered by an external power source, not by PoE, the radio is still up and providing good wireless connectivity to vehicles. However, because the wired link is down and the radio is not able to forward traffic to the wired network, the radio goes into handoff inhibition mode and rejects any handoff attempts from an SOV radio.

Figure 4-41 Link Backhaul Check: Handoff Inhibition

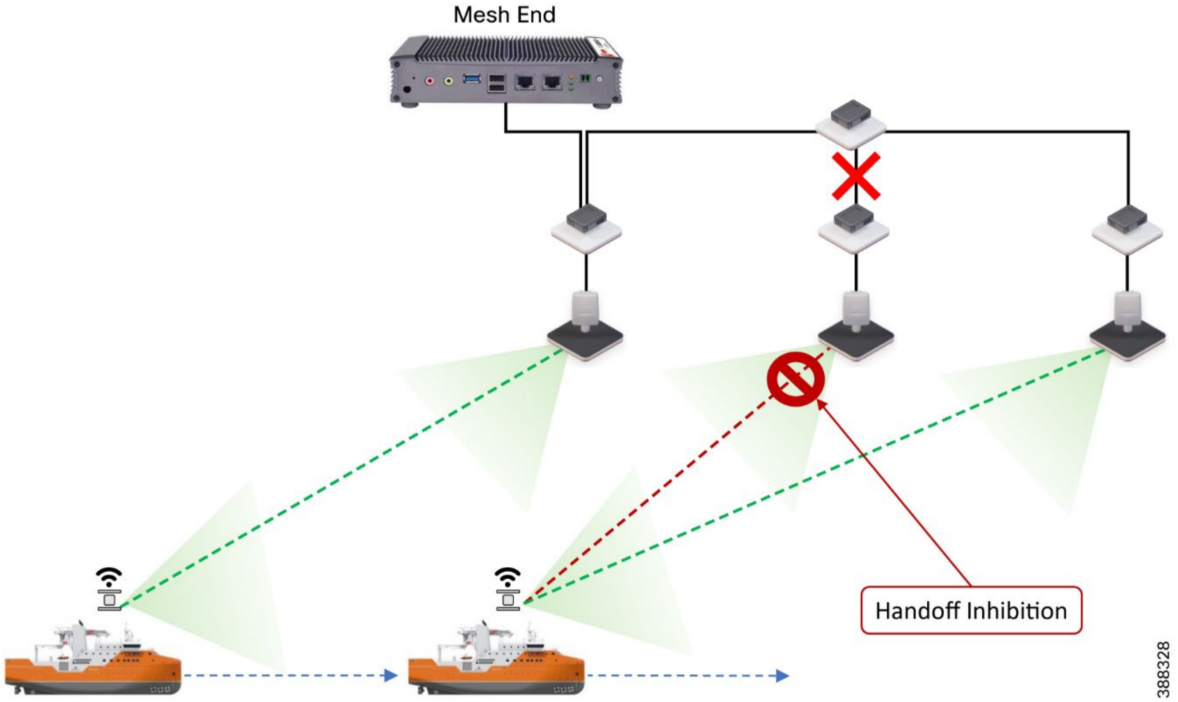


Mesh-End Backhaul Check: Handoff Inhibition

With the mesh end backhaul check feature, an access radio unit detects that it is not able to reach the active mesh end. This failure is triggered when layer 2 MAC reachability is lost to the active mesh end for 250 ms. The affected radio unit immediately advertises its status as Unavailable by transmitting a **handoff inhibition** message over the wireless channel. Upon receiving the **handoff inhibition** message, any existing mobile radios that are connected to the affected radio unit search for another access radio to connect to. All mobile radio units that are currently connected to the affected access radio find and connect to an alternative access radio unit within a few hundred ms, typically within less than 400 ms. In addition, handoff attempts from any other mobile radios to the affected access radio are rejected. We recommend that you enable the mesh end backhaul check feature on access radios in a wind farm deployment.

Figure 4-42 shows an access radio switch that has lost its fiber connectivity to the core switch. The access radio is powered on and providing good coverage and connectivity to vehicles. But because the radio is not able to forward traffic to the mesh end that is located within the control room, it goes into handoff inhibition mode and rejects the handoff request from the SOV radio.

Figure 4-42 Mesh End Backhaul Check: Handoff Inhibition



Onboard Radio Redundancy: Failover and Recovery

Titan high availability is not applicable for mesh ends only. In scenarios where two CURWB radios are deployed onboard a vehicle, the two radios can pair together by applying the Titan plugin to provide hardware redundancy.

The onboard failover process is similar to the mesh end failover process. It encompasses the same steps that are described in the previous section by just swapping the infrastructure and the onboard networks.

The main difference in these processes is that when a mobile unit becomes the new primary after a failure or recovery event, the mobile radio executes the following additional actions:

- If the automatic vehicle ID feature is enabled, the mobile radio computes a new vehicle ID and forces the update on all onboard units.
- It performs a forced handoff procedure instead of sending a **primary witch** command to update the infrastructure network more efficiently.

CURWB Security

All client traffic within an MPLS tunnel is already kept private by using the system passphrase However, CURWB radios also support AES encryption, which applies to MPLS tunnel traffic on wireless links.

Note: To enable the AES encryption feature, an AES plugin needs to be installed on the radio. When configuring AES encryption, AES encryption must be enabled on all radios within the system. Enabling AES only for a part of the system is not supported and causes a breakage.

SCADA Applications and Protocols

Turbine OEM and wind farm operators have steadily moved their substation operations to standard-based network (Ethernet, TCP/IP) with standard communication protocols, such as IEC 61850, DNP3 TCP, Modbus-TCP, IEC 60870-5-104, and OPC-UA. Nonetheless, a substation often contains devices that, for a number of reasons, are difficult or cost-prohibitive to migrate to standard-based network connectivity. These devices often use a variety of serial-based legacy SCADA protocols, including OPC-UA, Modbus, and IEC 60870-5-101. Because these devices often are critical to substation operations, they must be interconnected to the centralized SCADA applications of the substation operator.

SCADA protocols provide access to and from key operational devices within a wind farm network and a secure connection to the control center for telemetry and operational data. The OSS core provides key connectivity to these operational devices and communicates via these protocols over the WAN to the control center.

The types of devices that provide key operational data include:

- Wind turbine monitoring and control

- Fire detection and alarming
- HVAC
- Power systems protection and control
- Environmental and weather systems
- Wildlife detection and monitoring systems
- Lightning detection
- Marine systems (radar, radio)

These devices usually are key to operating a wind farm, providing both monitoring and control capabilities.

Legacy SCADA protocols, which are supported over legacy asynchronous interfaces, include:

- Modbus
- DNP3
- IEC 60870-5-101 (also known as T101)

Newer SCADA IP-based protocols that can be transported over Ethernet interfaces include:

- OPC UA
- Modbus-IP
- IEC 60870-5-104(also known as T104)

Many other SCADA protocols exist, but in the wind farm turbine SCADA network, only those listed above are commonly used.

Open Platform Communications Unified Architecture

Open Platform Communications Unified Architecture (OPC UA) is a data exchange standard for industrial communication (machine-to-machine or PC-to-machine communication). This open interface standard is independent of the manufacturer or supplier of an application, of the programming language in which the respective software was programmed, and of the operating system on which the application is running. OPC UA is the next generation of OPC technology. It's a more secure, open, reliable mechanism for transferring information between servers and clients.

In this architecture, there are two mechanisms for exchanging this data:

- A client-server model in which unified architecture (UA) clients use the dedicated services of the UA server
- A publisher-subscriber model in which a UA server makes configurable subsets of information available to any number of recipients

In a wind farm, communication between a third-party turbine control network and wind farm OSS SCADA devices uses the OPC UA protocol. OPC US is a client-server based model in which turbine vendor OPC UA clients can read turbine control data from an OPC UA server for monitoring in an offshore substation.

MODBUS and T104

Modbus TCP/IP (sometimes referred to as the Modbus TCP protocol or just Modbus TCP) is a variant of the Modbus family of simple, vendor-neutral communication protocols intended for supervision and control of automation equipment. Modbus TCP covers the use of Modbus messaging in an intranet or internet environment using the TCP/IP protocols. The most common use of the protocols is for the Ethernet attachment of PLCs, HMIs, I/O modules, and sensors to other I/O networks.

IEC 60870-5-104 (also known as T104) enables communication between a control station and a substation via a standard TCP/IP network. The TCP protocol is used for connection-oriented secure data transmission.

- T101 and T104 refer to IEC 60870-5-101 and IEC 60870-5-104 Standard respectively.
- T101 supports point-to-point and multi drop links over serial communications.
- T104 utilizes TCP/IP transport and network protocols to carry application data (ASDU), which is specified in T101.
- T104 allows balanced and unbalanced communication types.
- Balanced mode is limited to point-to-point links in which either station can initiate a transaction (similar to a dnp3 unsolicited response).
- Unbalanced mode is suitable for multi-drop links in which only the primary station can send primary frames.

Quality of Service Design

Quality of service (QoS) refers to the ability of a network to provide preferential or differential services to selected network traffic. QoS is required to ensure efficient use of network resources while adhering to business objectives. QoS also refers to network control mechanisms that can provide various priorities to different endpoints or traffic flows or guarantee a certain level of performance of a traffic flow in accordance with requests from application programs. By providing dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics, QoS can ensure better service for selected network traffic.

The wind farm network architecture consists of different kinds of switches with different feature sets. A QoS model is important to guarantee network performance and operation by streamlining traffic flow, differentiating network services, and reducing packet loss, jitter and latency.

QoS policies can be defined to classify ingress packets based on access control lists (ACLs), IP address, or class of service (CoS), set appropriate CoS values at ingress, and use the CoS values for further treatment on egress. We recommend classifying wind farm voice, video and network control packets on ingress based on ACLs or IP differentiated services code point (DSCP) values into the priority queue on egress. Remaining traffic can go into classes with guaranteed bandwidth.

Table 4-5 lists the possible traffic types in a wind farm network and the corresponding recommended ingress and egress classification, bandwidth and QoS treatment.

Table 4-5 Wind Farm Traffic Types, Bandwidth and QoS Requirements

Traffic Classes	DSCP	PHB	COS	Queue type	Assigned BW	Drop policy	Protocols
IP routing	48	CS6	6	Priority	100 Kbps	WTD	OSPF, EIGRP, BGP, HSRP, IKE
Latency sensitive critical data	47	EF	6			WTD	–
Voice	46	EF	5	Priority	300 Mbps	WTD	RTP
Mission critical data	40	CS5	7			WTD	OPC UA
Interactive video	34	AF41	4			WTD	CCTV
Streaming video	32	CS4	4				
Call signaling	24	CS3	3	CBWFQ	450 Mbps	WTD	SCCP, SIP, H323
Locally defined mission critical	26	AF31	5			WTD	–
Transactional Data and CURWB	18	AF21	2				
Network management	16	CS2	3			WTD	SNMP, SSH, Syslog
Bulk data	10	AF11	1	CBWFQ	150	WTD	Email, FTP, backup apps
Best effort	0	CS0	0				Default class
Scavenger	8	CS1	0				Internet

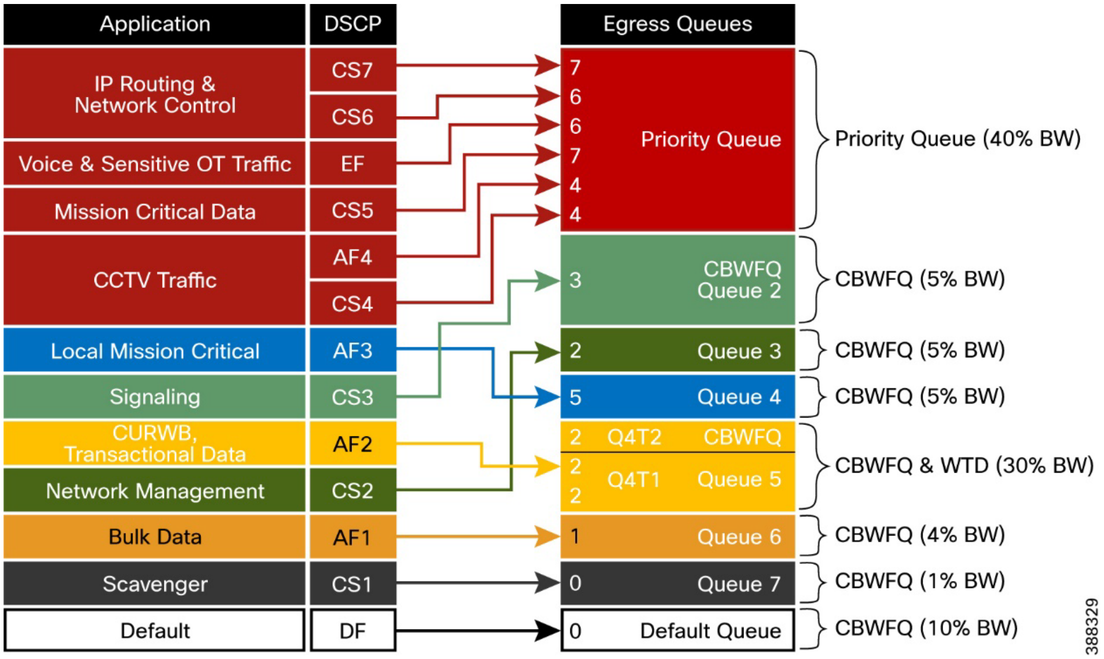
QoS Design Considerations

- Cisco IE3400 switches in the TAN and FAN support one priority queue, seven class based queues, and two QoS thresholds (1P7Q2T) at each egress interface. Traffic mapping at egress queues in the IE switches is performed as the QoS design shown in Figure 4-43.
- Cisco Catalyst 9300 Series and 9500 Series Switches in OSS and ONSS networks support two priority queues, six class based queues and three QoS thresholds (2P6Q3T) at each egress interface.
- Ingress traffic classification is based on DSCP, ACLs, or IP address (layer 3) and CoS or MAC ACL (layer 2), depending on the traffic type and set COS value.
- Each egress interface in the TAN, FAN, aggregation, and core switches in a network is mapped with a queuing policy, as per the

QoS design in Table 4-6.

- Egress weighted tail drop (WTD) is considered for the traffic beyond a certain bandwidth percentage.

Figure 4-43 Recommended 12 Class QoS Design and Egress Queue Mapping for Cisco IE Switches



Cisco Industrial Ethernet switches support the modular QoS command line interface. The modular approach can be implemented using the following steps.

1. Identify and classify the traffic. Various classification tools such as access control lists (ACLs), IP addresses, CoS, and IP differentiated services code point (DSCP) can be used. The choice of the tool depends on traffic types.
2. Perform QoS functions on the identified traffic. Available QoS functions include queuing, policing marking, shaping, and more. Functional selection depends on ingress or egress application traffic flow requirements.
3. Apply the appropriate policy map to the desired interfaces.

Chapter 5: Network Management and Automation

This chapter includes the following topics:

- Cisco DNA Center
- Device Discovery and Onboarding
- FAN REP Ring Provisioning using DNAC REP Automation Workflow
- Day N Operations and Templates
- SD-WAN Management

Cisco DNA Center

Cisco DNA Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides network visibility and uses network insights to optimize network performance and deliver an enhanced user and application experience. This guide focuses on a non-Software Defined Access (SDA) or a non-fabric design. A lack of network health visibility to network administrators, and manual maintenance tasks such as software upgrades and configuration changes are some of the common network challenges in an offshore wind farm network. Cisco DNA Center addresses these issues.

We recommend that Cisco DNA Center be placed as an application in the control center, but the final decision on location should be made considering your specific requirements.

Benefits of Cisco DNA Center include:

- As a single pane-of-glass, Cisco DNA Center network management performs critical functions to maintain the operational status of a network environment. These critical functions include assurance and monitoring of the production network, guided remediation of identified problems, and device replacement.
- Automated provisioning of network device configuration software updates and lifecycle management.
- Simplified network security policy deployment integrating with Cisco ISE.

Key considerations when adding Cisco DNA Center include the following:

- Cisco DNA Center requires connectivity to all network devices that it manages. All devices that need to be discovered and monitored should have an assigned IP address that is routable and able to reach the Cisco DNA Center.
- Cisco DNA Center requires internet connectivity for licensing information and updates. We recommend using a Smart License proxy. We also recommend that you allow secure access via the proxy service only to URLs and fully qualified domain names that are required by Cisco DNA Center. For more information see *Cisco DNA Center Security Best Practices Guide*:

  https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html
- If there is a firewall between Cisco DNA Center and managed devices, ensure that the required ports are allowed on the firewall.

  See "Required Network Ports" in *Cisco DNA Center Second-Generation Appliance Installation Guide* for a list of network ports that are required to be allowed in firewall:

  https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_3_5_2ndGen/m_plan_deployment_2_3_5_2ndgen.html#reference_rfc_g23_sfb
- Latency should be 100 ms or less to achieve optimal performance for all solutions that are provided by Cisco DNA Center. The maximum supported latency is 200 ms RTT. Latency from 100 ms through 200 ms is supported, although longer execution times could be experienced for certain functions, such as inventory collection and other processes that involve interactions with managed devices.
- Cisco ISE must be deployed with a version that is compatible with Cisco DNA Center. See *Compatibility Information*:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Some known limitations of Cisco DNA Center include the following:

- Cisco DNA Center does not support managing network devices with management IP address behind a network address translation (NAT) boundary.
- Firewalls running Firepower Threat Defense (FTD) software are not supported on Cisco DNA Center. However, devices that are connected behind an industrial firewall can be provisioned and managed by Cisco DNA Center.
- FAN REP ring provisioning using REP automation workflow is supported by Cisco DNA Center. However, the ring of rings (also

known as a subtended ring) REP provisioning is not automated in Cisco DNA Center workflows. We recommend using the Day-N template feature in Cisco DNA Center for all day N configurations and subtended TAN REP ring provisioning.

- Cisco DNA Center cannot manage products from third-party vendors.

  Figure 5-1 illustrates the Cisco DNA Center features that are used in this wind farm solution.

Figure 5-1 Firewall Design in Wind Farm Network Architecture

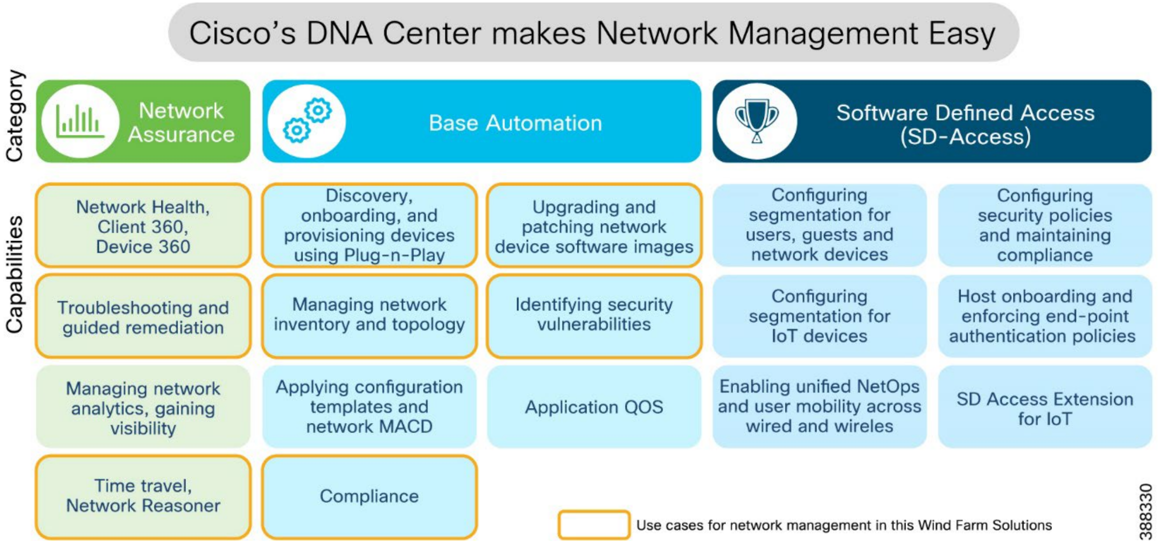
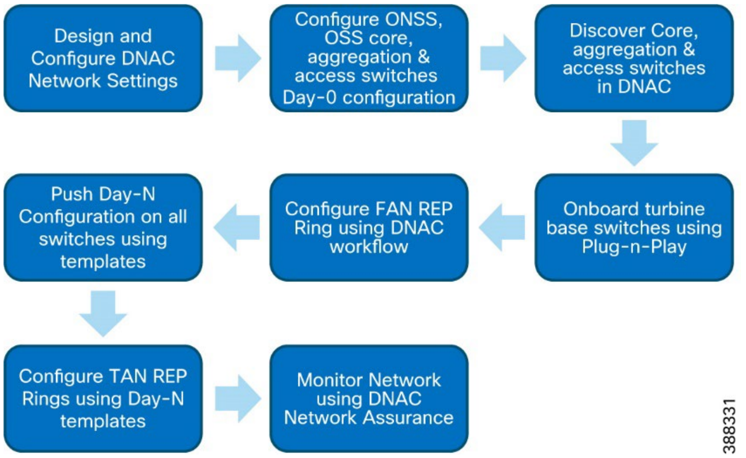


Figure 5-2 provides a flow diagram of Cisco DNA Center device settings, discovery, onboarding, and provisioning operations to manage wind farm network devices and endpoints.

Figure 5-2 Cisco DNA Center Wind Farm Network Management Flow Diagram



Device Discovery and Onboarding

This section covers the prerequisites for using Cisco DNA Center to discovery, provisioning, and network assurance features. It also covers offshore wind farm day 0 network provisioning, device discovery, and onboarding.

Prerequisites

- The Cisco DNA Center appliance and software have been installed. Those topics are covered in more detail in *Offshore Wind Farm Solution Implementation Guide*.
- Cisco DNA Center assigns users to roles that determine what types of operations a user can perform in the system. Users that need to provision the network should use the Network-Admin-Role. Only Cisco DNA Center system administrators should use the Super-Admin-Role.
- Define a network hierarchy by creating sites. Sites group devices by physical location, function, or both in a network. The network hierarchy represents your network locations. It allows for a hierarchy of sites, which contain areas, and areas contain buildings and floors. We refer to areas, buildings, and floors as site information. It is possible to create site information to easily

identify where to apply design settings or configurations. A site on Cisco DNA Center determines which network settings, software images, and customized templates are applied to a device. We recommend that you create a network hierarchy in Cisco DNA Center based on area, site, and building name per different places in the network. For example, sites, areas, and buildings could be named CC/WAN/ONSS/OSS, Infra/Core/DMZ, and so on.

- Configure network settings that apply to created sites, including settings for device credentials, DHCP, and NTP servers. These network settings may be applied to devices that belong to a site as part of automation workflows.
- Create network profiles. For switches, network profiles link configuration templates to sites.

  A network profile is a key concept in Cisco DNA Center and is used to standardize configurations for routers, switches, and WLCs in one or more sites. A network profile is used to assign configuration templates to devices based on their site information, device product family, and associated tags. For devices that require similar configuration, a template helps to reduce configuration time by enabling configuration re-use and using variables and logic statements as placeholders for any unique settings per device.
- We recommend that you manage software images within the DNA Center image repository for network infrastructure upgrades. Cisco DNA Center stores all unique software images according to image type and version. It is possible to view, import, and delete software images.
- Establish network connectivity between Cisco DNA Center in the control center and ONSS, OSS Core, access, and FAN aggregation switches in the wind farm network so that these devices can reach the Cisco DNA network. The switches in the ONSS, OSS, and FAN require initial manual configuration to be discovered and added into Cisco DNA Center inventory.

See *Cisco Wind Farm Solution Implementation Guide* for more information about Cisco DNA Center configuration in a wind farm solution:

Device Discovery

- The OSS and ONSS switches in a wind farm network are discovered and added to Cisco DNA Center manually. Therefore, these switches require day 0 configuration using the device CLI to be discovered and added to the Cisco DNA Center inventory.
- Day 0 CLI configuration on these manually added core, aggregation, and access switches in the OSS and ONSS involve configuration of basic SSH, SNMP, and CLI credentials, and the routing configuration that is needed to connect to Cisco DNA Center in a control center.

  See *Cisco Wind Farm Solution Implementation Guide* for more information about Cisco DNA Center device discovery configuration in a wind farm solution.
- Turbine base switches and nacelle switches (Cisco IE3400s) are connected to a FAN aggregation switch stack and are onboarded using the DNAC plug-and-play (PnP) feature.

Device Plug-n-Play Onboarding Using DNAC

Turbine base switches and nacelle IE3400 switches are onboarded one-by-one (in a linear topology depending on the ring size) using the DNAC plug-n-play feature. PnP onboarding considerations for turbine base switches and nacelle switches include the following:

- A turbine's base switch connected to a FAN aggregation Catalyst 9300 switch stack is initially onboarded with zero touch by configuring Cisco DNA Center as a PnP controller, the Catalyst 9300 as a PnP startup device (also called a seed device), and a central DHCP server in the OSS infrastructure network or control center.
- The next turbine base switch in a FAN is connected linearly to the previous turbine's base switch, which already is onboarded into Cisco DNA Center. This time, the uplink base switch acts as a PnP startup device for the newly connected base switch and initiates the PnP process on the newly connected base switch.
- Similarly, all switches in FAN and TAN must be PnP onboarded (in order around the ring) into Cisco DNA Center using the previously onboarded uplink switch as the PnP startup or seed device.

FAN REP Ring Provisioning using DNAC REP Automation Workflow

The Cisco DNA Center REP configuration workflow feature automates the provisioning of multiple IE switches in a ring topology. The ring topology is set up though a physical connection between two IE (base) switches that are onboarded into the Cisco DNA Center through PnP. The Cisco DNA Center non-fabric REP automation workflow feature considers a Catalyst 9300 switch stack as a REP edge device to form a closed REP ring with the IE switches that are connected to the same Catalyst 9300 switch stack.

Step-by-step instructions for configuring a REP ring using the DNA-C REP provisioning workflow for the FAN IE ring is discussed in *Cisco Wind Farm Solution Implementation Guide*.

REP Ring Design Considerations, Limitations, and Restrictions

- Only new REP ring (greenfield) deployments are supported. An existing REP ring topology, if any (one may have been configured using Day-N templates), in a wind farm FAN cannot migrated to a new REP ring configuration using the Cisco DNA Center REP automation feature.

- Considering the Catalyst 9300 switch stack as the STP root bridge, a maximum of 20 nodes (including Catalyst 9300 switches and up to 18 IE switches) in a stack is supported in a ring with default STP ring parameter values.
- A switch that is connected in a REP Ring cannot be deleted from the Cisco DNA Center inventory until the REP ring that the switch is part of is deleted.
- Multiple rings within a REP ring are not supported. A ring of rings is not supported. For example, a sub ring within the turbine cannot be provisioned using the DNAC REP workflow. See the following section for information about using Day-N templates to provision turbine sub rings.

Day N Operations and Templates

Cisco DNA Center provides an interactive template hub to author CLI templates. You can easily design templates with a predefined configuration by using parameterized elements or variables. After creating a template, you can use the template to deploy devices in one or more sites that are configured anywhere in your network. Templates allow you to define a configuration of CLI commands that can be used to consistently configure multiple network devices, reducing deployment time.

In the wind farm solution, the following day N configurations are pushed to devices using the templates features in Cisco DNA Center:

- Configuration of additional VRFs and VLANs.
- Configuration of TAN high availability REP ring (subtended REP ring of FAN ring).
- Configuration of NetFlow monitor and flow exporter for Cisco Secure Network Analytics flow collection.
- Network Device RMA operations that require configuration changes. For example, adding a new switch stack and pushing configuration in the OSS infrastructure.

Additionally, network devices lifecycle management, which includes running configuration compliance checks, guided troubleshooting, software image management (SWIM), and network assurance features are included in day N operations and management.

See *Cisco Wind Farm Solution Implementation Guide* for more information about Cisco DNA Network management day N provisioning and monitoring in the wind farm solution.

SD-WAN Management

Cisco SD-WAN is an enterprise-grade WAN architecture overlay that enables digital and cloud transformation for enterprises. It integrates routing, security, centralized policy, and orchestration into large-scale networks. It is multitenant, cloud-delivered, highly automated, secure, scalable, and application-aware with rich analytics.

In the wind farm solution, Cisco SD-WAN is used to provision and manage the WAN. Cisco IR8340 or 8000 series routers that are deployed as WAN edge routers in the ONSS are managed by Cisco vManage, a component of Cisco SD-WAN. The management of WAN edge routers and control center WAN headend routers is done by using Cisco SD-WAN.

For detailed design information about Cisco SD-WAN management, see the “WAN and vManage” section, in *Substation Automation Design Guide—The New Digital Substation*:

https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/3-0/CU-3-0-DIG.pdf

Chapter 6: Security Design Considerations

This chapter includes the following topics:

Security Approach and Philosophy

Many wind farms increasingly form part of a country’s national critical infrastructure and as such should be protected.

There is a need for a cost-effective security model, especially one that provides easier deployment, maintenance, and troubleshooting, and improved stability and resiliency for wind farm operations.

Cyber security must be comprehensive and a fully integrated part of the overall network design. Any design should seek to minimize administrative overhead in cybersecurity deployment and operations.

The ability to identify all wind farm assets and their associated vulnerabilities, detect any new threats or anomalous behavior on the network, and monitor traffic on an ongoing basis greatly enhances the capability to minimize the cybersecurity overhead.

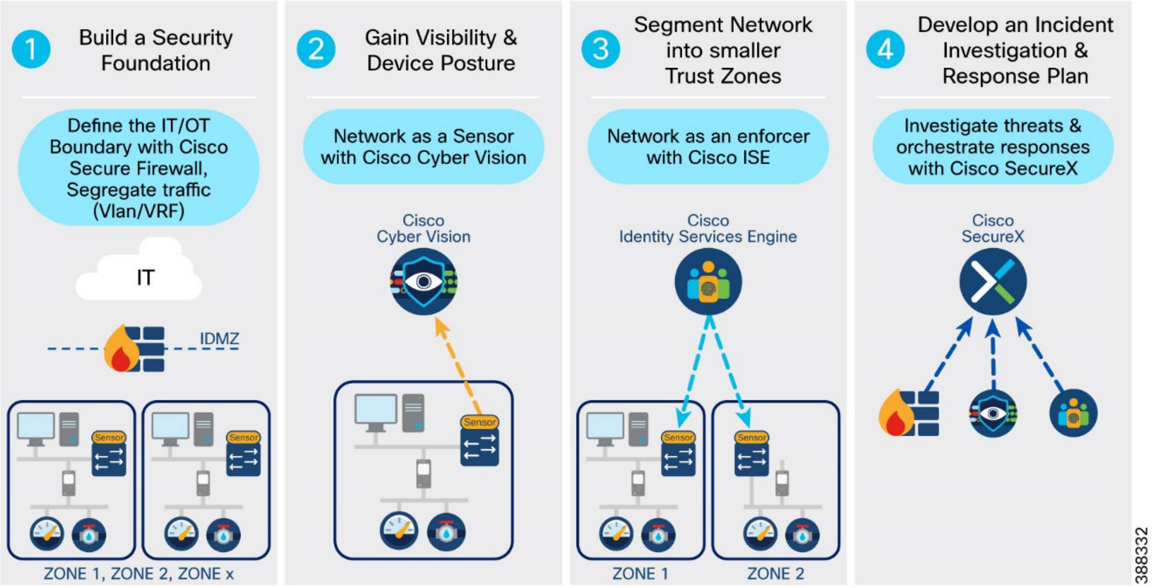
Improved security measures are necessary to become compliant with the North American Electric Reliability Corporation Critical Infrastructure Protection requirements (NERC CIP) or the NIS2 directive in the EU.

The following fundamental principles must be adopted by the asset network operator to ensure secure systems:

- Visibility of all devices in the wind farm networks: Traditionally, enterprise devices such as laptops, mobile phones, printers, and scanners are identified by the enterprise management systems when these devices access the network. This visibility can be extended to all devices on a wind farm network.
- Segmentation and zoning of the network: Segmentation is a process of bounding the reachability of a device and zoning is defining a layer where all members in that zone have identical security functions. Designing zones in a network is an organized method for managing device access within a zone and controlling communication flows across zones. Segmenting devices further reduces the risk of an infection spreading if a device is subjected to malware.
- Identification and restricting data flows. All devices in a wind farm network (operational network) and enterprise (IT-managed network) must be identified, authenticated, and authorized. The network must enforce a policy when users and industrial automation and control system (IACS) assets attach to the network.
- Detection of network anomalies: Any unusual behavior in network activity must be detected and examined to determine if the change is intentional or due to a malfunction of a device. Detecting network anomalies as soon as possible gives plant operators the ability to remediate abnormalities in the network quickly, which can help reduce possible downtime.
- Detection and mitigation of malware: Unusual behavior by an infected device must be detected immediately, and the security tools should allow remediation actions for an infected device.
- Implementation of appropriate firewalls: Traditional firewalls are not typically built for industrial environments. There is a need for a firewall that can perform deep packet inspection on industrial protocols to identify anomalies in IACS traffic flows.
- Hardening of the networking assets and infrastructure: This critical consideration includes securing key management and control protocols, such as using SSH instead of Telnet for remote sessions, using simple network management protocol (SNMP) V3, and using HTTPS instead of HTTP for device GUIs.
- Monitoring of automation and control protocols: It is important to monitor the IACS protocols for anomalies and abuse.
- Adhering to security standards: In the 1990s, the Purdue Reference Model and ISA 95 created a strong emphasis on architecture that uses segmented levels between various parts of a control system. This approach was further developed in ISA99 and with IEC 62443, which brought focus to risk assessment and business processes. Any security risk assessment identifies which systems are defined as critical control systems, non-critical control systems, and non-control systems.

Figure 6-1 shows a sequence of steps for implementing network security in an offshore wind farm network.

Figure 6-1 Offshore Wind Farm Network Security Approach



Steps to implement network security in an offshore wind farm:

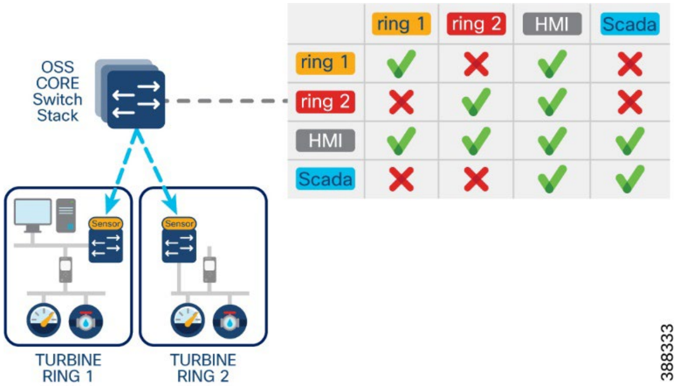
1. Creating zones and conduits: Using good design techniques provides the foundation for any cybersecurity architecture. Many standards (such as IEC62443 and NERC CIP) reference the concepts of segregating devices and controlling traffic flows between those devices. VLANs and VRFs create logical zones and segregate traffic and devices, thus restricting data flows between devices. Firewalls provide control points where traffic can be inspected and access restricted to only the traffic flows that are desired (least privilege). Where firewalls are not required, access control lists provide simple access control for traffic flows and define secure perimeters for the various subsystems.
2. Asset discovery and traffic flow visibility: Cisco Cyber Vision provides the ability to discover assets that are connected to the network and to determine how these assets are communicating. This visibility of assets and the traffic flows between them allows an asset operator to make informed decisions on allowed and undesirable traffic flows. This visibility also allows the asset operator to create a baseline for what is considered normal behavior and have alerts configured for any changes to the network assets or traffic flows. It is also important to have visibility of traffic flows north-south to the OSS and ONSS and externally to the data center.
3. Dynamic segmentation: Cisco Identity Services Engine (ISE) utilizes Cisco TrustSec to logically segment control system networks. Cisco TrustSec classification and policy enforcement functions are embedded into Cisco switching, routing, wireless LAN, and firewall products. At the point of network access, a Cisco TrustSec policy group, called a security group tag (SGT), is assigned to an endpoint, typically based on that endpoint's user, device, and location attributes. The SGT denotes the endpoint's access entitlements, and all traffic from the endpoint carries the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions. Cyber Vision can be integrated directly with ISE. Cyber Vision shows assets and their communications in maps that operations teams can easily relate to their industrial processes. This information gives administrators the opportunity to group assets into logical zones based on the business roles that these devices have on the network. ISE can use the asset groupings to implement more granular policies in the network switches that support SGTs. As organizations implement micro segmentation policies, groups can be made smaller, and conduits can be monitored to ensure that policies do not interfere with daily operations of the business.
4. Threat detection and response: The final consideration for securing the offshore wind farm network is the ability to detect and respond to potential threats. The NIST cybersecurity framework outlines five core cybersecurity principles—identify, protect, detect, respond, recover. The first three steps above cover the capabilities that are needed to identify the people and assets in your network, protect them through the use of network policies, and detect the occurrence of a cybersecurity event. The respond function supports the ability to contain the effect of a potential cybersecurity incident. Cisco SecureX is an incident investigation and response platform that aggregates intelligence from both Cisco security products and third-party sources. This intelligence enables security analysts to identify whether observable items such as file hashes, IP addresses, domains, and email addresses are suspicious. When you start an investigation using Cisco SecureX, context is automatically added from integrated Cisco security products, so you know instantly which of your systems was targeted and how. Cisco SecureX obtains relevant information from intel sources and security products, displaying results in seconds. Cisco SecureX also provides security operations teams with the ability to act immediately by triggering custom workflows or continue their investigation with the tools provided.

Using Cisco TrustSec on IE switches with ISE to enforce security policies at the OSS layer 3 boundary (macro segmentation) provides an easy path to move from manually configured access control lists to a centralized policy-based network. Security policies are configured centrally on ISE and pushed into the network. Cyber Vision shares the discovered asset attribute information to ISE, as ISE does not natively contain industrial asset information.

Security policies and traffic rules are defined based on zones. For example, a security zone can be determined by VLANs, Ports or locations etc.

Figure 6-2 shows an example microsegmentation security policy based on IE rings, HMI. and SCADA devices.

Figure 6-2 Example Microsegmented Network Security Policy



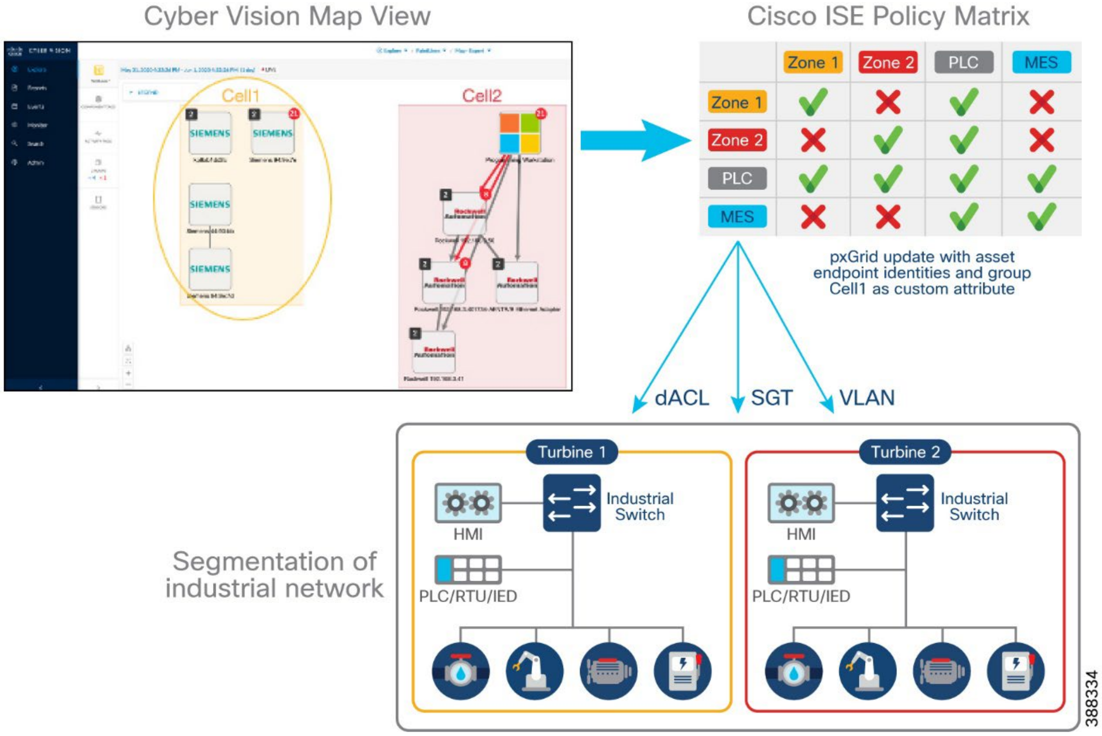
	ring 1	ring 2	HMI	Scada
ring 1	✓	✗	✓	✗
ring 2	✗	✓	✓	✗
HMI	✓	✓	✓	✓
Scada	✗	✗	✓	✓

Using micro segmentation, operations personnel can group assets on Cyber Vision into more meaningful groups. These group names are pushed to ISE (group tag attributes are shared from Cyber Vision to ISE). Subsequently, ISE can match a policy of the same name (preconfigured by IT) and ISE pushes the required SGTs and dACLs to the appropriate switches in the network.

This approach allows a deep level of segmentation of devices into smaller groups based on their roles rather than their VLANs. membership.

Figure 6-3 shows an example industrial network topology in Cisco Cyber Vision, its security policy matrix in ISE, and the application of a security policy (dACL) based on SGT and VLAN.

Figure 6-3 Example Industrial Network with Microsegmentation and Security Policy



	Zone 1	Zone 2	PLC	MES
Zone 1	✓	✗	✓	✗
Zone 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

Wind Farm Network Security Use Cases and Features

This section describes the wind farm network security use cases for various services, applications, equipment, and devices (also known as wind farm actors) that are found in different places within the architecture. Security must be comprehensive and fully integrated with the overall network architecture. Wind farm network security design has many commonalities with various other industry solutions such as substation automation, industrial automation, and so on. The objective is to promote the use of common security designs and principles across solutions, where possible.

Table 6-1 lists various wind farm network security use cases, solution design considerations, and security features to be adopted to address security challenges in the network.

Table 6-1 Wind Farm Security Use Cases and Features

Security Use Case	Security Solution	Security Features
Network segmentation and zoning	Define macro and micro network segments: ▪ VRF ▪ VLAN ▪ SGT ▪ SGACL	Macro segmentation (virtual routing and forwarding and VLANs) ▪ Network logically separated into smaller network segments to be managed independently Micro segmentation (scalable group tag) ▪ Allow policy control within a VRF/VLAN ▪ Segments map to an SGT group (user, application, device, and so on) ▪ Segments allows the group information to be carried from the source to the destination, allowing policies to be applied on the group ▪ Designing zones is an organized method for managing device access within a zone and to control communication flows across zones
Traffic and asset visibility	Detect IT and OT traffic flows and assets: ▪ Cisco SNA (Stealthwatch) ▪ Cisco Cyber Vision	▪ NetFlow and Cisco SNA for flow collection and anomaly detection ▪ Cisco Cyber Vision Network sensors for OT asset visibility and flow detection
IT an OT operational insight	Gain visibility and monitor network operations: ▪ Cisco Identity Services Engine (ISE) ▪ Cisco Stealthwatch Management Console (SMC) ▪ Cisco Cyber Vision Center (CVC)	▪ AAA identity services ▪ Network management ▪ Asset inventory ▪ Anomaly detection ▪ Deep packet inspection (DPI) ▪ Centralized analytics and data visualization
Data encryption, threat detection and protection	Protect network edges: ▪ Firewall and intrusion detection at DMZ ▪ Network edge firewall (Cisco Firepower) ▪ Secure IPSec tunnels for WAN Edge routers connectivity over public backhaul	▪ Access control lists (ACLs) ▪ Intrusion detection systems (IDS) and intrusion prevention systems (IPS) ▪ Advanced malware protection ▪ VPN services ▪ Wide area VPN and encryption (IPsec)
Secure remote access	Secure remote connectivity: ▪ Remote VPN service ▪ Control center firewall as VPN concentrator	▪ IPSec and SSL VPN encryption ▪ Cisco AnyConnect VPN Mobility Client

User and endpoints authentication and access control	Secure edge and device connectivity	▪ Layer 2 security features (port security, DHCP snooping, ARP inspection, storm control, and so on) ▪ 802.1X authentication ▪ MAC authentication bypass (MAB) authentication ▪ QoS marking ▪ NetFlow ▪ Cisco TrustSec tagging (SGT) and policy (SGACL) enforcement

Network Segmentation Design

Network segmentation is the practice of dividing a large network into several smaller subnetworks that are isolated from one another.

- Macro segmentation:
    - Network is logically separated into smaller network segments that are managed independently. Virtual routing and forwarding (VRF) provides a separate routing table for each of the network zones that requires separation from other network zones. VRFs provide layer 3 segmentation.
    - Network traffic for each segment (VLAN) is segregated (unless a network policy defines otherwise). VLANs provide layer 2 segmentation.
    - When a network or security issue occurs within the network, the issue is contained within a segment. Thus, a security risk is minimized to a particular segment.
- Micro segmentation:
    - Allows security and policy control within a VRF or VLAN.
    - A segment maps to an SGT group (user, application, device, and so on). Scalable groups (SG) allow security policy definitions for allowing and denying group communication, SGT propagation, and policy enforcement in the network edge.
- Define group access policy based on macro and micro segments
    - Define whether or not VRF to VRF communications are allowed.
    - Define group communication based on SGTs and SGACLs.

See Table 4-3, VLANs and VRFs in the Wind Farm Network Design, for a list of VLANs and VRFs in the wind farm network that is validated in this solution.

Advantages of Network Segmentation

- Improved security: Network traffic can be segregated to prevent access between network segments.
- Better access control: Allows users to access only specific network resources.
- Improved monitoring: For login events, monitoring allowed and denied internal connections, and detecting suspicious behavior.
- Improved performance: With fewer hosts per subnet, local traffic is minimized. Broadcast traffic can be isolated to a local subnet.
- Better containment: When a network issue occurs, its effects are limited to the local subnet.

Cisco Secure Network Analytics (Stealthwatch)

Network visibility is the foundation for the continuous monitoring that is needed to gain awareness of what is happening in a network. Complete visibility is critical to making proactive decisions and getting to resolutions as quickly as possible. Network threat defense prevents threats from an external network entering the internal network and identifies suspicious network traffic patterns within a network.

Cisco Secure Network Analytics Enterprise (formerly Cisco Stealthwatch) provides network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Cisco Secure Network Analytics Enterprise can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, DDoS attacks, illicit crypto mining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring across network traffic, even if the traffic is encrypted.

Cisco Secure Network Analytics enlists the network to provide end-to-end visibility of traffic. This visibility includes knowing every host—seeing who is accessing what information at any point. It is important to know what normal behavior for a particular user or host is and to establish a baseline from which you can be alerted to any change in the user or host behavior the instant it happens.

Cisco Secure Network Analytics offers many advantages, including:

- Network visibility: Provides comprehensive visibility in a private network and the public cloud, without deploying sensors everywhere.
- Threat detection: Constantly monitors the network to detect advanced threats in real time. Using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, Cisco Secure Network Analytics reduces false positives and alarms on critical threats affecting your environment.
- Incident response and threat defense: Protects network and critical data with smart and effective network segmentation. Uses secure network analytics integration with Cisco Identity Services Engine (ISE) to create and enforce policies, and keep unauthorized users and devices from accessing restricted areas of the network.

Flexible NetFlow Data Collection

NetFlow is a network protocol system created by Cisco that collects active IP network traffic as it flows in or out of an interface. NetFlow is now part of the Internet Engineering Task Force (IETF) standard (RFC 3954) as Internet Protocol Flow Information eXport (IPFIX, which is based on NetFlow Version 9 implementation), and the protocol is widely implemented by network equipment vendors.

NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. NetFlow creates flow records for the packets that flow through the switches and the routers that are in a network between end devices, and exports the flow records to a flow collector. The data collected by the flow collector is used by different applications to provide further analyses. NetFlow is primarily used for providing security analyses, such as malware detection, network anomalies, and so on.

The Cisco Industrial Ethernet (IE) 3x00 Series switches, Cisco Catalyst 9300, and Cisco Catalyst 9500 support full Flexible NetFlow. Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine whether the packet is unique or similar to other packets.

Typically, an IP flow is based on a set of five and up to seven IP packet attributes. All packets with the same source or destination IP address, source or destination ports, protocol interface, and class of service are grouped into a flow and then packets, and bytes are tallied. This methodology of fingerprinting or determining a flow is scalable because a large amount of network information is condensed into a database of NetFlow information called the NetFlow cache.

With the release of NetFlow v9, a switch or router can gather additional information, such as ToS, source MAC address, destination MAC address, interface input, interface output, and so on.

As network traffic traverses a Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Secure Network Analytics Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is active (long lived) for a configured time. The active flow lasts longer than the configured active timer (for example, long FTP download and the standard TCP/IP connections). There are timers to determine whether a flow is inactive, or a flow is active (long lived).

We recommend that NetFlow monitoring be enabled in a wind farm network for security on all the interfaces in the network, including within the FAN and TAN switches interfaces to OSS infrastructure where application servers reside, and so on. Configuring NetFlow can be done using Cisco DNA Center templates, and is covered in detail in *Cisco Wind Farm Solution Implementation Guide*.

Cisco Secure Network Analytics for Windfarm Network Security

The main components of the Cisco Secure Network Analytics system are:

- Secure Network Analytics Flow Collector (SFC)
- Secure Network Analytics Management Console (SMC)

Note: The SFC or SMC resides on different virtual or hardware appliances.

The SFC collects NetFlow data from network devices, analyses it, creates a baseline for normal network activity, and generates an alert for any behavior that falls outside of the baseline. Based on the volume of traffic, there could be one or multiple SFCs in a network. The SMC provides a single interface for the IT security architect to get a contextual view of the entire network traffic. The SMC collects NetFlow information to gain visibility across all network conversations (north-south and east-west traffic) to detect internal and external threats. It also conducts security analytics to detect anomalous behavior.

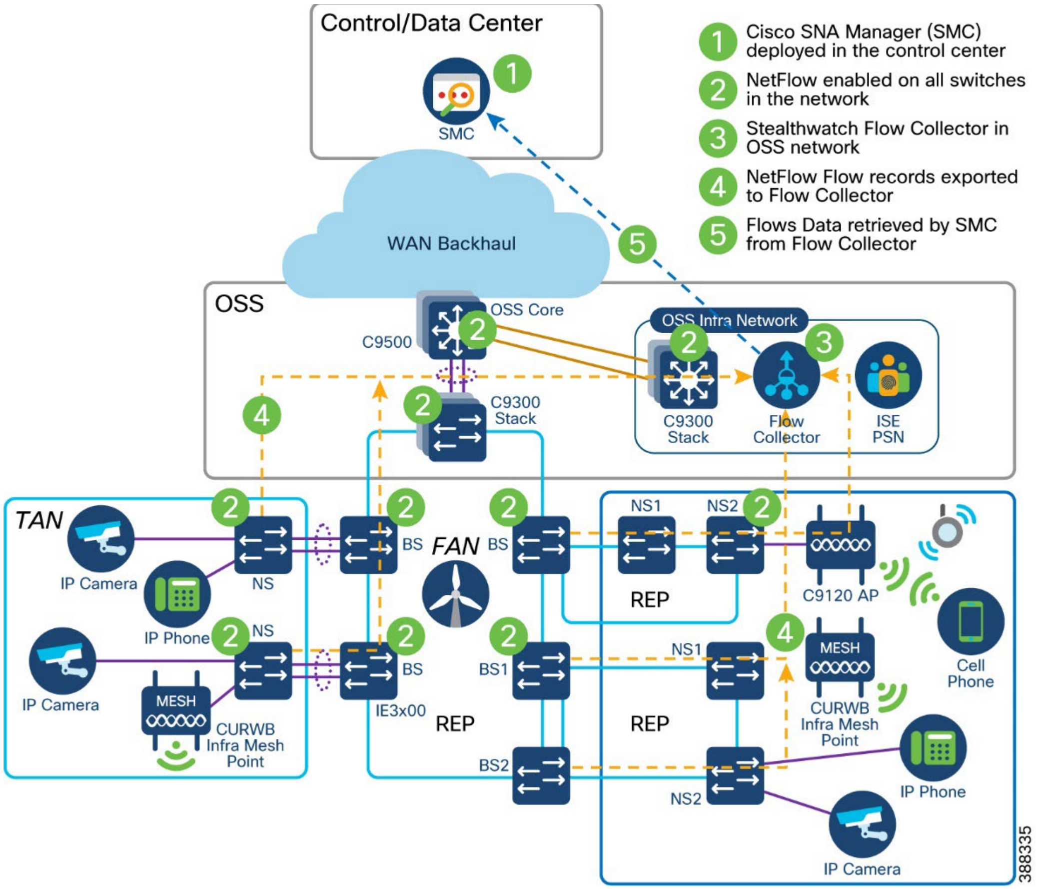
The SMC has a Java-based thick client and a web interface for viewing data and configurations. The SMC provides the following:

- Centralized management, configuration, and reporting for up to 25 SFCs
- Graphical charts for visualizing traffic
- Acceleration of threat detection and incident response to reduce security risk
- Integration with ISE, providing visibility of device and user information

The SMC Network Security Dashboard provides security insights such as top alarming hosts, today’s alarms, flow collection trends, top applications in the network, and so on.

Because the SFCs are to be accessed by all endpoints in the wind farm network, we recommend that the SFC be deployed in the OSS infrastructure network and SMC in the control center network, as shown in Figure 6-4.

Figure 6-4 Wind Farm Secure Network Analytics (Stealthwatch) Design



Important considerations when deploying a Secure Network Analytics system include the following:

- Secure Network Analytics is available as both hardware (physical appliances) and virtual appliances.
- Resource allocation for the SNA Flow Collector depends on the number of flows per second (FPS) that is expected on the network, the number of exporters (networking devices that are enabled with NetFlow), and the number of hosts that are attached to each network device.
- Data storage requirements must be taken into consideration, which again depends on the number of flows in the network.
- A specific set of ports needs to be open for the Secure Network Analytics solution in both the inbound and outbound directions.

See *Cisco Secure Network Analytics System Configuration Guide* for information about the installation of Secure Network Analytics, SFC scalability requirements, and data storage and network inbound and outbound ports requirements:

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/7_4_1_System_Configuration_Guide_DV_1_6.pdf

Cisco Secure Network Analytics for Abnormal Traffic Detection

A wind farm network engineer or security architect can use Cisco Secure Network Analytics with NetFlow enabled on Cisco Industrial Ethernet (IE3x00) switches in the ring, Cisco Catalyst 9300 or 9500 switches acting as FAN aggregation, and core switches to monitor the network flows in WF.

By integrating Secure Network Analytics and ISE, you can see myriad details about network traffic, users, and devices. Instead of showing just a device IP address, Cisco ISE delivers many key details, including username, device type, location, the services being used, and when and how the device accessed the network.

NetFlow is enabled on all wind farm networking devices to capture traffic flows, which are then sent to the SFCs. Flow records from the network devices are exported to SFCs in the OSS infrastructure network. The SMC retrieves the flow data from the SFCs and runs prebuilt algorithms to display the network flows. The SMC also detects and warns if there is any malicious or abnormal behavior occurring in the network.

Secure Network Analytics includes many machine learning algorithms that can assist a network security professional with detecting abnormal and malicious traffic in a network. It can detect abnormal behavior and provide the IP address of the device that is causing the issue. This information greatly simplifies the detection process.

Benefits of SNA in wind farm network include the following:

- Secure Network Analytics detects a possible infiltration or abnormal traffic activity using NetFlow in the wind farm network by raising an alarm under the High Concern index.
- SMC triggers an alarm whenever it detects abnormal or malicious activity on the network.
- Wind farm network security professionals respond to the alarms by planning remediation that involves further investigation and restricting access to the device that is causing the abnormal or malicious activity on the network.
- The device or user that is causing abnormal or malicious activity in the network is identified with the help of Cisco ISE, and the network security professional triggers a policy action to quarantine the device access in the network.

Operational Technology Flow and Device Visibility using Cisco Cyber Vision

For wind farms, SCADA with DNP3 or MODBUS protocol traffic in an OT VRF network is an example of an operational technology (OT) flow in the network. A Cyber Vision sensor deployment for OT flow and device detection shows different actors, such as the SCADA client, Cyber Vision Sensor, SCADA server, and Cyber Vision Center, that are involved in the network for OT traffic flow and device detection.

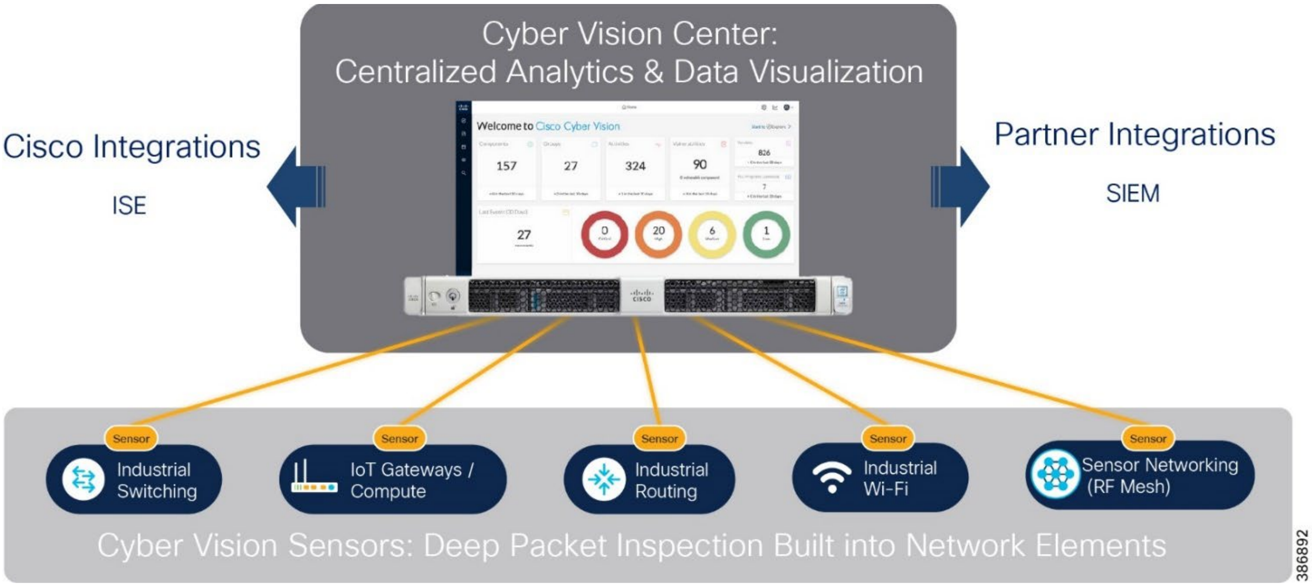
Cyber Vision Design Considerations

Cisco Cyber Vision gives OT teams and network managers full visibility into their assets and traffic flows. With this visibility, teams can implement security best practices, drive network segmentation, and improve operational resilience. Cisco Cyber Vision and ISE combined threat response helps to address many of the design requirements for visibility, anomaly detection, and mitigation.

The Cisco Cyber Vision solution is a two-tier architecture made of the inline network sensors on Cisco IE3400 IE3300-X, Catalyst 9300, IR1101 devices, and the Cisco IC3000 Industrial Compute Gateway as a dedicated hardware sensor. The sensors are dedicated to capturing network traffic by using various SPAN features. The sensors then decode the SCADA and other OT protocols that are supported by Cyber Vision using the Cyber Vision deep packet inspection (DPI) engine.

Figure 6-5 illustrates the Cisco Cyber Vision two-tier architecture.

Figure 6-5 Cisco Cyber Vision Two Tier Architecture

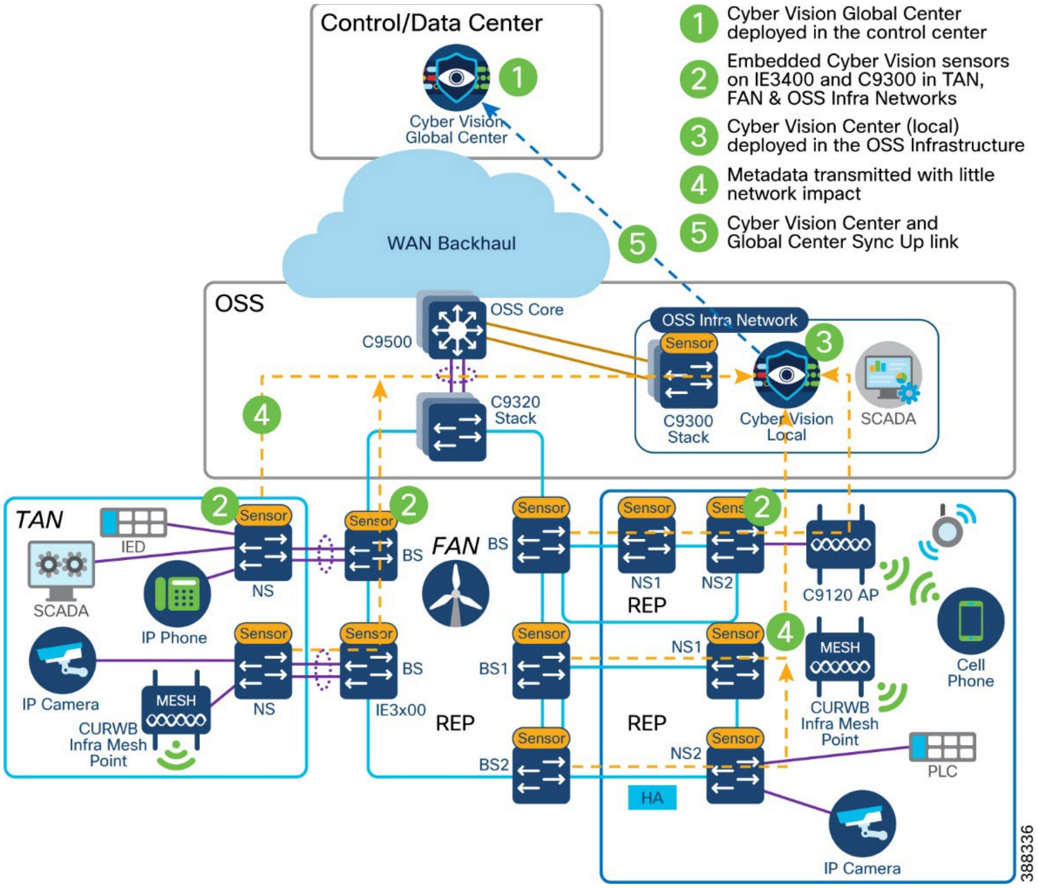


Cisco Cyber Vision design considerations in an offshore wind farm network include the following:

- A local Cisco Cyber Vision Center located in WF OSS infrastructure network to collect metadata from CV network sensors that are deployed across TAN and FAN.
- Local Center synchronizes with Cyber Vision Global Center located in a data center or control center.
- Cisco Cyber Vision Global Center feature allows synchronization of several local centers within a single repository.
- The Global Center aggregates local centers into a single application and presents a summary the activities of several centers.
- The collection network design: Consists of a separate VLAN for collection network and separate VLANs for OT traffic with a SPAN design as required for the sensor type.

Figure 6-6 illustrates the Cisco Cyber Vision design in the wind farm network architecture.

Figure 6-6 Wind Farm Cyber Vision Design for Traffic Visibility



For more detailed information about Cyber Vision Global and Local Center deployments, see *Cisco Cyber Vision Data Sheet*:

https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-743222.html

Wind Farm Cyber Vision Network Sensors

Cisco IE3400 switches in a TAN and FAN and Catalyst 9300 switch in an OSS network act as Cyber Vision network sensor to capture OT protocol flows and messages in a wind farm network. For a list of supported OT protocols, see OT Protocols Support.

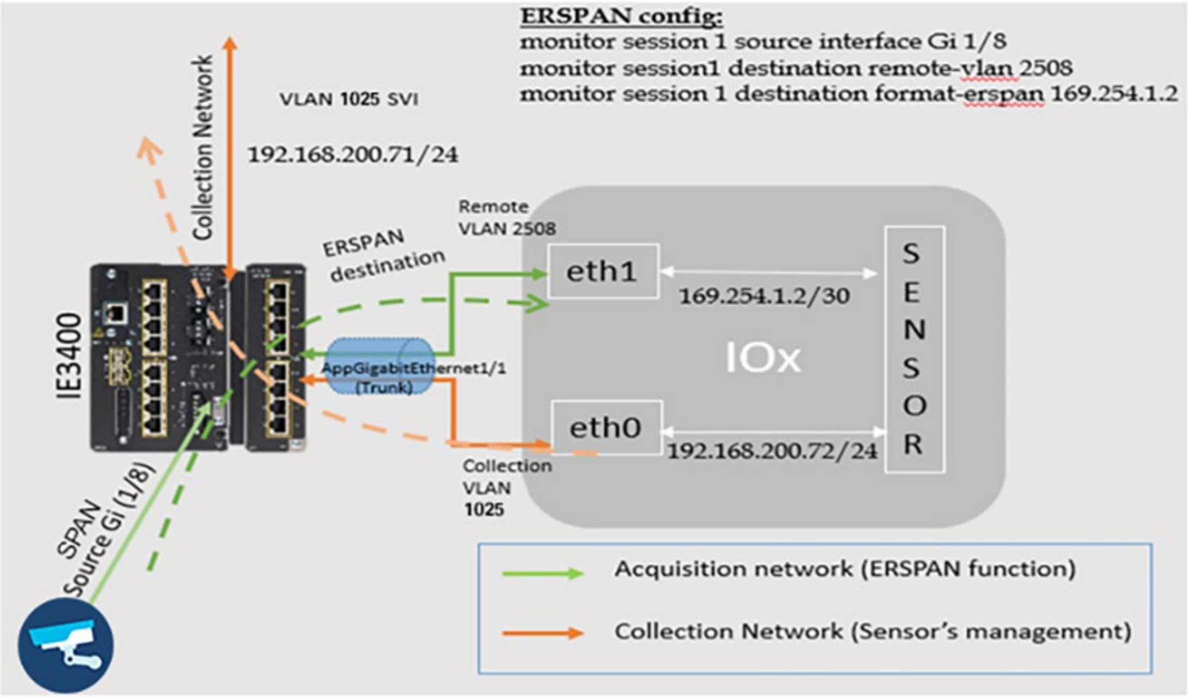
The Cisco Cyber Vision sensor application hosted on Cisco IE3400 and Catalyst 9300 switches. The IOx architecture of these switches provides an internal AppGigabitEthernet1/1 interface that can be configured as either access or trunkmode and enables connectivity for the hosted application.

Currently, an IOx application interface must have VLAN ID configured even if the AppGigabitEthernet1/1 interface is configured as access mode. We recommend configuring the AppGigabitEthernet1/1 as a trunk interface for hosting the Cisco Cyber Vision sensor application. This application uses two interfaces, one for capturing traffic from the IE3400 switch physical interfaces and one for the Cisco Cyber Vision Center collection network.

The IE3400 may have multiple VLANs provisioned as part of a wind farm network segmentation. Different VLANs can also be provisioned to forward the traffic that is monitored on physical interfaces or VLANs of IE3400, forward the same traffic to the hosted sensor application for further processing, or enable connectivity from the sensor application to the Cisco Cyber Vision Center collection network interface.

The AppGigabitEthernet1/1 interface is a non-routed interface and the sensor application interprets source packets to be GRE encapsulated. For monitoring and forwarding packets in ERSPAN format to the sensor application, enable ERSPAN on the provisioned AppGigabitEthernet1/1 VLAN. IE3400 IOx application interface mapping depicts the logical mapping of physical interfaces and the hosted IOx application on the IE3400.

Figure 6-7 **IE3400 Network Sensor Application Interface Mapping**



ERSPAN config:

```
monitor session 1 source interface Gi 1/8
monitor session1 destination remote-vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
```

OT Protocols Support

Table 6-2 lists the OT protocols that are supported by Cyber Vision in the wind farm network architecture.

Table 6-2 **OT Protocols Supported by Cisco Cyber Vision for Wind Farms**

Protocols	Type of Communication
MODBUS	TCP/IP
DNP3	▪ TCP/IP ▪ Serial over TCP raw socket
T101	TCP/IP
T101 to T104	T101 to T104
OPC-UA	TCP/IP

For additional information about Cyber Vision 4.x protocol support, see *Cisco Cyber Vision Protocol Support Data Sheet*:

https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/cyber-vision-protocol-support-ds.html

Network Firewall Design

A DMZ in a wind farm OSS network provides a layer of security for the internal network by terminating externally connected services from the internet and cloud at the DMZ and allowing only permitted services to reach the internal network nodes.

The DMZ design in the wind farm architecture is a dual firewall model: the DMZ is protected by firewalls with redundancy. The OSS DMZ firewall at the OSS DMZ or third-party network helps provide controlled access into OSS network. It also provides segmentation and separation between OSS zones. The DMZ design uses a single firewall (with redundancy) with a minimum of three network interfaces to separate the external network, internal network, and DMZ.

Traditional stateful firewalls with simple packet filtering capabilities efficiently block unwanted applications because most applications meet the port and protocol expectations. However, in today's environment, protection based on ports, protocols, or IP addresses is no longer reliable or workable. This fact led to the development of an identity-based security approach, which takes organizations a step beyond conventional security appliances that bind security to IP addresses.

NGFW technology offers application awareness that provides you with a deeper and more granular view of network traffic in your systems. The level of information detail that NGFW provides can help with both security and bandwidth control.

Cisco NGFW (Firepower appliance) resides at the network edge to protect network traffic from the external network. In the wind farm design, a pair of Firepower appliances (Firepower 2140s) are deployed as active and standby units for high availability. The Firepower units must be the same model with the same number and types of interfaces and must be running the same software release. In the software configuration, the two units must be in the same firewall mode (routed or transparent) and have the same network time protocol (NTP) configuration.

The two units communicate over a failover link to check each other's operational status. Failovers that are triggered by events such as the primary unit losing power, the primary unit physical interface link going down, or the primary unit physical interface link having a connection issue. During a stateful failover, the primary unit continually passes per-connection state information to the secondary unit. After a failover occurs, the same connection information is available at the new primary unit. Supported end-user applications (such as TCP/UDP connections and states, and SIP signaling sessions) are not required to reconnect to keep the same communication session.

For more information, see *Firepower Management Center Configuration Guide*:

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

In a wind farm network, Cisco Firepower at the control center, OSS, and ONSS network edges provide zone-based network access control and remote access VPN services for secure remote connectivity into the wind farm network.

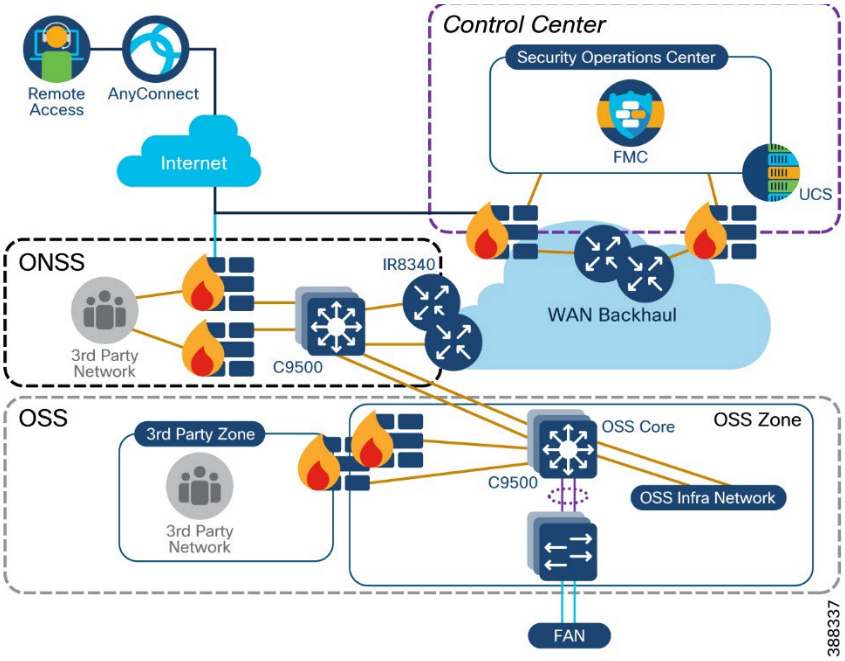
Securing the wind farm perimeter ensures that all traffic entering or exiting onshore and offshore networks is controlled and inspected where required.

Validated design security control points include the following:

- DMZ at a data center
    - Normal enterprise security model for incoming WAN connectivity
    - Clustered firewalls for IDS and IPS
- DMZ at onshore substation
    - Redundant firewalls for IDS and IPS
    - Secure local perimeter for third-party network connections
    - Monitoring traffic flows for known threats
    - Blocking undesirable traffic
- DMZ at offshore substation
    - Redundant firewalls for IDS and IPS
    - Secure perimeter for third-party network connections
    - Monitoring traffic flows for known threats
    - NAT for third-party networks
    - Blocking undesirable traffic

Figure 6-8 shows the Firepower design with security zones in wind farms. The Firepowers in different places in the network are managed by a centralized management application called Firepower Management Center (FMC), which is deployed in the control center.

Figure 6-8 Firewall Design in Wind Farm Network Architecture



The following Cisco NGFW features are used in a wind farm network security:

- Standard firewall features:
  - Includes traditional firewall functionalities such as stateful port and protocol inspection, network address translation (NAT), and virtual private network (VPN).
- URL filtering:
  - Set access control rules to filter traffic based on the URL that is used in an HTTP or HTTPS connection. Because HTTPS traffic is encrypted, consider setting SSL decryption policies to decrypt all HTTPS traffic that the NGFW intends to filter.
- Application visibility and control (AVC):
  - Discover network traffic with application-level insight with deep packet visibility into web traffic.
  - Analyze and monitor application usages and anomalies.
  - Build reporting for capacity planning and compliance.
- Next-generation intrusion prevention system (NGIPS):
  - Collected and analyzed data includes information about applications, users, devices, operating systems, and vulnerabilities.
  - Build network maps and host profiles to provide contextual information.
  - Security automation correlates intrusion events with network vulnerabilities.
  - Network weaknesses are analyzed and automatically generate recommended security policies to put in place to address vulnerabilities.
- Advanced malware protection (AMP):
  - Collects global threat intelligence feeds to strengthen defenses and protect against known and emerging threats.
  - Uses that intelligence, coupled with known file signatures, to identify and block policy-violating file types, exploitation attempts, malicious files trying to infiltrate the network.
  - Upon detection of threats, instantly alert security teams with an indication of the threat and detailed information about malware origin, system effects, and what the malware does.
  - Update the global threat intelligence database with new information.

Table 6-3 lists the ports that must be allowed in a firewall to allow external third-party applications to access applications or services in the wind farm network.

Table 6-3 List of allowed Firewall Ports Facing Third-Party Networks

Application	Port Number	References
IPSec tunnel	UDP ports: 500 (ISAKMP), 4500 (NAT-T) ,1701 (L2TP), 10000 IP numbers: 50 (ESP), 51	*Cisco Security Design Guide*: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Grid_Security/DG/DA-GS-DG/DA-GS-DG.html#pgfId-494488
Remote access VPN	TCP ports: 443,80	*Firepower Management Center Configuration Guide*: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security__internet_access__and_communication_ports.html
Internet access (HTTP or HTTPS)	TCP ports: 443,80	*Security, Internet Access, and Communication*: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Security__Internet_Access__and_Communication_Ports.pdf
SCADA OPC-UA (Turbine SCADA network to OSS infrastructure)	TCP ports: 4840,4843, 4990 (See the reference document for various OPC-UA applications)	“Unified Architecture Technology Sample Applications” on the OPC Foundation web site.

Chapter 7: Network Scale and High Availability Summary

Failure of any part of the network (either a network device or a network link) can affect the availability of services. The effect of availability increases with the increase in the aggregation level of the failing node or link. Availability is improved by avoiding a single point of failure by means of high availability (HA) or redundancy. Therefore, every critical component and link in the overall network should have HA or redundancy designed in and configured.

This chapter discusses scale, HA, and redundancy considerations for the entire solution, and includes the following topics:

- FAN Ring Size
- FAN Aggregation Scale
- Network High Availability Summary

FAN Ring Size

A large offshore wind farm with multiple locations can have from 50 to 300 turbines. We recommend that a maximum FAN ring size of no more than 18 switches be configured because Cisco DNA Center automated REP workflow provisioning can support up to a maximum of 18 switches in a REP ring. Form multiple FAN rings of IE3400 turbine base switches when the number of turbines exceeds 18.

FAN Aggregation Scale

Cisco Catalyst 9300 series switches serve as FAN ring aggregation switches. Each switch can have up to 48 ports, and 8 switches can be stacked together to provide scale and redundancy. Each REP ring uses two ports on a 9300 for termination. With a minimum of 2 switches in a stack, up to 24 concurrent rings are supported. Each FAN ring can support a maximum of 18 Cisco Industrial Ethernet switches. For further expansion, either additional switches can be added to the stack or additional switch stacks can be created with Cisco Catalyst 9300 series switches.

We recommend aggregating no more than 10 FAN rings on a stack of dual Catalyst 9300 switches for optimal network performance. If the number of turbines or base switches is greater than 180 (10 FAN rings of 18 nodes each), another stack of dual Catalyst 9300 switches should be added to FAN aggregation network.

Thus, the wind farm FAN ring, FAN aggregation, and OSS and ONSS core systems can be scaled from a small deployment to a large deployment in terms of the number of endpoints connected, bandwidth requirements, and area to be covered.

The scale numbers are summarized below:

- Maximum number of access ports per nacelle or base (IE switch): 26 (IE 3x00)
- Maximum number of nodes per ring: 18
- Maximum bandwidth of a FAN ring: 1 Gbps
- Maximum number of concurrent FAN rings per FAN aggregation stack (one pair of 9300): 10
- Maximum number Cisco Catalyst 9300 switches in a stack: 8 (we recommend configuring a stack of 2 switches)
- Maximum number of Cisco Catalyst 9500 switches in a StackWise Virtual: 2

Network High Availability Summary

TAN High Availability

For information about the high availability design for TANs, see TAN High Availability Design with REP.

FAN Ring High Availability

FAN ring connectivity is provided with Cisco Industrial Ethernet (IE) switches and an REP ring. REP rings provide redundancy for the uplinks of the base switches in a FAN ring. A REP ring network converges within 100 ms and provides an alternate path if a link failure occurs.

For more information about the FAN high availability design, see FAN REP Ring Design.

FAN Aggregation High Availability

High availability is provided at the FAN aggregation layer for the Cisco Catalyst 9300 by configuring Cisco StackWise-480. Cisco StackWise-

480 is an advanced Cisco technology with support for son-stop forwarding with stateful switchover (NSF/SSO) for the most resilient architecture in a stackable (sub-50 ms) solution. For more information, see *Cisco Catalyst 9300 Series Switches Data Sheet*:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

OSS and ONSS Core High Availability

9500 StackWise Virtual

A Cisco Catalyst 9500 at an OSS and ONSS core network differs from the Catalyst 9300 (StackWise 480) insofar as the 9300 has physical backplane stacking cables, with a maximum distance of 30 ft (10 m) between switches in a stack, whereas the Catalyst 9500 (StackWise Virtual) uses Ethernet interfaces and can be split across much greater distances.

The StackWise Virtual Link (SVL) is typically made up of multiple 10 or 40 Gbps interfaces, associated transceivers (for example, SFP+/QSFP), and cabling. These items are dedicated to the SVL and provide a virtual backplane between the two physical Catalyst 9500 switches. They cannot be used for any other purpose. In a wind farm, we recommend having two physical SVL links, and one dual-active detection (DAD) link.

For more information about SVL, see *High Availability Configuration Guide, Cisco IOS XE Dublin 17.10.x (Catalyst 9500 Switches)*:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-10/configuration_guide/ha/b_1710_ha_9500_cg/configuring_cisco_stackwise_virtual.html

Wireless High Availability

Catalyst 9800 WLC HA

For information about Cisco C9800 WLC high availability configuration, see *High Availability SSO Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Amsterdam 17.1*:

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-ha-sso-deployment-guide-rel-17-1.pdf

C9800 WLC HA can also be configured using the prebuilt DNA-C workflow. Sample configuration and steps are provided in *Cisco Wind Farm Solution Implementation Guide*.

URWB FM1000

For information about gateway FM1000 redundancy deployment. See CURWB Wireless Backhaul.

Management High Availability

Redundancy should be configured for various critical servers in the network, such as Cisco DNA Center, ISE, FND, DHCP, DNAC, and CA. The Cisco DNA Center supports inherent redundancy within cluster.

Cisco DNA Center Redundancy

Cisco DNA Center redundancy is provided by clustering three Cisco DNA Center appliances together. Clustering provides for sharing of resources and features and helps enable high availability and scalability. The Cisco DNA Center supports single-host or three-hosts cluster configurations.

The three-hosts cluster provides both software and hardware high availability. The three-nodes cluster can inherently do service and load distribution, database replication, and security replication. This cluster survives the loss of a single node.

The single host cluster does not provide hardware high availability. Therefore, we recommend using a three hosts cluster for wind farm Cisco DNA Center high availability deployments. For more detailed information, see *Cisco DNA Center High Availability Guide*:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/ha_guide/b_cisco_dna_center_ha_guide_2_3_5.html

If the Cisco DNA Center appliance becomes unavailable, the network still functions, but automated provisioning and network monitoring capabilities are not possible until the appliance or cluster is repaired or restored.

Cisco ISE Redundancy

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary administration ISE node to manage the secondary ISE nodes that are deployed in the network. For more detailed information, see *Cisco Identity Services Engine Administrator Guide*:

https://www.cisco.com/c/en/us/td/docs/security/ise/3-2/admin_guide/b_ise_admin_3_2/b_ISE_admin_32_deployment.html

NGFW Redundancy

Configuring high availability, also called failover, requires two identical Firepower Threat Defense devices connected to each other through a dedicated failover link and, optionally, a state link. Firepower Threat Defense supports active and standby failover, where one unit is the active unit and passes traffic. The standby unit does not actively pass traffic but synchronizes configuration and other state information from the active unit. When a failover occurs, the active unit fails over to the standby unit, which then becomes active.

For more detailed information, see *Cisco Secure Firewall Management Center Device Configuration Guide*:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73/high-availability.html

Cisco SD-WAN Redundancy

Cisco SD-WAN redundancy is achieved in different ways, depending on the SD-WAN components. We recommend the cloud-hosted deployment for Cisco SD-WAN controllers, which provides an easy way to deploy and scale with high availability.

Cisco vBond Orchestrator

Cisco vBond orchestrator redundancy is achieved by spinning up multiple Cisco vBond controllers and using a single fully qualified domain name (FQDN) to reference the Cisco vBond controllers. To maintain proper redundancy, we recommended using Cisco vBond orchestrators in different geographic regions if they are managed from the cloud, or in different geographic locations or data centers if they are deployed on premises. This approach ensures that at least one Cisco vBond controller is always available when a Cisco SD-WAN managed device attempts to join the network.

Cisco vSmart Controller

For Cisco vSmart controllers, redundancy is achieved by adding additional controllers which act in an active/active fashion. To maintain proper redundancy, we recommend using Cisco vSmart controllers in different geographic regions if they are managed from the cloud, or in different geographic locations or data centers if they are deployed on premises.

Cisco vManage Clustering

A Cisco vManage cluster can distribute various NMS service loads and provide high availability and scalability for the Cisco vManage services. A Cisco vManage cluster consists of at least three Cisco vManage server instances, with each instance active and running independently. Control connections between the Cisco vManage servers and WAN routers are load balanced. Control connections (from each Cisco vManage instance to each Cisco vSmart controller from each Cisco vManage instance to each other Cisco vManage instance, and from each Cisco vManage instance core to each Cisco vBond orchestrator) are fully meshed.

For more detailed information about Cisco SD-WAN high availability design, *see Cisco Secure Firewall Management Center Device Configuration Guide*:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

Chapter 8: Conclusion

Cisco is a global leader in industrial networking and provides a wide range of products to address the offshore renewable energy market. By applying our secure and hardened industrial networking, IoT expertise, and experience working with industry leaders to address challenges existing in the industry, we have created innovative technology solutions that optimize and secure renewable energy assets.

Our goal is to future-proof your investment by providing an evolution path from today's isolated deployments to secure, connected renewable energy deployments that support the energy needs of today and tomorrow.

Since the inception of IP networking, Cisco Validated Designs (CVDs) have been used to validate, architect, and configure industry best practices and technology solutions. CVDs start with solution use cases and architect the flow from the edge device to the application, validating key Cisco and third-party components along the way. Each aspect of the architecture is thoroughly tested and documented with sample configurations, helping to simplify integration and de-risk implementations through proven solutions.

The goal is to ensure a deployment and a solution that's simple, fast, reliable, secure, and cost effective. Cisco developed renewable energy network solutions to specifically address the networking and security needs of renewable energy asset operators.

Acronyms and Initialisms

The following table summarizes the acronyms and initialisms used in this document.

Term	Definition
AAA	Authentication, authorization, and accounting
ACL	Access control list
AD	Active Directory
ADM	Axis Device Manager
AIS	Automatic identification system
AP	Access point
AMP	Advanced malware protection
ARP	Address resolution protocol
AVC	Application visibility and control
BGP	Border gateway protocol
BS	(Turbine) base switch
BW	Bandwidth
CA	Certificate authority
CBWFQ	Class-based weighted fair queuing
CC	Control center
CCTV	Closed circuit television
CDN	Cisco Developer Network
CE	Carrier Ethernet
CLI	Command line interface
Cisco DNAC	Cisco Digital Network Architecture Center
CoS	Class of service
CTS	Cisco TrustSec
CURWB	Cisco Ultra Reliable Wireless Backhaul
CV	(Cisco) Cyber Vision
CVC	Cisco Cyber Vision Center
CVD	Cisco Validated Design
DAD	Dual active detection
DC	Data center
DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DNS	Domain name system
DODAG	Destination oriented directed acrylic graph
DoS	Denial of service

Term	Definition
DSCP	Differentiated services code point
ECC	Elliptic curve cryptography
ECMP	Equal-cost multi path
EIGRP	Enhanced interior gateway routing protocol
EN	Extended nodes
EPs	Endpoints
FAN	Field area network
FAR	Field area routers
FC	Fiber channel
FCAPS	Enhanced fault, configuration, accounting, performance, and security
FM	FluidMesh
FMC	Firepower Management Center
FNF	Flexible NetFlow
FP	Firepower
FW	Firewall
HA	High availability
HER	Headend router
HMI	Human machine interface
HSRP	Hot standby touter protocol
HQ	Headquarter
HQoS	Hierarchical quality of service
IA	Industrial automation
IE	(Cisco) Industrial Ethernet
IEC	International Electrotechnical Commission
IED	Intelligent end device
IKE	Internet key exchange
IOT	Internet of things
I/O	Input and output device
IP	Internet protocol
IPSec	Internet protocol security
IR	(Cisco) Industrial Routers
ISE	(Cisco) Identity Services Engine
IT	Information technology

Term	Definition
L3VPN	Layer 3 virtual private network
LAN	Local area network
4G LTE	Fourth generation long-term evolution
MAC	Media access control
MQC	Modular QoS CLI
ME	Mesh end
MMS	Manufacturing message specification
MPLS	Multi-protocol label switching
MP	Mesh point
MRP	Media redundancy protocol
MTU	Maximum transmission unit
NAT	Network address translation
NBAR2	Cisco Next Generation Network-Based Application Recognition
NGFW	Next general firewall
NGIPS	Next-Generation Intrusion Prevention System
NMS	Network management system
NOC	Network operation center
NS	(Turbine) nacelle switch
NTP	Network time protocol
OAM	Operations, administration, and management
OEM	Original equipment manufacturer
OFTO	Offshore transmission owner
OPC UA	Open Platform Communications Unified Architecture
OSPF	Open shortest path first
OSS	Offshore substation
ONSS	Onshore substation
OT	Operational technology
PAN	Policy administration node; personal area networks
PAgP	Port aggregated protocol
PHB	Per hop behavior
PEP	Policy enforcement point
PKI	Public key infrastructure
PLC	Power line communication
PnP	Plug-and-play
PoP	Point of presence
PoE	Power over Ethernet
PQ	Priority queuing
PRP	Parallel redundancy protocol
PSN	Policy services node

Term	Definition
pxGrid	Platform eXchange grid
QoS	Quality of service
RADIUS	Remote authentication dial-In user service
REP	Resilient Ethernet protocol
RTU	Remote terminal unit
SA	Substation automation
SCADA	Supervisory control and ta acquisition
SD-WAN	Software-defined wide area network
SFC	Secure Network Analytics Flow Collector
SGTs	Security group tags
SGACL	Security group-based access control list
SLC	Street light controller
SMC	Secure network analytics management console
SOV	Service operations vessel
SSID	Service set identifier
SSM	Software security module
STP	Spanning tree protocol
SVI	Switched virtual interface
SVL	StackWise virtual link
SXP	SGT eXchange protocol
TAN	Turbine area network
TBN	Turbine base network
TCP	Transmission control protocol
TFTP	Trivial file transfer protocol
TLS	Transport layer security
TLV	Type length value
UCS	Cisco Unified Computing System
UDP	User datagram protocol
UHF	Ultra-high frequency

Term	Definition
VHF	Very high frequency
VN	Virtual network
VoD	Video-on-demand
VoIP	Voice over internet protocol
VRF	Virtual routing and forwarding
VLAN	Virtual LAN
VPN	Virtual private network
WAN	Wide area network
WF	Wind farm
Wi-Fi	Wireless fidelity
WLC	Wireless LAN controller
WLAN	Wireless local area network
WPAN	Wireless personal area network
WRED	Weighted random early detect
WTD	Weighted tail drop
WTG	Wind turbine generator
ZTD	Zero touch deployment
ZTP	Zero touch provisioning