Connected Ports and Terminals Design Guide

First Published: 2013-08-02

Last Modified: 2023-05-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Connected Ports and Terminals: Overview and Network Requirements

Ports play an important role in promoting international trade and regional development. Ports are catalysts for economic development as they enable trade and support supply chains. Operational efficiency is crucial for ports, given that seaborne trade accounted for 80% of the total volume and 70% by value of global trade in 2016. See "The Role of the Port in International Trade" on the World Bank Group eLibrary website.

Overview

There are various kinds of ports—container ports, bulk ports, dry ports, cruise ship ports, and passenger ports. The subject of this guide is container ports.

The key challenges for ports and terminals include:

- Growing volume of operations. Operation data volume is up 210% from 2021, which demands reliable and scalable infrastructure.
- Cyber security OT and IT concerns.
- Increasing labor costs.
- Heavy labor intensity, harsh working environments, and insufficient personnel.
- Improving workplace safety and security to mitigate risk (loss prevention, worker safety).
- Meeting regulatory requirements—sustainability and environmental targets

Reducing costs and improving efficiency through automation have become the industry's overarching goals. Digital innovations and artificial intelligence (AI), big data, Internet of Things (IoT), autonomous vehicles, and tele-remote operations provide new impetus for port automation.

Higher levels of automation are being used at container terminals to help improve productivity and efficiency, and ensure competitiveness. As the shipping throughput increases year after year, global ports and terminals are undergoing reconstruction to achieve a higher level or automation. As congestion concerns and demand for transport services increase, advanced automation is being implemented as one tool to improve port and terminal operations.

Smart ports and terminals require communications systems that support low latency, high bandwidth, low loss, and high reliability communication services to handle control data, safety systems, and multichannel video data of port equipment.

Ports and Terminals Digital Transformation

There is an overwhelming trend for better integration of ports into the extended supply and value chain, from transport and intermodal facilities, all the way to the customer—port authorities, customs, quarantine, services, transport authorities, and so on.

The decision to automate a port is based on the relentless drive for effective, efficient, fast, and continuously monitored supply chain processes. Full automation enables port and terminal managers to meet and exceed client requests and market demands, while allowing flexibility and dependability.

Smart ports and terminals require communications systems that support low latency, high bandwidth, low loss, and high reliability communication services to handle control data, safety systems, and multichannel video data of port equipment.

Advantages of Automating Ports and Terminals

As congestion concerns and demand for transport services increase, advanced automation is being implemented as one tool to improve port operations. Some advantages of automating ports and terminalsare:

- Operational and maintenance cost savings
- Improved efficiency and availability
- Improved worker safety
- Reduced environmental impact in terms of reduced emissions and noise pollution
- Reduced labor cost
- Increased revenue from decreased downtime

Ports and Terminals Use Cases

Terminal Operating System

There is a strong trend toward remote operations of terminal operations—centralizing expertise and skills, increasing safety by removing people from hazardous operational areas, and reducing costs. The Terminal Operating System (TOS) software controls the logistics of a terminal, including key functions such as vessel planning, container inventory maintenance, job order creation, and gate operations. TOS software is provided by several commercial companies and many terminal operators themselves. In a modern container terminal, some container handling equipment (CHE) may be uncrewed and operated by a computer and navigation system (autonomous operations) while other parts of them may be manually operated. The manual operation consists of two different modes:

- The operator physically sits inside a cabin on the vehicle
- The vehicle is remotely operated from a central control room (tele-remote)

There is little difference between these modes for the TOS. However, where differences occur, it is usually where remote drivers improvise container moves from a computer room.

Several advanced TOSs are available that provide functions to control operations in a yard and interfaces to interact with CHE. The TOS precalculates and creates stacking jobs using rubber tired gantry cranes (RTG) or rail-mounted gantry cranes (RMG), or transport jobs using automated straddle carriers (AutoSC) for CHE. The TOS also controls the execution of respective jobs or a certain sequence of jobs.

Typical features of a TOS influencing the operation of CHE are:

- Standard handling and sequence of stacking activities for CHE
- Management of stacking or put-away rules in the yard
- Container target positions on the yard
- Working areas for handling equipment
- Pooling of CHE in working areas
- Load balancing of jobs over equipment per working area
- Position dsection and calculation of travel distances
- Sending and control stacking and transport jobs to selected CHE
- Calculating necessary shifting jobs

In brownfield automation projects, automated handling equipment needs to be integrated with the TOS and into existing conventional equipment still in use. In a conventional terminal environment with human operated, nonautomated equipment, the typical interface between the TOS and the handling equipment is a job control monitor installed on a vehicle-mounted terminal (VMT) in the cabin of a crane. The operator sees the next job on the monitor, and can select, execute, and confirm tasks accordingly.

To enable applications such as TOS, tele-remote, or OCR, all the vehicles need to have network connectivity. For the occasional exception where a vehicle can have fiber connectivity, the connectivity to the vehicles needs to be provided using a highly reliable and secure wireless link. The wireless technology must also provide seamless handoffs with minimal latency and packet loss between various infrastructure access points around the terminal as the vehicles move around to accomplish their tasks.

Tele-Remote Operations

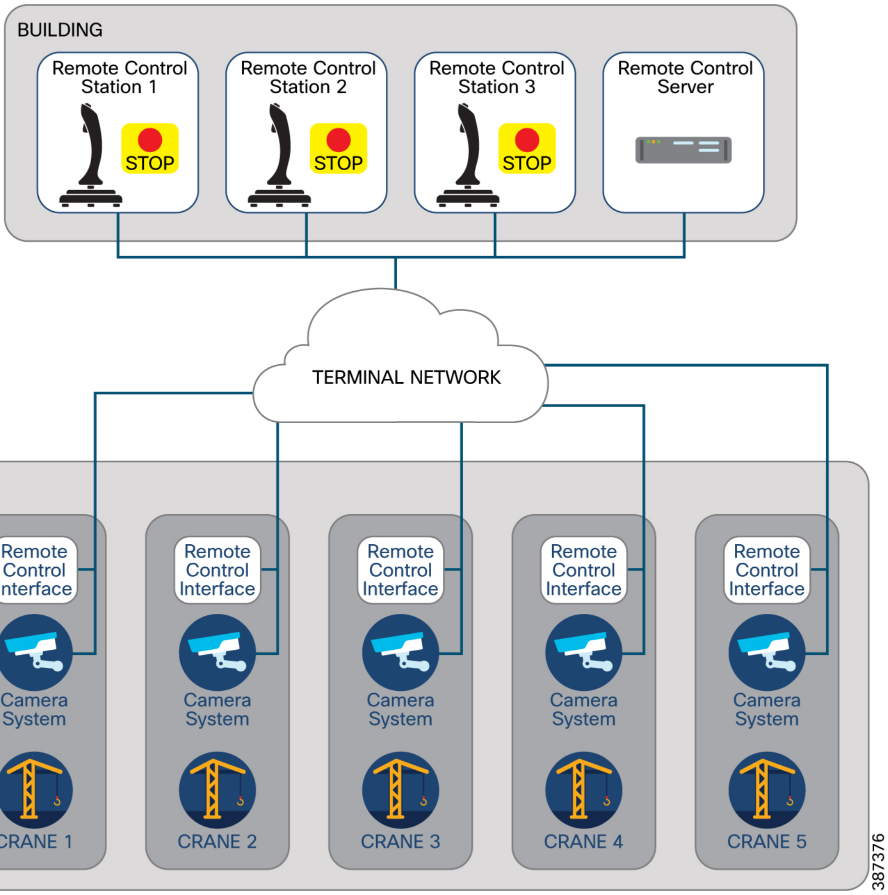
As the pressure mounts to improve efficiency, safety, and the port environmental footprint, the means to achieve these goals are already within reach. And it is not about reducing headcount.

Port operations and logistics have significantly changed over the years, yet the core of this line of work remains dangerous, polluting, and repetitive. Autonomous technologies and teleoperation can change the nature of industrial drudgery, increasing productivity and efficiency, while reducing its harmful nature to employees and to the environment.

Tele-remote operations and a remote operation center (ROC) enable operators to control container cranes from the safety and comfort of a remote location. They deliver a complete crane control solution from operator login, through carrying out operations, to operator logout. The remote-control station (RCS) location can be anywhere if the RCS prerequisites, such as network requirements, are considered.

RCS assists operators with performing their control tasks by presenting task-dependent information on a customized human-machine interface.

Figure 1: Tele-Remote Operations



The remote control operation system typically consists of:

- One or several RCSs
- One RCS server
- One ROS interface per crane
- Several cameras per crane

The operator uses the human machine interface (HMI) on the RCS to control a crane from a remote location. To provide situational awareness to the operator, the RCS HMI provides live video streams from the remote-controlled crane combined with graphical information.

The operator controls the crane using hardware and software controls. The hardware controls should include an emergency stop push button, master controllers for controlling crane movement, and buttons for frequently used crane functions.

Use Cases and Advantages of Tele-Remote Operations within Ports and Terminals

Tele-remote operations in ports can be used in two main scenarios. In the first scenario, one operator to directly control one vehicle continuously throughout the completion of a task. The vehicle doesn't have to be an autonomous vehicle, although it requires integration to a teleoperation kit. In this scenario, the vehicle can be used to conduct hazardous activities, such as operating a tractor in the belly of a coal ship, or conduct nonroutine operations that aren't relevant for autonomous operations, such as short distance transport by terminal tractors.

In the second scenario, tele-remote operation can support autonomous vehicles such as terminal tractors, forklifts, and trucks that mostly operate autonomously. Tele-remote operation allows these vehicles to navigate edge cases that require human intervention for situations such as abnormal stops, lost self positioning, incomplete jobs, or changes to the operational environment. In this scenario, one operator can support several vehicles as each vehicle requires the human operator attention only for a few moments at a time. After vehicles receive that help, they continue autonomously.

Although autonomous vehicle technology is advancing toward providing a complete solution for all logistics and port operation scenarios, for the foreseeable future, it's easier and safer to have a human help operate these vehicles remotely by using tele-remote operation technology.

The advantages of tele-remote operation go beyond economic efficiencies and safety as they can also contribute to reductions in emissions. Tele-remote operated vehicles require less energy and operate fewer hours. They don't need to run air conditioning or heating, and they don't need to transport a driver back and forth around the port, as their operators control the vehicles from the comfort of their offices.

Ports and Terminals Network Requirements

Reliable, resilient, and secure data transfer is especially important when introducing remote-controlled or automated solutions. Video data has to be transferred as real-time data for the operator to be able to control equipment remotely. Fiber is the preferred connectivity mode when reliability is concerned, however even fiber has difficulty providing high availability (HA) and reliable service to mobile assets.

Examples of where fiber is problematic in mobile assets are quay cranes and overhead gantry cranes that employ rotary fiber couplers (typically within high voltage power cables) that deteriorate over time. Radio networks are therfore an essential component for network connectivity within ports and terminals. All network technology needs to be designed appropriately for HA environments. Radio systems have evolved over time to offer better HA capabilities.

TOS

Terminal operating system (TOS) is a store and forward system, therefore any information collected or retrieved is stored for delivery at the first opportunity of connection. The bandwidth requirements for a TOS system are typically less than 1 Mbps per vehicle. The latency requirements less stringent than requirements for the other applications such as automated guided vehicles (AGVs), tele-remote operations, optical character recognition (OCR), and video surveillance.

Autonomous and Tele-Remote Operations

Autonomous and tele-remote operation for vehicles around a terminal requires the network link to support high throughput: 30 Mbps for AutoSCs and 60 Mbps for RTGs, with a maximum latency of 30 ms. The traffic consists of a combination of PLC control traffic and live video feeds to allow a remote operator to view the terrain.

Remote Control of Gantry Cranes

A single gantry crane needs to upload anywhere between 5 and 16 channels of surveillance videos, and 1080p videos requiring a cumulative bandwidth of around 30 Mbps. In addition, PLC communications between the central control room and a gantry crane require a network latency of less than 50 ms. In a typical deployment, about 60 gantry cranes are deployed within a 1 square Km area. The handoff requirements vary by manufacturer, with most requiring handover times of less than 50 ms and some requiring less than 10 ms.

Remote Control of Ship-to-Shore and Quay Cranes

The main service unit in the berth and quay area is the ship-to-shore(STS)/quay crane. The height of a quay crane is 200 to 230 ft (60 to 70 m) and wireless networks are required to provide network coverage in operation areas. Quayside container cranes have communication requirements for both remote control and monitoring. In the remote-control scenario, there are more than 20 cameras on a single quayside container crane and the uplink bandwidth is estimated to be up to 50 Mbps. In addition, the deployment of quayside container cranes is relatively dense. Typically, 8 to 12 cranes are deployed along a 1 km port coastline.

Because most container terminals are built along seashores, berths must be sufficiently submerged in water and may be equipped with bollards and fenders. Therefore, wireless network devices need to serve the production and monitoring purposes of quayside container cranes and TOS components, while providing network coverage for berthing vessels in some cases.

Automated Horizontal Transport

When designing a network to be used by any kind of autonomous horizontal transport system, such as automated stacking cranes or automated guided vehicles (AGVs), coverage must be guaranteed across the entire working zone by facilitating overlapping radio coverage zones from the infrastructure radios. Bandwidth requirements are comparatively low (approximately 1 Mbps for an AutoSC or AGV), however interruptions in signal and gaps during handover are not acceptable. There is constant data traffic to and from on-board PLCs, and interruptions in data flow cause the relevant solution to experience operational delays, or in extreme cases might stop the operation altogether.

Optical Character Recognition

Optical character recognition (OCR) is an automated identification and data collection (AIDC) technology. It is often used in modern ports and terminals to identify and track containers. OCR systems that process data locally on the cranes or RMGs do not require a high amount of bandwidth, a constant connection. and continuous stream of data. Only if OCR needs to be processed off machine and live is a constant connection needed and a higher throughput of 15 to 20 Mbps required. Interruptions in received signal and gaps during handovers are not acceptable because these gaps may cause the relevant equipment to experience operational delays. Network latency must not exceed 50 ms.

Summary of Wireless Requirements

Table 1: Terminal Automation Wireless Network Requirements

Use Case	Overall Requirement	Wireless Network KPI Requirements			
		Latency	Bandwidth	Reliability	RF Coverage
Terminal operating system (TOS)	Low bandwidth, high reliability	Less than 1 second	450 Kbps to 1 Mbps	99.999%	Good port-wide coverage
Autonomous and tele-remote operations	Low latency, high reliability, constant PLC traffic	Less than 50 ms	30 Mbps for AutoSC 60 Mbps for RTG	99.9%	Coverage across the working area
Autonomous horizontal transport (automation for PLC applications)	Low bandwidth, low latency	Less than 50 ms	Approximately 1 Mbps for AutoSC/AGV	99.999%	Overlapping coverage across the working area
Off-machine live optical character recognition (OCR)	High bandwidth	Less than 50 ms	15 to 20 Mbps	99.999%	100% coverage

A terminal automation network requires a flexible and reliable wireless technology that can provide full coverage, extremely low latency, zero packet loss, fast handoff, high bandwidth, and easy installation, provisioning, and management. The Cisco Ultra-Reliable Wireless Backhaul technology (CURWB) is designed with such requirements in mind and delivers unique capabilities, as outlined in Chapter 3, to overcome these challenges and satisfy the stringent requirements.

There are other wireless use cases within the port and terminal vertical, such as mobile worker communication with the terminal and on the ship, drone surveillance, connectivity for IoT sensors, and so on. However, these use cases are outside the scope of this document.

CHAPTER 2

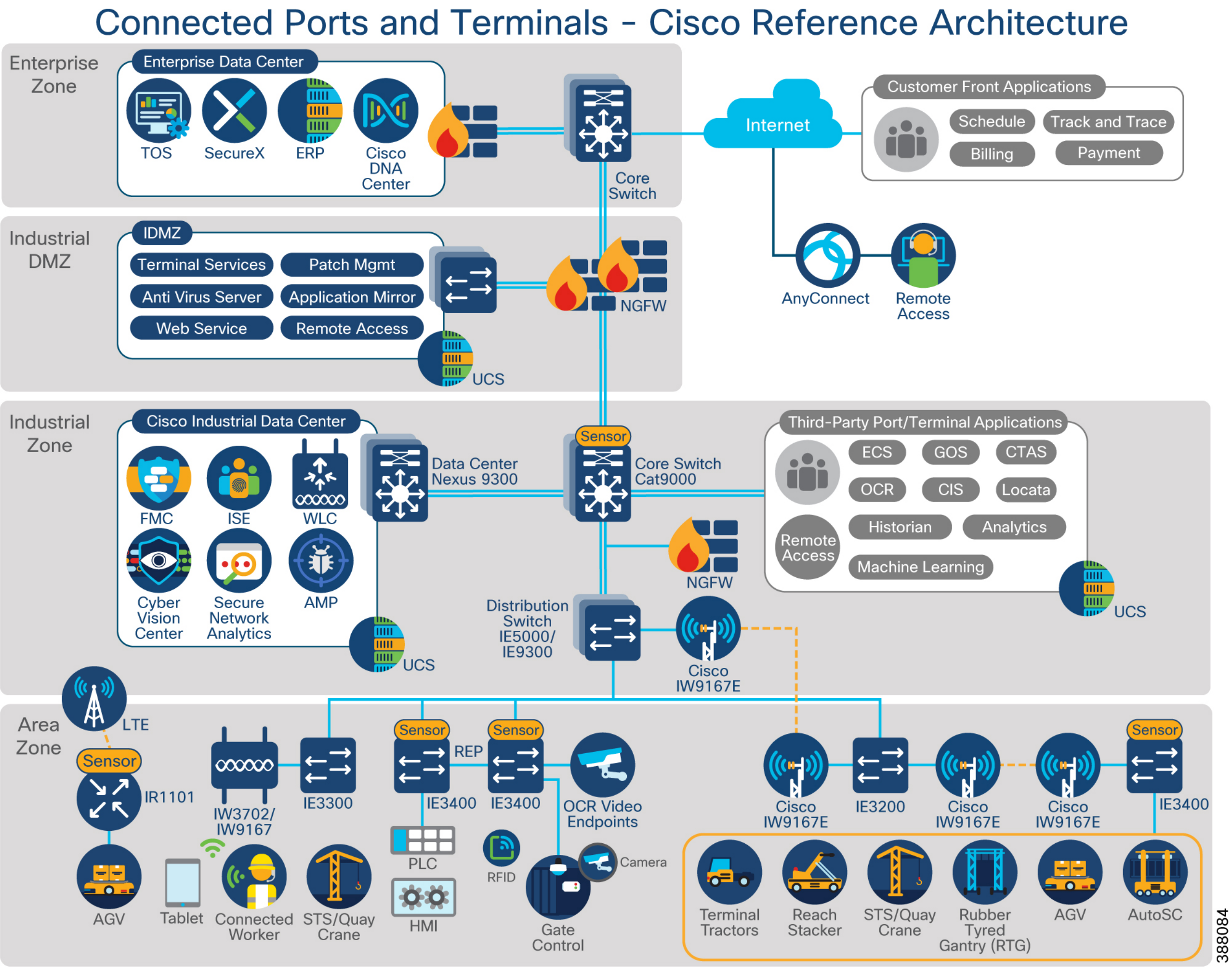
Connected Ports and Terminals: Reference Architecture

This chapter provides an overview of a recommended design for a ports and terminals network deployment. It also covers OT security considerations for this deployment.

High-Level Network Design

The Cisco connected ports and terminals reference architecture, depicted in the following figure, follows the blueprint of ISA-95 and is based on the Cisco reference architecture for Industrial Automation and Control Systems (IACS). This reference architecture is composed of four major functional modules: the Industrial Zone, Area Zone, Enterprise Zone, and Industrial Demilitarized Zone (Industrial DMZ). The following sections explain the functions and capabilities of each module in more detail.

Figure 2: Connected Ports and Terminals—Cisco Reference Design



Industrial Zone

The Industrial Zone is important because all applications, devices, and controllers that are critical to monitoring and controlling terminal operations reside within this zone. To enable smooth and secure operations and functioning of the ports and terminals applications and devices, the Industrial Zone requires clear logical segmentation and protection from the Enterprise Zone.

The Industrial Zone in this architecture refers to a zone that all industrial and mission-critical port and terminal applications are confined to. It is composed of a Cisco industrial data center and third-party port and terminal application services. Due to the sensitive nature of the assets and data flow in the Industrial Zone, a pair of redundant firewalls located in the Industrial DMZ blocks all traffic in and out of the Industrial Zone and allows only traffic that is explicitly defined. This configuration may cause a challenge when communication patterns are not well understood, particularly in cases where communication between the Industrial Zone and the upper levels is required. For this reason, application visibility is important. Technologies such as Cisco Cyber Vision and Secure Network Analytics can be beneficial in this regard.

The Cisco industrial data center follows the best practices of Cisco data center design. The platform choice of the Cisco Catalyst 9000 family for the Industrial Zone core switch and the Cisco Nexus 9300 for the data center switch enables Cisco intent-based networking with Cisco DNA Center management and data center solutions such as Cisco Application Centric Infrastructure (Cisco ACI). To minimize the need for communication between Level 3 (the Industrial Zone in the industrial automation reference architecture) and upper levels, key infrastructure services should be located within the industrial data center. These services include dedicated identity services such as Active Directory (AD) and Cisco Identity Services Engine (ISE), dedicated wireless controllers to manage wireless connections within the Industrial Zone, and Cyber Vision and Secure Network Analytics to gain visibility into the production asset and application flows. ACI or Cisco Secure Workload also provide application security compliance, flow visibility, and layered segmentation of compute-based control systems outlined in IEC 62443-3.

Third-party applications that are responsible for port and terminal operations are in the server farms at the industrial data center, which is in the Industrial Zone. These applications include equipment control systems, crane interface systems, OCR servers, container terminal automation systems, and gate operating systems. By having these essential services and applications located in the Industrial Zone, the operation is less likely to be disrupted if external connectivity via the Industrial DMZ is lost or the upper-level network is brought down by a cyber attack. We recommend that NGFW be introduced in the network for northbound communication, such as between the industrial data center and Area Zones for advanced threat protection between devices that pose a higher security threat but would not cause production downtime if security were prioritized over connectivity.

The site operations and control level generally are carpeted spaces, meaning that they have HVAC with typical 19 inch rack-mounted equipment in hot and cold aisles utilizing commercial grade equipment. These areas are where applications that are related to port and terminal operations reside. Examples of services at this level are historians, control applications, TOS, OCR, gate control, video surveillance, and network security services. The systems and applications that exist at this level manage terminal-wide operations. These operations typically need to be up and running 24 x 7 and any downtime has a huge and direct impact on revenue and end-customer satisfaction.

The applications within the Industrial Zone need to communicate with devices in the Area Zone. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). For this reason, these systems are more likely to communicate using standard Ethernet and IP networking protocols.

Additionally, because these systems tend to be more aligned with standard IT technologies, they may be implemented and supported by personnel with IT skill sets.

Area Zone

The Area Zone is the access layer located at the edge of the industrial network that provides either wired or wireless connectivity to industrial devices. These devices include industrial devices at Levels 0 through Level 2 in the ISA-95 model, such as actuators, controllers, and sensors that communicate via traditional control protocols such as PROFINET. They also include devices such as Wi-Fi or Bluetooth-enabled handheld devices, voice communication radios, access points, cameras, vehicle telemetry sensors, and weather sensors that use traditional network protocols such as IP or serial links for communications.

The Area Zone module delivers the following important characteristics:

- Industrial characteristics: The platform choices are heavily influenced by the environmental conditions at the port and terminal. The Cisco IoT product portfolio delivers hardware that is hardened with a small form factor, can sustain an extended temperature range and shock and vibration, and provides protection against water and dust ingress. Industrial control protocols such as PROFINET and EtherNet/IP are supported natively on the Cisco Catalyst Industrial Ethernet (IE) switches.

- Multiple access technologies: Depending on the application requirements, deployment scenario, and existing network infrastructure, multiple access technologies, including wired and wireless, might be needed for successful operations. The Cisco IoT wireless portfolio includes LTE and 5G, suitable for wide mobility and high throughput; Wi-Fi 6 and Cisco Ultra-Reliable Wireless Backhaul for mobility and fixed infrastructure with high throughput, low latency, and ultrareliable, resilient mesh; and LoRaWAN for massive scale and broad coverage. The Cisco IoT wired product line offers Ethernet connections over copper or fiber, and serial and DSL connections from Internet service providers.

- Highly resilient network: An IACS network must be highly resilient, with latency, reliability, scalability, and performance considered in the network design. For industrial control traffic, packet latency, loss, and jitter have a significant impact on the underlying industrial process. Network availability and convergence time are also key metrics for critical IACS communication. The Cisco Resilient Ethernet Protocol (REP) available on IE switches typically is suitable for IACS applications that can tolerate up to a 100 ms network convergence recovery time. When zero-second convergence time is required, parallel redundancy protocol (PRP) or high-availability seamless redundancy (HSR) can also be used and are supported on the Cisco Catalyst IE3400, IE4000, and IE5000 Series.

- Security: Security in the Area Zone needs to be viewed as a subset of the overall end-to-end security architecture within the port and terminal. It is critical that security capabilities span the breadth of the port and terminal to be effective, yet this requirement may pose a challenge when the IT and OT are not well integrated and are managed by different groups. The fundamental requirements are visibility into current network devices and industrial assets; grouping and separation of network assets and applications through segmentation; anomaly detection and mitigation; and network hardening on the management plane, control plane, and data plane. Meeting these requirements can be achieved through Cisco Cyber Vision, Cisco TrustSec, and Cisco Secure Network Analytics, and their integration with Cisco ISE. Also, at the application layer, within the control layers of ISA 95, ACI or Cisco Secure Workload can provide interapplication and application to control asset security.

The Area Zone is where the most critical operations for a port and terminal take place. These operations include container loading and unloading, container movement, container storage, container tracking, and so on. Commonly used handling equipment in container ports include the following:

- STS/quay cranes perform loading and unloading activities between vessels and quayside

- Straddle carriers (AutoSCs) pick up and transport containers between quayside and storage yard

- AGVs are used to transport containers between quayside and storage yard

- RMG cranes are used for container acceptance, delivery, and stacking operations in a storage yard or rail terminal

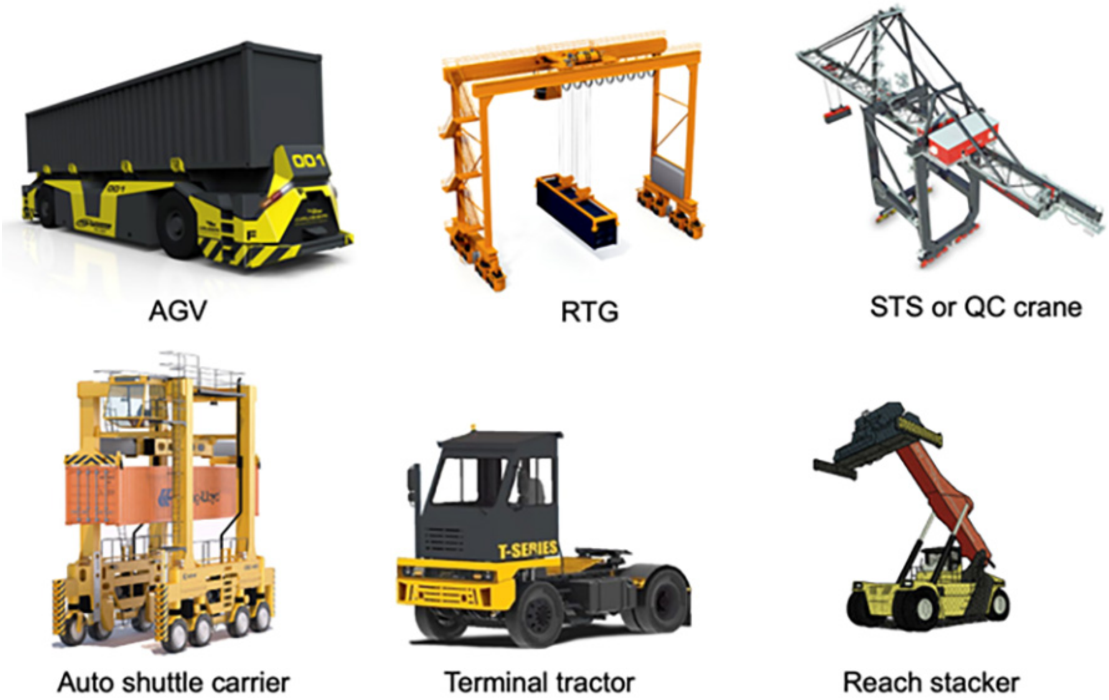
- RTG cranes are typically used for acceptance, delivery, and stacking at a storage yard

- Reach-stackers (RSs) are vehicles used to transport a container for short distances and load and unload containers on or off a truck or train

- Top lifters are lift trucks that can use their spreaders to lift a container

- Sideloaders are lift trucks that are fitted with lifting attachments operating on one side for handling containers

Figure 3: Vehicles and Handling Equipment Used in Typical Port and Terminals Operations



The vehicles and handling equipment listed above can be operated manually, semiautonomously, or in a fully autonomous mode. Most of them also need to integrate with TOS to receive their schedules and sets of instructions. A ruggedized tablet (typically running a Windows OS) is installed within each of these vehicles and handling equipment and needs connectivity to the TOS server installed in the site control room. A few TOS vendors have also started hosting the TOS server in the cloud. In these scenarios, secure cloud connectivity is needed to the cloud. Where remote operation is used, these vehicles and handling equipment also house cameras. In rare cases where the TOS application server is hosted within the enterprise data center, the appropriate ports need to be opened to allow TOS traffic to traverse between the vehicle or handling equipment and the TOS server on both the DMZ and enterprise firewalls.

Gate control systems are used to process entry and exit of external trucks to retrieve or deliver containers by connecting the hinterland road to the storage yard. Network connectivity needs to be provided to each of the gates to transport control information to the gate from the gate control system located in the Industrial Zone and transport video feeds from the gate to the gate control system. Most likely, interaction also is needed between the TOS application and the gate control system. The network connectivity to each gate can be achieved by using a fiber or a wireless link.

Three other important zones where network connectivity needs to be provided are:

- Weighbridge
- Container turnaround area
- Truck waiting area

An in-depth overview of the wireless design and deployment best practices to support TOS applications is covered in the following chapters.

Entperprise Zone

The Enterprise Zone is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level. Often, the external partner or guest access systems exist here, although it is not uncommon to find them in lower levels of the framework to gain flexibility that may be difficult to achieve at the enterprise level. However, this approach may lead to significant security risks if not implemented within IT security policy and standards.

The ports and terminals applications and systems must communicate with the enterprise applications to exchange operational data. Direct access to the ports and terminals applications typically is not required. One exception is remote access to the terminal equipment for management (configuration, troubleshooting) by employees or partners such as system integrators and machine builders. Access to data and the operations network must be managed and controlled through an industrial DMZ to maintain the security, availability, and stability of the operations network.

The services, systems, and applications at this level are directly managed and operated by the IT organization.

Industrial DMZ

Although not part of the Purdue reference model, a reference architecture for the automated manufacturing industry, the design includes a DMZ between the Industrial and Enterprise Zones. The industrial DMZ is inserted to separate the enterprise networks and the operational domain of the ports and terminals environment. Downtime in the operations network can be costly and have a severe affect on revenue, so the operational zone cannot be affected by any outside influences. Network access is not permitted directly between the Enterprise Zone and the Industrial Zone. However, data and services are required to be shared between the zones. Thus, the industrial DMZ provides an architecture for the secure transport of data between the Industrial and Enterprise Zones. Typical services deployed in the Industrial DMZ include remote access servers and mirrored services such as Windows update servers, antivirus servers, and so on.

As with IT network DMZs, the industrial DMZ serves primarily as a buffer between the ports and terminals operations area and the enterprise or the Internet, placing the most vulnerable services, such as email, web, and DNS servers, in this isolated network. The industrial DMZ not only isolates the port operations network from the outside world, but also from its own enterprise networks. The primary reason that this additional isolation is recommended is that, unlike enterprise services, the port operations area contains the most critical and revenue generating part of the business. Often, devices and applications that are used within the ports and terminals operations area are antiquated, running on vulnerable operating systems such as Windows 95. The industrial DMZ provides another level of security for these vulnerable systems.

Another key use of the industrial DMZ is for remote access, aiding in remote configuration and troubleshooting of production equipment that is deployed within a ports and terminals operation. The industrial DMZ hosts the jump servers that can be logged into to access equipment within the terminals operations area.

Wired Network Components

Cisco Catalyst 9300 Access Layer Switch

Figure 4: Cisco Catalyst 9300 Access Layer Switch

The Cisco Catalyst 9300 Series Switches are the next generation of enterprise-class, stackable, aggregation layer switches. They provide full convergence between wired and wireless networks on a single platform.

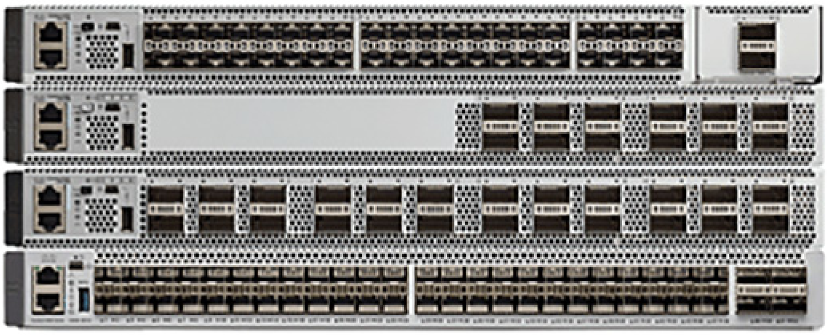
- Delivers 480 Gbps stacking bandwidth capacity
- Flexible uplinks: Cisco multigigabit, 1 Gbps, 10 Gbps, 25 Gbps, and 40 Gbps fixed (C9300L), and modular (C9300) options.
- Flexible downlinks: Cisco multigigabit, 5 Gbps, 2.5 Gbps, or 1 Gbps copper, or 1 Gbps fiber. Perpetual Cisco UPOE+, Cisco UPOE, and PoE+ options.
- Supports ETA, AVB, Cisco Umbrella cloud security, MACsec-256 encryption, hot patching, NFS/SSO, redundant power, and fans.

For more information, see the Cisco Catalyst 9300 Series Switches Data Sheet and switch model selector.

The Cisco Catalyst 9300 Series Switches are positioned within the access layer in the Industrial zone. They can be deployed on some large ports and terminals vehicles to provide access layer connectivity to cameras and sensors.

Cisco Catalyst 9500 Series Switch

Figure 5: Cisco Catalyst 9500 Switch Distribution and Core Layer)



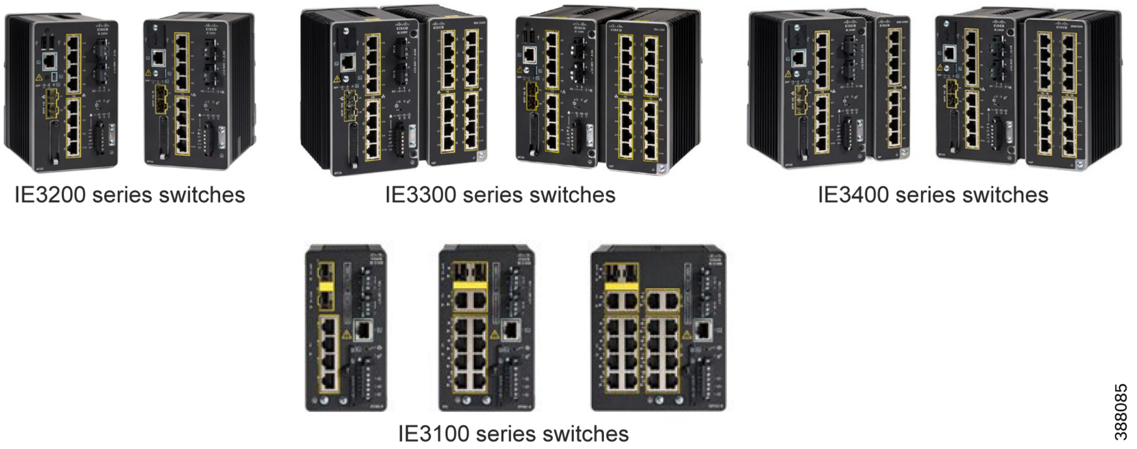
The Cisco Catalyst 9500 Series Switches are the next generation of enterprise-class, stackable, core layer switches.

- 4-core x86, 2.4-GHz CPU, 16-GB DDR4 memory, and 16 GB internal storage
- Up to 6.4-Tbps switching capacity with up to 2 Bpps of forwarding performance
- Up to 32 nonblocking 100 Gb Ethernet QSFP28 ports
- Up to 32 nonblocking 40 Gb Ethernet QSFP+ ports
- Up to 48 nonblocking 25 Gb Ethernet SFP28 ports
- Up to 48 nonblocking 10 Gb Ethernet SFP+ ports

For more information, see the Cisco Catalyst 9500 Series Switches Data Sheet and switch model selector.

Cisco IE3x00 Rugged Industrial Switches

Figure 6: Cisco IE3x00 Rugged Industrial Switches



Cisco Catalyst IE3100 Rugged Series switches offer up to 20 Gb Ethernet interfaces in a compact form factor and are ideal for harsh environments that are space constrained.

Cisco Catalyst IE3200 Rugged Series switches feature advanced, full Gb Ethernet with a modular, future-proof design. Expandable to 26 ports in a compact form factor, these rugged switches are optimized for size, power, and performance.

Cisco Catalyst IE3300 Rugged Series switches deliver high speed, up to 10 Gb Ethernet connectivity in a compact form factor. They are designed for a wide range of industrial applications in which hardened products are required. The modular design of the Cisco Catalyst IE3300 Rugged Series offers the flexibility to expand to 26 ports of Gb Ethernet or up to 24 ports of Gb Ethernet and 2 ports of 10 Gb Ethernet with a range of expansion module options.

The Cisco Catalyst IE3400 has the same basic functionality as the IE3300 but provides other features because of additional internal hardware. The IE3400 supports HSR, PRP, TrustSec, IOx, and more. See the data sheets for these switches for more detailed information about their differences.

These switches run Cisco IOS XE, a next-generation operating system with built-in security and trust, featuring secure boot, image signing, and the Cisco Trust anchor module.

All of the these platforms are built to withstand harsh environments in manufacturing, energy, ports and terminals, transportation, mining, smart cities, and oil and gas.

Cisco IC3000 Industrial Compute Gateway

Figure 7: Cisco IC3000 Industrial Compute Gateway

The Cisco IC3000 Industrial Compute Gateway extends data intelligence to the edge of the Internet of things (IoT) network.The Cisco Cyber Vision sensor can be installed in ports and terminals deployments where the sensor cannot be embedded into supported switches.

Security

As port and terminal operations move toward greater digitization, more machines, and more people, and applications are networked together, more equipment and applications are brought online to enable the automation, and more attack surfaces and vulnerabilities are created. According to a 2020 Marine Insite study, cyberattacks on the maritime industry OT systems have increased by 900% over the last three years (*Maritime Cyber Attacks Increase By 900% In Three Years*). A simple malicious attack can bring down an entire network, create an unprecedented backlog for the supply chain, disrupt network infrastructure and terminal operations for weeks, and cause great financial loss to port and terminal operators. For example, in June 2017, ransomware called NotPetya hit the Maersk shipping company, locking down access to the system that Maersk uses to operate its shipping terminals worldwide. According to the August 17, 2017 *Los Angeles Times* article, “Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks,” the attack cost the company almost $300 million and took two weeks to fix.

With an increase in the number of attacks on industrial installations, a smart port and terminal needs to have its cyber security in order. There is a large degree of data exchange with many third-parties, increasing the risk of receiving malware or viruses that can spread to other devices. The fact that containers carry high-value goods also makes them a potential target of cyber crime. Finding the right container by hacking into a system and setting up an illegal delivery is not a hypothetical scenario. Cyber security must be part of the daily IT process. Making sure that staff are aware of the risks is key, as people are always the weakest link. It has become obvious that cyber security also needs to be a top priority for container terminals, especially at the board level. Reliance on IT and data, and their responsibility for valuable goods, are simply too great to ignore, and there remains much to do.

Network security should be included from day one and not as an afterthought. An effective cybersecurity strategy requires a comprehensive, systematic, coordinated approach to protect against a broad and continually evolving set of threats. Cisco offers an ever-expanding, industry-leading portfolio of cybersecurity products to provide comprehensive protection for IT and operations networks. The Cisco portfolio includes Cisco Cyber Vision, which provides visibility into industrial devices and their traffic flows; Secure Network Analytics, which can be used to monitor data flows and detect traffic anomalies that can be used to enhance network segmentation policies; Cisco Identity Services Engine (ISE), a policy platform called that helps define and manage user profiles and access policies at scale; Cisco Malware Defense (formerly Advanced Malware Protection) to provide up-to-date monitoring and detection of malware threats; and Cisco Umbrella to prevent workers from accessing malicious network domains. Additionally, Cisco SecureX provides a consolidated view for simplified management of the overall security approach.

Securing the Industrial Network is a Journey

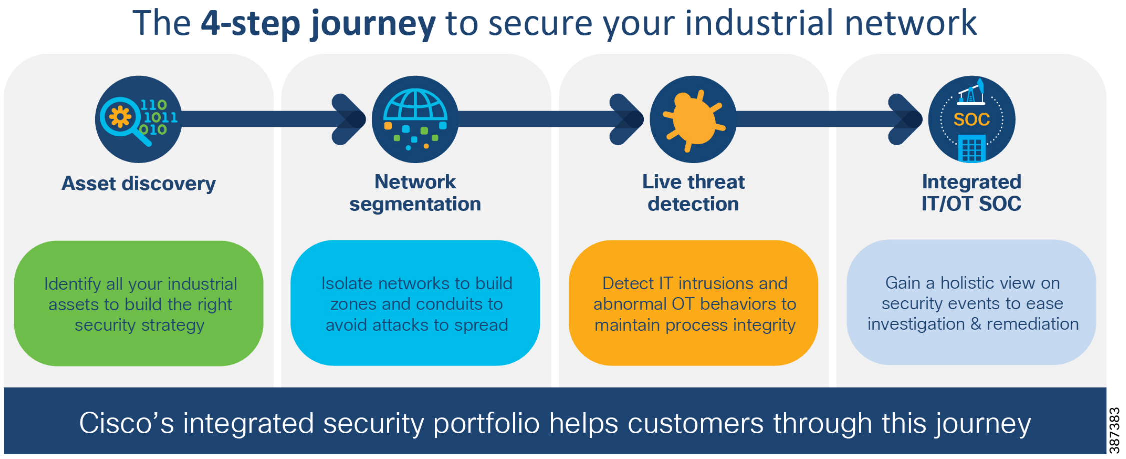
Industrial control networks connect devices that have been deployed over a period of many years—sometimes even decades—beginning when cyber security wasn't a concern. When organizations attempt to secure their industrial IoT networks, they encounter three primary issues:

- A lack of visibility: Enterprises often don't have an accurate inventory of what's on their industrial network. Without this visibility, they have limited ability to build a secure communications network architecture.
- A lack of control: Lack of visibility also leads to a lack of control because enterprises are unaware of which devices are communicating and where that communication is going.
- A lack of collaboration: OT devices and processes are managed by the operations team. Cybersecurity generally is driven by the IT and security teams. These stakeholders need to collaborate to build the specific security policies and enrich events with context so that security does not disrupt production.

Addressing these issues and building a secure industrial network does not happen overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

The following figure depicts the stepwise journey that you can embark on to integrate IT and OT security within your IT operations.

Figure 8: The Four-Step Journey to Secure Your Industrial Network


The 4-step journey to secure your industrial network
110 1011 010
SOC
Asset discovery
Network segmentation
Live threat detection
Integrated IT/OT SOC
Identify all your industrial assets to build the right security strategy
Isolate networks to build zones and conduits to avoid attacks to spread
Detect IT intrusions and abnormal OT behaviors to maintain process integrity
Gain a holistic view on security events to ease investigation & remediation
Cisco's integrated security portfolio helps customers through this journey
387383

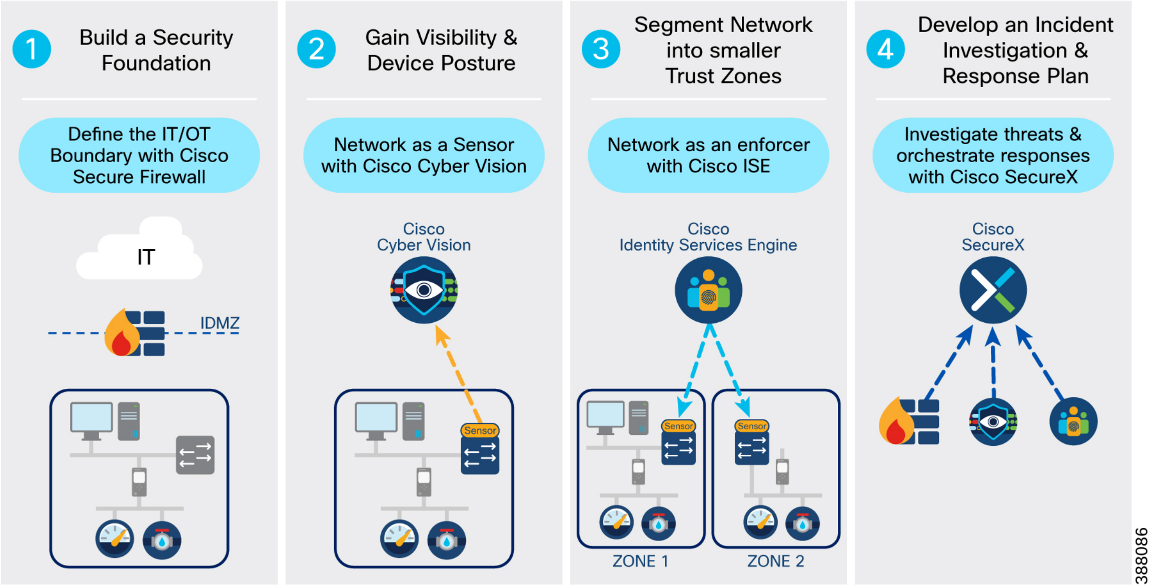
Extending IT Security to OT Through Effective Collaboration

To successfully secure the OT environment, all stakeholders must work together. Operations understands the industrial environment—the devices, the protocols, and the business processes. IT understands the IP network. And the security team understands threats and vulnerabilities. By working together, these teams can leverage existing security tools and expertise to protect the industrial network without disrupting operational safety and uptime.

Cisco security solutions are built into the industrial networks to monitor operations, feed security platforms with OT context, and enable this crucial collaboration.

Network managers appreciate the unique simplicity and lower costs of Cisco edge architecture when looking to deploy OT security at scale. Operations gains real-time insight into the industrial processes, so that they can maintain system integrity and operations continuity. Security teams have visibility into industrial assets and communications with context enriched by control and OT engineers.

Figure 9: Foundational Components of Industrial Security


1 Build a Security Foundation
Define the IT/OT Boundary with Cisco Secure Firewall
IT
IDMZ
2 Gain Visibility & Device Posture
Network as a Sensor with Cisco Cyber Vision
Cisco Cyber Vision
Sensor
3 Segment Network into smaller Trust Zones
Network as an enforcer with Cisco ISE
Cisco Identity Services Engine
Sensor
Sensor
ZONE 1
ZONE 2
4 Develop an Incident Investigation & Response Plan
Investigate threats & orchestrate responses with Cisco SecureX
Cisco SecureX
388086

Cisco Identity Services Engine

Figure 10: Ciscol SE Appliance

Cisco Identity Services Engine (ISE) is a centralized identity and policy management server. It provides dynamic endpoint visibility, which can then be used to drive visibility-based network segmentation. ISE also integrates with other Cisco security and third-party security services to provide automated threat containment. Cisco ISE is available as either a physical appliance or as a virtual machine.

Segmenting the Network into Smaller Trust Zones

The main goal of segmentation is to minimize the affect of any potential breach. Part one of the security journey provides segmentation between the enterprise and industrial network. However, the risk of a breach remains. Malware could be introduced to the network by using rogue USBs, or infected devices connecting to the plant floor infrastructure. Further segmenting the network into smaller trust zones can reduce the effectiveness of a security breach and contain a breach within a network boundary.

ISA/IEC62443 recommends segmenting the functional levels of an industrial network into zones and conduits. A zone is a collection of physically and functionally united assets that have similar security requirements. These areas are defined from the physical and functional models of the industrial system control architecture. A conduit supports and defines allowed communication between two or more zones.

Multiple segmentation technologies can be implemented:

- VLAN: A virtual local area network (VLAN) can be created on a Layer 2 switch to reduce the size of the broadcast domain. Each VLAN is considered to be a separate logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a device that supports routing.
- VRF-lite: Virtualization of a Layer 3 device can be achieved by using virtual routing and forwarding (VRF). VRF technology allows you to virtualize a network device from a Layer 3 standpoint, creating different *virtual routers* in the same physical device. VRFs can be used in a service provider context with MPLS to create a multitenant environment, but it is known as VRF-lite when used locally in a single router.
- Access control list: An access control list (ACL) is a series of statements that is primarily used for network traffic filtering.
- Stateful firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block the traffic based on a defined set of security rules. A stateful firewall allows or blocks traffic based on the connection state, port, and protocol. We recommend that NGFW be introduced in a network for northbound communication, such as communication between and industrial datacenter and the Area Zones, for advanced threat protection between devices that pose a higher security threat but would not cause production downtime if security were prioritized over connectivity.
- TrustSec: Cisco TrustSec (CTS) defines policies using logical device groupings known as security group tags (SGTs). An SGT is a 16-bit identifier embedded into the MAC layer of IP traffic. The SGT is a single label that indicates the privileges of the group within the entire network. It is in turn propagated between network hops, allowing intermediary devices (switches, routers) to enforce policies based on the group identity tag.

Networks usually are designed in a modular fashion in which the overall network infrastructure is divided into functional modules. Policies can be applied to larger functional zones based on subnet, VLAN, or other network-based information. This segmentation model is known as macrosegmentation. For OT environments, microsegmentation can be thought of as the segmentation within a VLAN segment. While microsegmentation can be an effective tool for segmenting the OT network, it is a complicated starting point and requires a deep understanding of the OT network. We recommend that you begin with macrosegmentation across the distribution network and then slowly introduce microsegmentation policies after effective visibility has been gained of the plant floor operations. With this hybrid approach, both macrosegmentation and microsegmentation are implemented using the same TrustSec technology. Cisco ISE uses TrustSec technology to logically segment control system networks. For implementation details, see Cisco Industrial Automation Security Design Guide.

OT Security Challenges

Some of the challenges to OT security are:

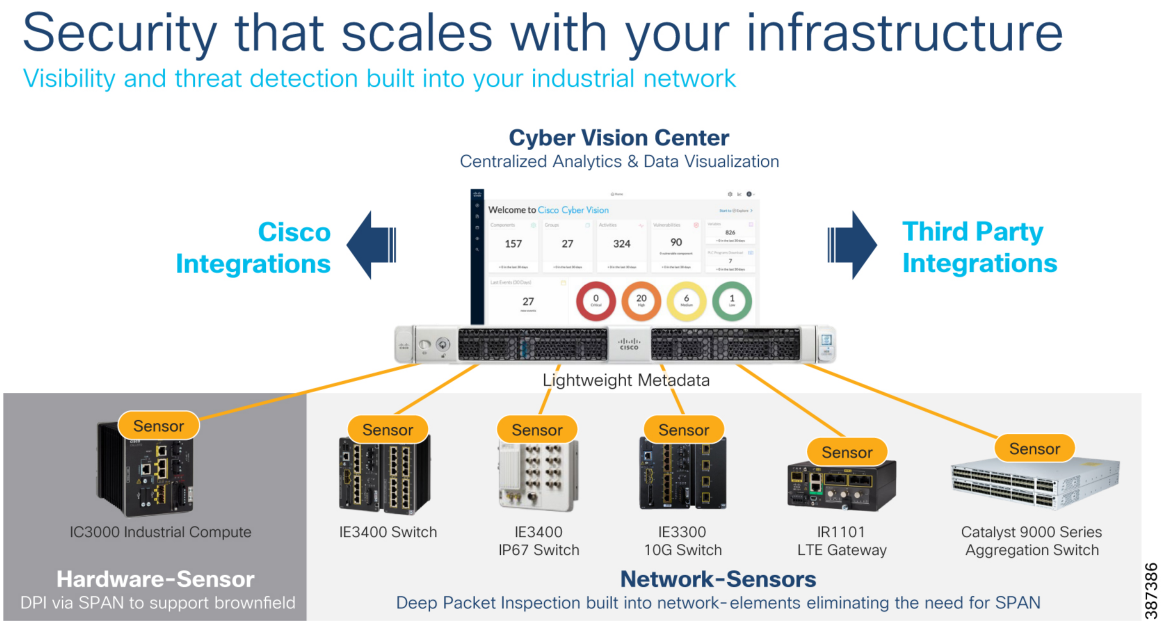
- Some OT assets cannot be patched
- Legitimate instructions can disrupt processes
- As more devices connect to the network, the attack surface increases, and the airgap is no longer sufficient
- Low visibility into the type and number of OT assets that are present in the network.

  Low visibility over disconnected endpoints
- Multiple third-parties might be involved in day-to-day operations

Standard IT cyber security solutions and methodologies are not sufficient to fulfill OT cybersecurity requirements. Securing OT networks requires new IT procedures and tools. This requirement is where Cisco Cyber Vision comes to the rescue.

Cisco Cyber Vision

Figure 11: Cisco Cyber Vision


Security that scales with your infrastructure
Visibility and threat detection built into your industrial network
Cyber Vision Center
Centralized Analytics & Data Visualization
Cisco Integrations
Third Party Integrations
Welcome to Cisco Cyber Vision
157
27
324
90
27
0
20
6
1
Lightweight Metadata
Sensor
IC3000 Industrial Compute
Hardware-Sensor
DPI via SPAN to support brownfield
Sensor
IE3400 Switch
Sensor
IE3400 IP67 Switch
Sensor
IE3300 10G Switch
Sensor
IR1101 LTE Gateway
Sensor
Catalyst 9000 Series Aggregation Switch
Network-Sensors
Deep Packet Inspection built into network-elements eliminating the need for SPAN
387386

Cisco Cyber Vision enables IoT and OT security in an industrial network to gain full visibility to the industrial assets and their application flows in real time. The edge sensors are embedded in selected Cisco network equipment and the Cyber Vision Center is deployed as a virtual machine or physical appliance. This deeper integration between IT, cloud, and industrial networks creates many security issues that are becoming the primary obstacles to your industry digitization efforts.

Cisco Cyber Vision gives you full visibility into your ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk. Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can easily be deployed at scale so that you can ensure the continuity, resilience, and safety of your industrial operations within your port and terminal deployment.

Cisco Cyber Vision Key Features

- OT inventory and security assessments: Kick-start your OT security journey by building an accurate list of all your industrial assets, and baseline the network topology and communication patterns between the network devices and applications Besides helping you detect and build an OT asset inventory, Cyber Vision highlights device vulnerabilities and provides a risk score for each vulnerability.
- Network segmentation: Prevent attacks from spreading and build a network that can be effectively monitored with adaptive, dynamic network partitioning.
- Converged IT and OT SOC: Feed your security operations center (SOC) with OT context and leverage the time and money you have invested in IT cybersecurity to secure your OT network.
- Threat detection: Behavioral anomaly detection; snort intrusion detection (IDS) with Talos signatures; integration with Cisco SecureX for threat investigation.
- Governance and compliance: Take OT security to the next level. Have detailed information to comply with regulations and enable effective collaboration between OT and IT experts.

Cisco Cyber Vision Architecture

Cisco Cyber Vision uses a unique two-tier architecture consisting of a central server and distributed edge sensors. The Cyber Vision sensors capture network traffic at the edge of the network and run deep packet inspection (DPI) on application flows. The Cyber Vision Center is a centralized server that performs all the analytics and integrates with other security platforms such as firewalls and security information and event management (SIEMs). The strength of the edge sensor is that the software can be embedded into Cisco network equipment (IoT switches, routers, access points, or industrial compute platform). With Cyber Vision, industrial cybersecurity is built into your network equipment and fully integrated with your existing IT security platforms.

Deploying OT cybersecurity can quickly become complex. For your OT cybersecurity project to be successful, you must be able to scale it easily and at a reasonable cost.

Advantages of Cisco Cyber Vision

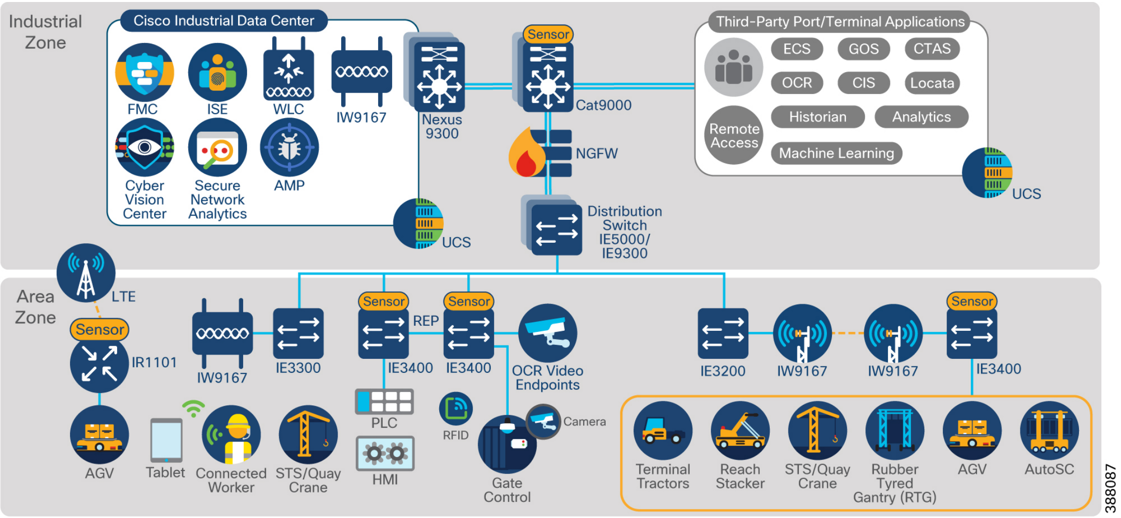
CiscoCyber Vision is the only solution on the market that embeds OT security within your industrial network. Its advantages include:

- No dedicated security appliance needed
- No need to build out a separate out-of-band monitoring network to send industrial traffic to a central security server, and no need for any additional cabling
- Instead of sending all network traffic to the Cyber Vision Center, the sensors decode the traffic locally at the edge of the network and send only the required metadata, which typically represents only 2% to 3% of the network traffic

Application of Cisco Cyber Vision to Ports and Terminals

To minimize latency between the Cyber Vision Center and edge sensors that collect data, we recommend that the Cyber Vision Center be installed in the data center that resides in the Industrial Zone, as shown in Figure 2: Connected Ports and Terminals—Cisco Reference Design, on page 10.

Figure 12: Cisco Cyber Vision Sensor Placement



Cyber Vision sensors are installed in the industrial network as either dedicated devices or running as a software package on a switch or router. As shown in the preceding figure, there are several places that the Cyber Vision sensor can be installed for maximum visibility.

The sensor requires a management interface to communicate with the Cyber Vision Center and send the metadata, which includes device attributes, packet headers, and operational events, from the captured IoT traffic. We recommend that the switch management interface be used for this communication.

The other required interface is for data collection. On a switch platform, this requirement is met by using a SPAN session to an RSPAN VLAN that is private to the switch. On a Cisco IC3000 Industrial Compute Gateway, there must be at least two physical interfaces used, one for the management network and one for the capture network. When using the Cisco Catalyst IR1101, only the routed gigabit Ethernet port is supported for the SPAN session to the sensor application. The management traffic can also use this routed port, the cellular interface, or even the LAN ports.

Ideally, the sensor would be installed on every switch with IoT devices connected to it. In the ports and terminal operations context, installations would include any vehicles or structures with PLCs or other sensors. This approach provides Cyber Vision Center with the most information about the connected devices and their traffic flows. For instance, when a controller communicates with a PLC on a crane, the sensor can monitor this communication and create a baseline for future monitoring. Any deviations from this baseline would be flagged as an anomaly.

If this installation guideline is not reasonable given cost or platform limitations, the traffic flows must be analyzed to pick the best sensor placement. In the case of a centralized distribution switch, such as the Cisco Catalyst 9x00, installing the sensor there provides the ability to monitor all northbound and southbound communications. However, this deployment model does not provide visibility into any eastbound or westbound communication, whether between access switches or within the access switch itself. In cases where upgrading the access switch to a supported model is not feasible, an IC-3000 with the Cyber Vision sensor installed on it can be deployed at that location. However, because the Cisco IC3000 Industrial Compute Gateway is not in the data path, a SPAN session on the switch must be configured to mirror all the IoT traffic to the Cisco IC3000 Industrial Compute Gateway.

For more detailed installation instructions, see the appropriate Install and Upgrade Guide.

A sensor can be installed in active or passive mode. The following table explains the differences between these modes.

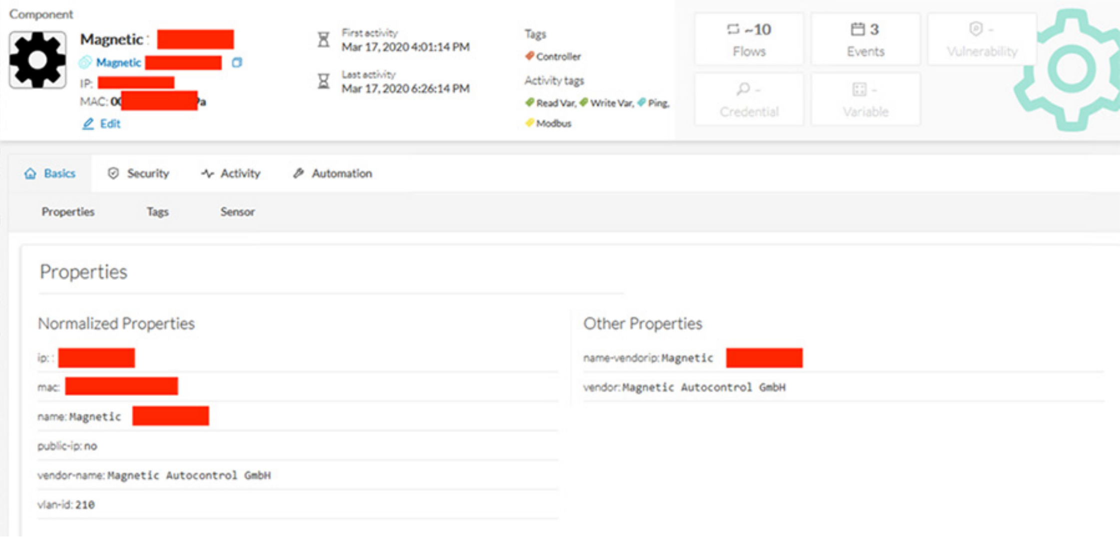
Table 2: Differences between Cyber Vision Sensor Active and Passive Modes

Property	Passive Mode	Active Mode
Discovery method	Captures packets sent by the device as part of its operation.	Actively sends hello messages using selected protocols to search for devices.
Network device impact	Traffic is passively listened to on monitored ports. Impact is higher when network traffic is duplicated to a sensor outside of the data path.	Constantly sending hello packets to devices increases network load and the load on assets.
Asset discovery	As long as the sensor is in the data path of a communicating device, it is discovered.	The assets must be responsive to the sensor requests. Depending on the frequency of the active discovery hellos, it can take some time before assets are discovered.
Asset information	Only the information that the asset transmits can be used for discovery. If data is not transmitted for a long time, it is undiscovered.	If the asset is online and responds to the active discovery, all relevant information is discovered. Otherwise, it can be marked as unresponsive or offline.
Asset discovery timing	Timing depends on how quickly an asset sends all the relevant information.	Discoveries can be performed on demand for quick information gathering. Excessive discoveries could be perceived as a denial of service attack.

If an asset communicates regularly, a passive approach is sufficient for profiling a device without adding to the traffic load. We also recommend using a passive approach if devices do not communicate using the active discovery protocol. These protocols are EtherNet/IP (Rockwell Automation), PROFINET, and S7 Communication (Siemens). If an asset communicates infrequently and a full picture of the network is desired quickly, we recommend using active discovery.

After Cyber Vision Center starts collecting data from the assets, it profiles the devices and categorize the data. The port operator can see which devices are communicating, what kind of data is being transmitted, and whether any issues have been identified. The following figures provide some examples.

Figure 13: Cyber Vision Asset Visibility



Component

Magnetic : [redacted]

Magnetic [redacted]

IP: [redacted]

MAC: [redacted]

Edit

First activity
Mar 17, 2020 4:01:14 PM

Last activity
Mar 17, 2020 6:26:14 PM

Tags
Controller

Activity tags
Read Var, Write Var, Ping, Modbus

~10 Flows

3 Events

- Vulnerability

- Credential

- Variable

Basics | Security | Activity | Automation

Properties | Tags | Sensor

Properties

Normalized Properties

ip: [redacted]

mac: [redacted]

name: Magnetic [redacted]

public-ip: no

vendor-name: Magnetic Autocontrol GmbH

vlan-id: 210

Other Properties

name-vendorip: Magnetic [redacted]

vendor: Magnetic Autocontrol GmbH

Figure 14: Cyber Vision Asset Communication Map

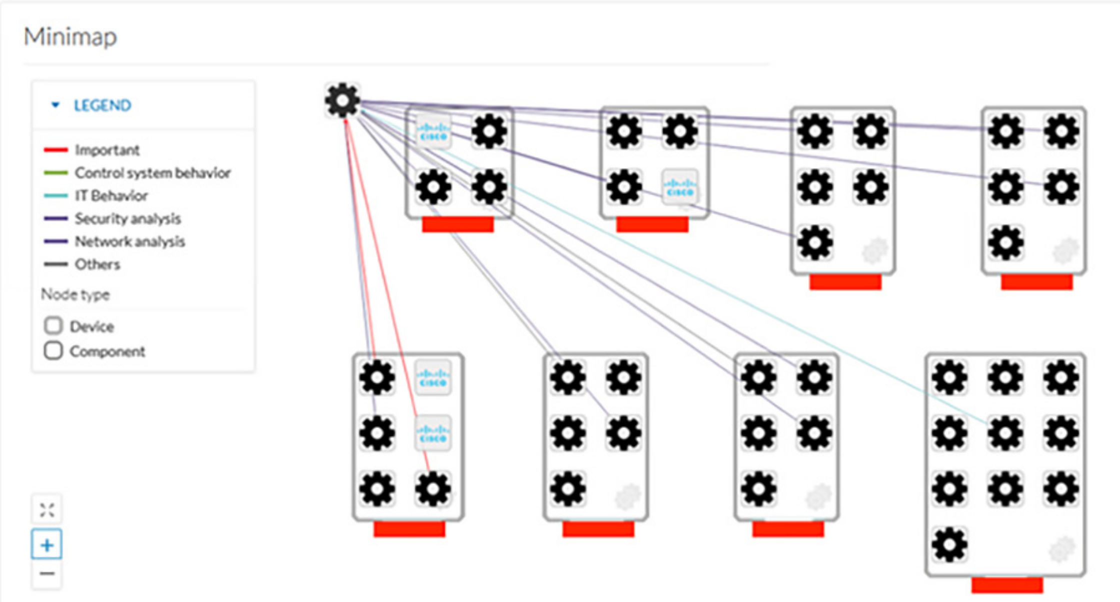
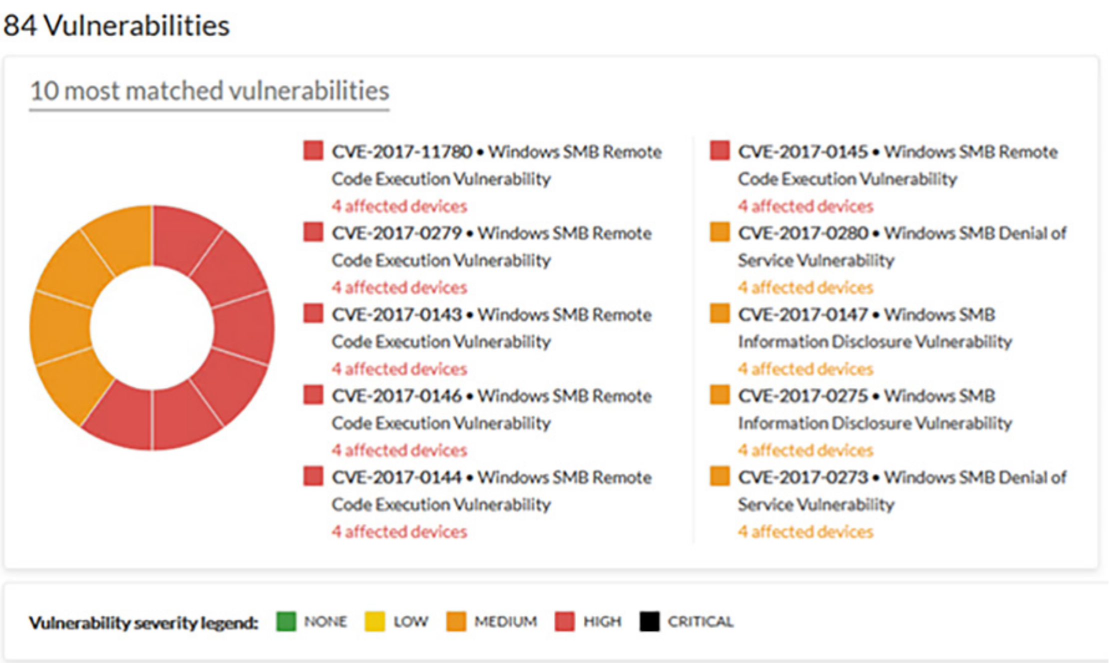


Figure 15: Cyber Vision Detected Vulnerabilities



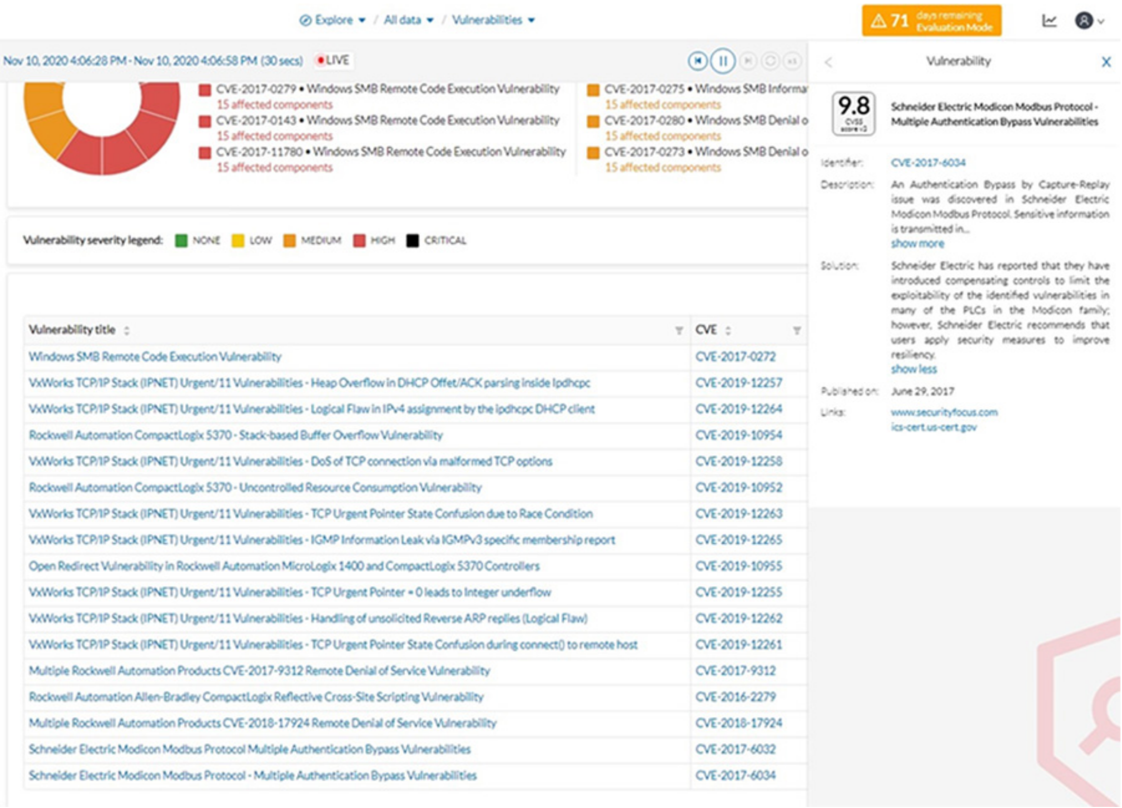
84 Vulnerabilities

10 most matched vulnerabilities

- 🟥 CVE-2017-11780 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟥 CVE-2017-0279 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟥 CVE-2017-0143 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟥 CVE-2017-0146 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟥 CVE-2017-0144 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟥 CVE-2017-0145 • Windows SMB Remote Code Execution Vulnerability
  4 affected devices
- 🟧 CVE-2017-0280 • Windows SMB Denial of Service Vulnerability
  4 affected devices
- 🟧 CVE-2017-0147 • Windows SMB Information Disclosure Vulnerability
  4 affected devices
- 🟧 CVE-2017-0275 • Windows SMB Information Disclosure Vulnerability
  4 affected devices
- 🟧 CVE-2017-0273 • Windows SMB Denial of Service Vulnerability
  4 affected devices

Vulnerability severity legend: 🟩 NONE 🟨 LOW 🟧 MEDIUM 🟥 HIGH ⬛ CRITICAL

Figure 16: IT and OT Vulnerabilities Detected by Cyber Vision



Explore ▾ / All data ▾ / Vulnerabilities ▾
⚠ 71 days remaining Evaluation Mode

Nov 10, 2020 4:06:28 PM - Nov 10, 2020 4:06:58 PM (30 secs) ● LIVE

- 🟥 CVE-2017-0279 • Windows SMB Remote Code Execution Vulnerability
  15 affected components
- 🟥 CVE-2017-0143 • Windows SMB Remote Code Execution Vulnerability
  15 affected components
- 🟥 CVE-2017-11780 • Windows SMB Remote Code Execution Vulnerability
  15 affected components
- 🟧 CVE-2017-0275 • Windows SMB Informa
  15 affected components
- 🟧 CVE-2017-0280 • Windows SMB Denial o
  15 affected components
- 🟧 CVE-2017-0273 • Windows SMB Denial o
  15 affected components

Vulnerability severity legend: 🟩 NONE 🟨 LOW 🟧 MEDIUM 🟥 HIGH ⬛ CRITICAL

Vulnerability title	CVE
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0272
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - Heap Overflow in DHCP Offet/ACK parsing inside Ipdhcpc	CVE-2019-12257
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264
Rockwell Automation CompactLogix 5370 - Stack-based Buffer Overflow Vulnerability	CVE-2019-10954
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258
Rockwell Automation CompactLogix 5370 - Uncontrolled Resource Consumption Vulnerability	CVE-2019-10952
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265
Open Redirect Vulnerability in Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers	CVE-2019-10955
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer = 0 leads to Integer underflow	CVE-2019-12255
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - Handling of unsolicited Reverse ARP replies (Logical Flaw)	CVE-2019-12262
VxWorks TCP/1P Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host	CVE-2019-12261
Multiple Rockwell Automation Products CVE-2017-9312 Remote Denial of Service Vulnerability	CVE-2017-9312
Rockwell Automation Allen-Bradley CompactLogix Reflective Cross-Site Scripting Vulnerability	CVE-2016-2279
Multiple Rockwell Automation Products CVE-2018-17924 Remote Denial of Service Vulnerability	CVE-2018-17924
Schneider Electric Modicon Modbus Protocol Multiple Authentication Bypass Vulnerabilities	CVE-2017-6032
Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities	CVE-2017-6034

Vulnerability

9.8 CVSS score v3

Schneider Electric Modicon Modbus Protocol - Multiple Authentication Bypass Vulnerabilities

Identifier: CVE-2017-6034

Description: An Authentication Bypass by Capture-Replay issue was discovered in Schneider Electric Modicon Modbus Protocol. Sensitive information is transmitted in...
show more

Solution: Schneider Electric has reported that they have introduced compensating controls to limit the exploitability of the identified vulnerabilities in many of the PLCs in the Modicon family; however, Schneider Electric recommends that users apply security measures to improve resiliency.
show less

Published on: June 29, 2017

Links: www.securityfocus.com
ics-cert.us-cert.gov

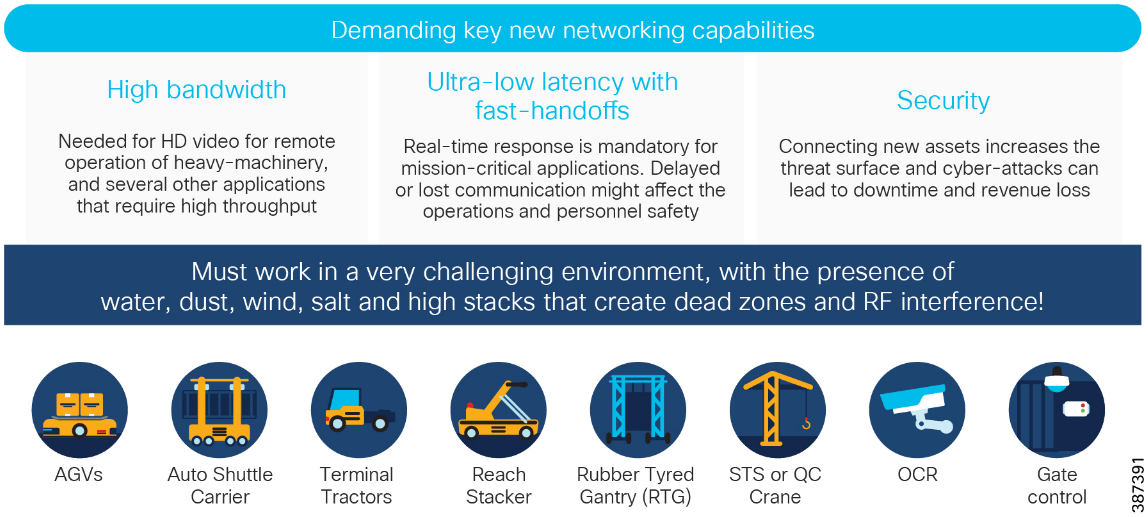
CHAPTER 3

Ports and Terminals CURWB Wireless Deployment: Architecture and Best Practices

Wireless Network Requirements

The following figure shows the key high-level wireless network requirements for terminal automation and digitization.

Figure 17: Terminal Automation and Digitization: High-Level Wireless Network Requirements



Demanding key new networking capabilities

High bandwidth

Needed for HD video for remote operation of heavy-machinery, and several other applications that require high throughput

Ultra-low latency with fast-handoffs

Real-time response is mandatory for mission-critical applications. Delayed or lost communication might affect the operations and personnel safety

Security

Connecting new assets increases the threat surface and cyber-attacks can lead to downtime and revenue loss

Must work in a very challenging environment, with the presence of water, dust, wind, salt and high stacks that create dead zones and RF interference!

Cisco Ultra-Reliable Wireless Backhaul Overview

The key technical requirements met by Cisco Ultra-Reliable Wireless Backhaul (CURWB) for the ports and terminals vertical are:

- Operates in globally available ISM frequency bands
- Enables customized or full terminal RF service coverage
- Under total control of the terminal operator
- Compatible with, and validated by all, main market vendors
- Supports PROFINET and CIP safety
- Uptime of 99.999%
- Ultralow latency of les than 10 ms
- Seamless roaming (handoff)—multifrequency capability with 0 ms handoff
- Fast failover
- High bandwidth
- Easy installation

CURWB: Key Technology Pillar

Three key technologies underlie the foundation for the CURWB solution:

- MPLS-based transmission protocol built to overcome the limits of standard wireless protocols.
- Fluidity achieved through a proprietary fast-roaming algorithm for vehicle-to-infrastructure communication with a 0 ms roam delay and no roam-loss for speeds up to 200 miles per hour (360 kilometers per hour).
- Proprietary fast failover high-availability mechanism that provides hardware redundancy and carrier-grade availability.

MPLS Overlay

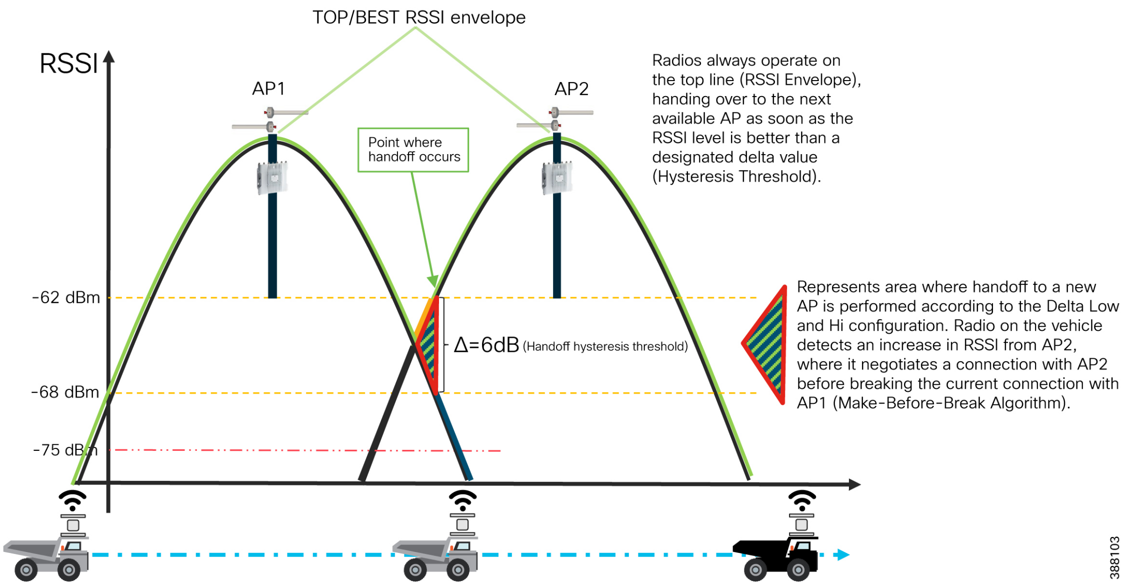
CURWB uses a proprietary wireless-based MPLS transmission protocol to discover and create label-switched paths (LSPs) between mesh point radios and mesh ends. This approach helps with making the wireless mesh networks resilient for both fixed and mobility networks. MPLS provides an end-to-end packet delivery service operating between Levels 2 and 3 of the OSI network stack. It relies on label identifiers, rather than 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.

Fluidity

Fluidity enables a vehicle that is moving between multiple infrastructure appcess points (APs) to maintain end-to-end connectivity with seamless handoffd between APs. A vehicle radio negotiates with the infrastructure APs and forms a new wireless connection to a more favorable infrastructure AP with better signal quality before breaking or losing its currently active wireless connection.

As shown in the following figure, because of the unique make-before-break handoff algorithm, the vehicle radios always operate 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 threshold.

Figure 18: Fluidity Dynamic Handoff Decision


TOP/BEST RSSI envelope
RSSI
AP1
AP2
Point where handoff occurs
Radios always operate on the top line (RSSI Envelope), handing over to the next available AP as soon as the RSSI level is better than a designated delta value (Hysteresis Threshold).
-62 dBm
-68 dBm
-75 dBm
Δ=6dB (Handoff hysteresis threshold)
Represents area where handoff to a new AP is performed according to the Delta Low and Hi configuration. Radio on the vehicle detects an increase in RSSI from AP2, where it negotiates a connection with AP2 before breaking the current connection with AP1 (Make-Before-Break Algorithm).
388103

Hardware Redundancy and High-Availability

CURWB has a proprietary fast failover function that provides high availability and protection against hardware failures. This feature virtually guarantees uninterrupted service for mission-critical applications where safety or operations would be compromised by failure of a single radio or gateway device. Using the MPLS-based protocol, CURWB radios are able to achieve device failovers within 500 ms on both L2 and L3 networks.

CURWB L2 Fluidity Deployment: Network Components

There are three primary components in a CURWB fluidity deployment: the mesh end, mesh point, and vehicle radio.

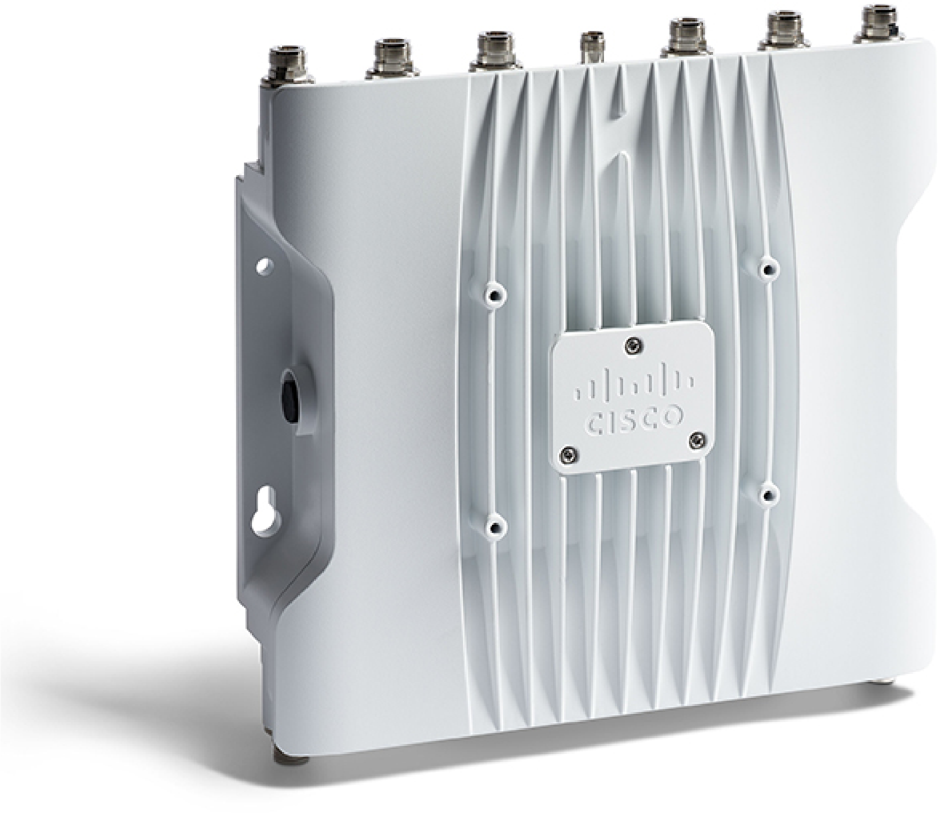
The mesh end functions as a gateway between the wireless and wired network. Mesh ends can also be thought of as MPLS label edge routers (LERs) on the infrastructure network. They are responsible for encapsulating the traffic coming from the wired network into the fluidity overlay network using MPLS, and de-encapsulating MPLS and delivering standalone datagrams onto the wired network. For a resilient network, we recommend using a pair of mesh ends for each wireless cluster.

The mesh point is where traffic enters the fluidity network from a vehicle or connected endpoint. Mesh points are positioned to maximize the RF coverage for vehicles that need wireless connectivity. All mesh points are tied to a single mesh end (or to a pair of mesh ends in redundant mode) and all mesh points that are connected to a mesh end form a wireless cluster.

The vehicle radio is a mesh point that is configured to provide wireless connectivity from one vehicle to the network infrastructure.

The Cisco Catalyst IW9167E Heavy Duty Access Point serves as the wireless radio, enabling mobility and fixed deployments. It features three RF radios (2.4 GHz is not supported in current CURWB mode), dual multigigabit Ethernet interfaces that also support M12 connections, and numerous power options. Because of its ruggedness and versatility, it can serve as any component in the CURWB architecture, whether mesh end, mesh point, or vehicle radio. When using the IW9167 as the mesh, it can run with antennas disabled or enabled, depending on the placement in the network.

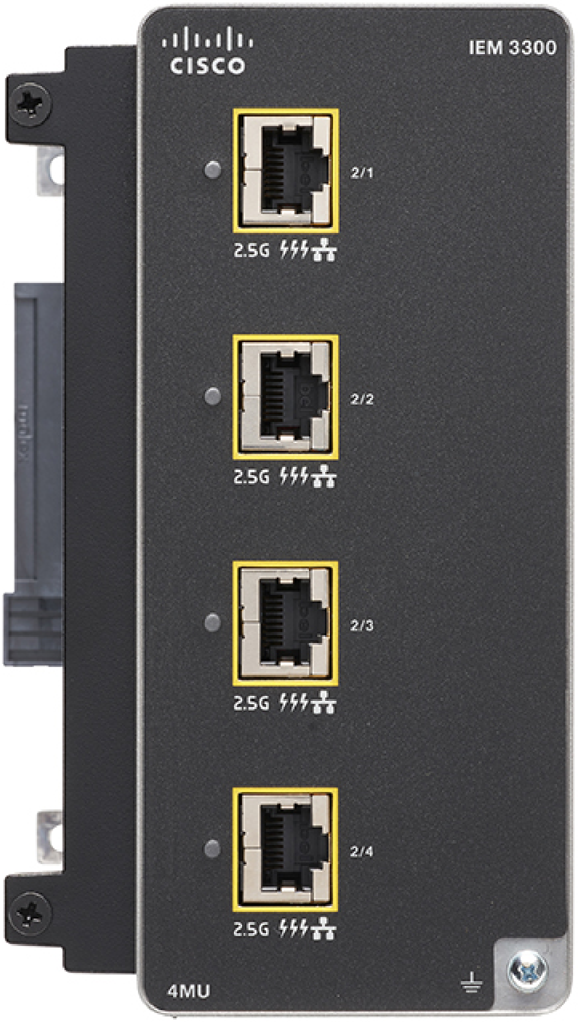
Figure 19: Cisco Catalyst IW9167E Heavy Duty Access Point



Power Requirements

Special attention should be made to the power requirements for the IW9167. It can operate from 24 VDC to 48 VDC, 802.3bt (uPOE), or 802.3at(PoE+) in limited power mode. In limited power mode, certain features are disabled or have reduced functionality. See the product's data sheet for more specifics. The IE3x00 switches support up to 802.3at, but some models can be combined with the IEM-3300-4MU to support four ports of 802.3bt.

Figure 20: IEM-3300-4MU



Network Licensing

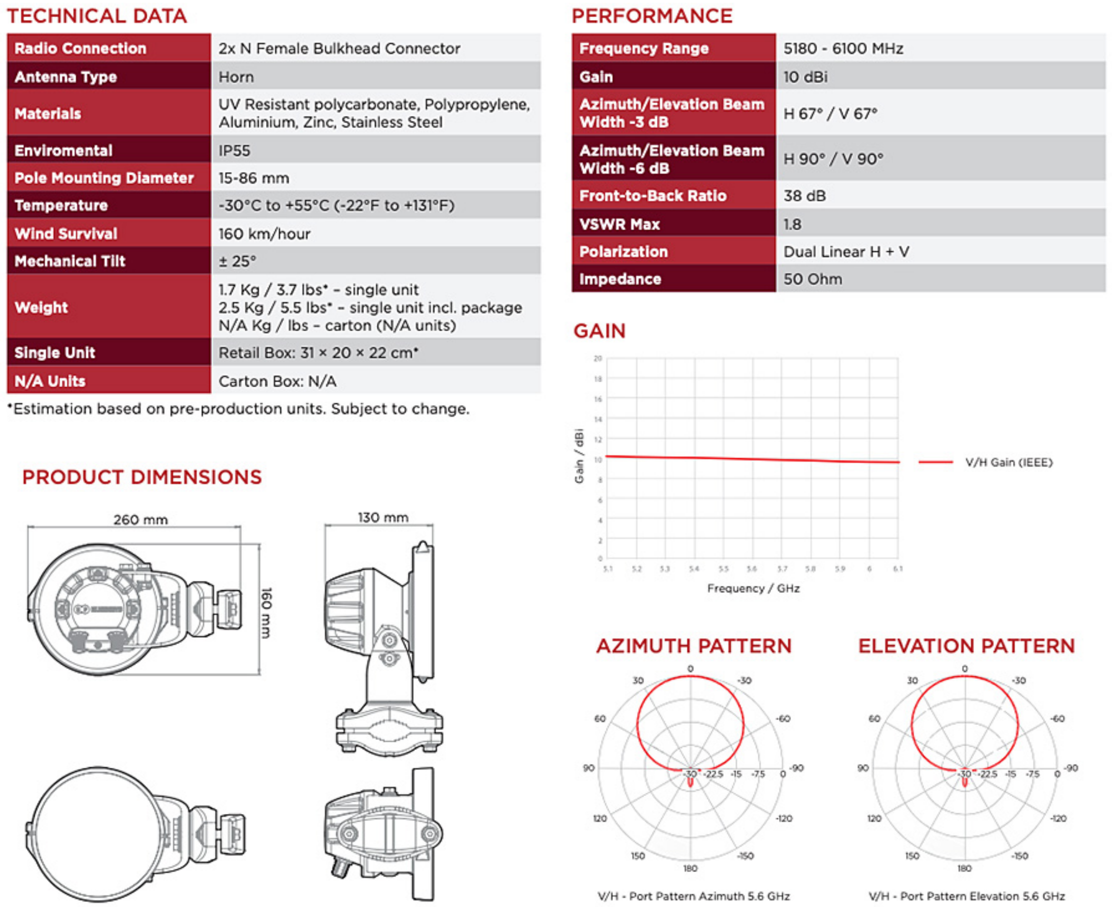
As described in the IW9167 data sheet, the network license level determines the amount of mobility throughput that a vehicle can support. By default, Network Essentials is installed, which supports 500 kbps of throughput on a vehicle. For most applications, this throughput is not sufficient. Network Advantage supports up to 50 Mbps, which supports all but the most demanding video applications. Network Premier supports unlimited throughput up to the maximum of the RF channel.

FM-Horn-90 Antenna

The FM-Horn-90 (Cisco PID FLMESH-HW-HORN-90) is a connectorized symmetrical horn antenna with carrier class performance. The FM-Horn-90 antenna 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. High-density AP clusters and radio colocation is practical due to the radiation pattern and a compact size of the antenna. The FM-Horn-90 antenna is equipped with N-female connectors.

Figure 21: 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

The FM-Horn-90 is the best choice for ports and terminals because most of the poles in ports are structured in a way that radios have to be installed on top of high mast lamp poles (HMLPs) at 115 ft (35 m) and installing OMNI antennas at such a height does not provide low ground vehicles with good coverage. The Horn-90 directional antenna can be tilted down, and due to being symmetrical, can provide good coverage for small vehicles that operate at a height of 7 ft (2 m), such as terminal tractors and other ground vehicles.

Cisco Tri-Band Omnidirectional Antenna

The Cisco Tri-Band Omnidirectional Antenna was designed to complement the tri-radio nature of the IW9167 for interior or exterior applications. It is available horizontally or vertically polarized, depending on the required orientation. For more information, see the following documentation:

- Horizontally polarized: Cisco 2.4/5/6 GHz Tri-Band Omnidirectional Antenna (IW-ANT-OMH-2567-N)
- Vertically polarized: Cisco 2.4/5/6 GHz Tri-Band Omnidirectional Antenna (IW-ANT-OMV-2567-N)

IoT Operations Dashboard

The IoT Operations Dashboard (IoT-OD) is a cloud-based dashboard that enables IT and OT to securely deploy, monitor, and configure industrial assets at scale. In the context of CURWB, the IW9167 can be onboarded with zero touch provisioning (ZTP) and all configuration managed through the dashboard.

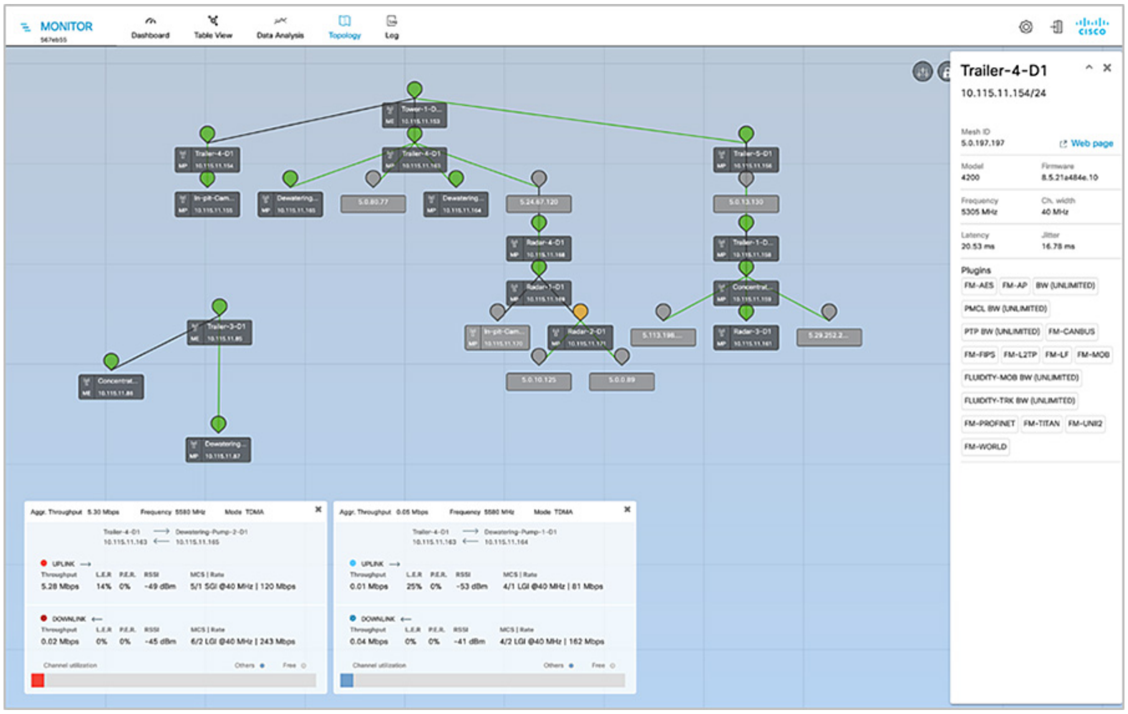
The IoT-OD enables centralized configuration management and visibility for all the CURWB devices in a single dashboard. It also provides the ability to manage and update the firmware installed on the radios. This management can be done in real time if the radios have connectivity to the Internet, or the configurations can be exported from the IoT-OD and uploaded to the radios if they operate in offline mode.

IW-Monitor: Centralized Management of CURWB Infrastructure

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

IW-Monitor supports fixed and roaming network architectures and allows easier 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 smart cities, rail, mining, ports and terminals, entertainment, smart factories, and military applications.

Figure 22: W-MonitorTopology View



Trailer-4-D1

10.115.11.154/24

Mesh ID: 5.0.197.197 — Web page

Model: 4200 — Firmware: 8.5.21a484e.10

Frequency: 5305 MHz — Ch. width: 40 MHz

Latency: 20.53 ms — Jitter: 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 10.115.11.163 ⟶ / ⟵ Dewatering-Pump-2-D1 10.115.11.165

	Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
UPLINK ⟶	5.28 Mbps	14%	0%	-49 dBm	5/1 SGI @40 MHz | 120 Mbps
DOWNLINK ⟵	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 10.115.11.163 ⟶ / ⟵ Dewatering-Pump-1-D1 10.115.11.164

	Throughput	L.E.R	P.E.R.	RSSI	MCS | Rate
UPLINK ⟶	0.01 Mbps	25%	0%	-53 dBm	4/1 LGI @40 MHz | 81 Mbps
DOWNLINK ⟵	0.04 Mbps	0%	0%	-41 dBm	4/2 LGI @40 MHz | 162 Mbps

Channel utilization — Others ● Free ○

Features and benefits:

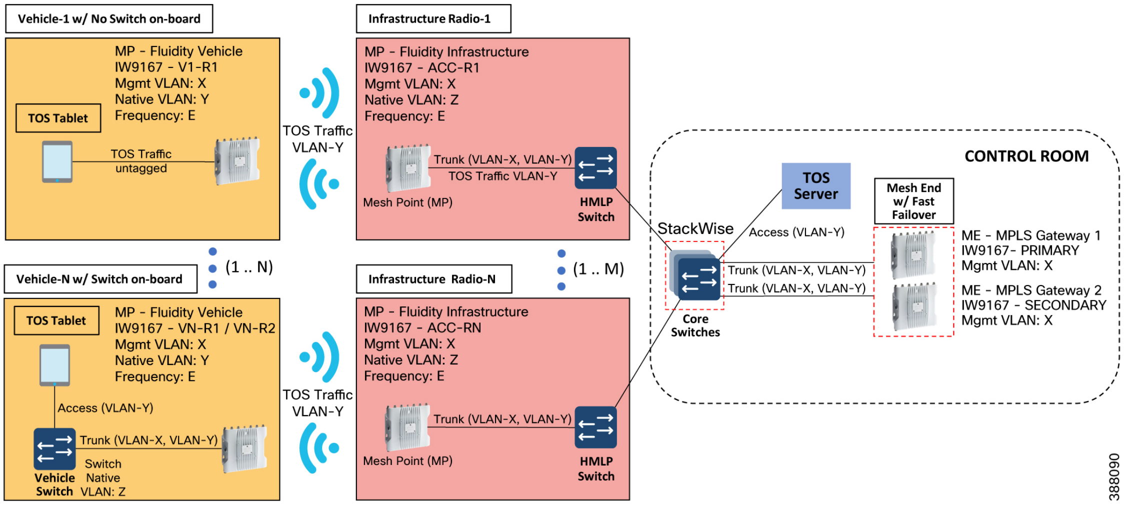
- On-premises monitoring tool for CURWB networks
- Wizard setup for quick and easy installation and deployment
- Real-time dashboard that displays uptime, throughput, latency, jitter, and other network KPIs

- 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 information display for quick and accurate troubleshooting
- Side-by-side comparison of radio KPIs over time and over vehicle position
- Alerts and events can be forwarded to a syslog server
- Radio KPIs such as RSSI, LER, PER, and so on can be exported to a CSV file for graphing.

A primary advantage of IW-Monitor is the ability to configure alerts for a group of radios based on certain KPIs. Imagine needing to support an application mix of automation and CCTV. The set of radios supporting the automation application can be grouped and alarms can be configured for KPIs such as latency, jitter, RSSI, and so on. At the same time, the group of radios supporting the CCTV network can have alarms configured using different KPIs such as link error rate (LER), MCS rate, and so on.

L2 Fluidity Architecture

Figure 23: L2 Fluidity Architecture (Single Frequency)



The previous figure depicts the high-level L2 fluidity mobility architecture for a single frequency deployment. A prerequisite for L2 fluidity is that all CURWB devices (mesh end gateways, access radios, and mobile radios) must be within the same VLAN, IP subnet, and L2 broadcast domain and ust be configured with the same passphrase.

The distribution and core layer consists of a redundant pair of mesh end gateways. As mentioned previously, the role of the mesh ends is to terminate the MPLS tunnels from each of the vehicle 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, the mesh ends act as default gateways and are responsible for the MPLS encapsulation and forwarding the traffic to the appropriate vehicle radios.

The access radios are configured as mesh points in L2 fluidity mode with the same passphrase that is configured on the mesh ends. The role of the access radios is to provide RF coverage for the mobility domain. The access radios are distributed across the area where wireless coverage is required while the vehicles roam. In the above architecture, all access radios are configured to operate in the same frequency.

For the mobility domain, there are two primary deployment models. A vehicle can either have a switch on board or no switch on board.

Redundancy and Fast Failover at the Core Layer

Cisco Catalyst 9500 Switch StackWise Virtual High Availability

Cisco StackWise Virtual is a two node solution that provides a unified control plane architecture by assigning one switch as active and the other as a hot standby. Both switches play an active role in data forwarding. Two Cisco Catalyst 9500 switches are connected using a StackWise Virtual Link (SVL). The SVL brings the two switches together, forming a single logical switch. Both switches can be managed as a single entity. Because the control plane, management plane, and data plane are integrated, the system behaves as a single switch. The advantage of configuring the switches in a StackWise pair is that it provides hardware redundancy and fast failover.

Mesh End Redundancy and MPLS Fast Failover

The mesh end gateway is a critical component within the network. It terminates all MPLS tunnels, aggregates all traffic coming from the wireless network, and is the demarcation point between the wired and the wireless domain. Therefore, we recommend that MPLS fast failover be enabled for a pair of redundant IW9167 mesh ends to be used within the ports and terminals deployment.

After it is configured, fast failover is 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, the fast failover feature 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 power each IW9167s using a different power source and connect them to different switches within the Cisco 9x00 StackWise pair. This approach provides protection against power outages and switch hardware failure.

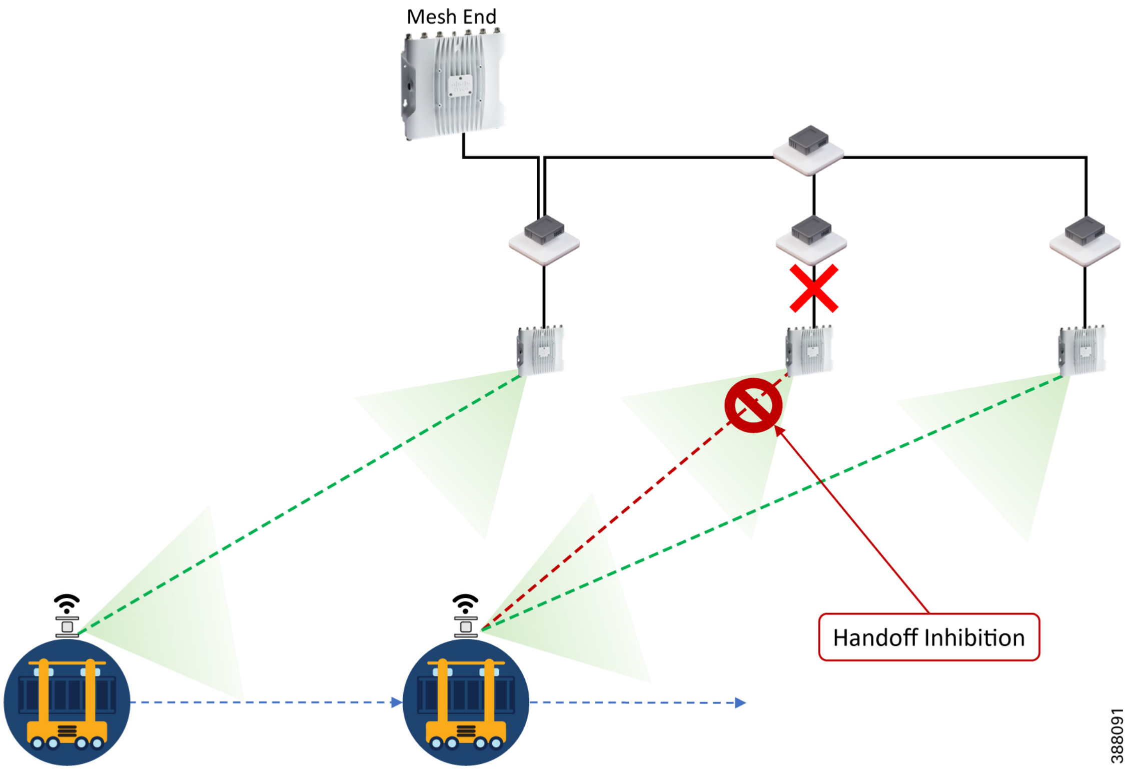
CURWB Access Layer: Fast Convergence on Failure

Link Backhaul Check: Handoff Inhibition

With the link backhaul check feature, an access radio unit detects a carrier loss on its Ethernet or fiber port, which stops its ability to deliver mobility traffic to the mesh end. The affected radio unit immediately advertises its status as Unavailable by transmitting a message **handoff inhibition** over the wireless channel. Upon receiving the **handoff inhibition** message, any mobile radios that are connected to this radio unit search for another access radio to connect to. All mobile radio units that are connected to this unavailable access radio find and connect to an alternative access radio unit within a few hundred ms, typically within less than 400 ms. Also, any handoff attempts from other mobile radios to this affected access radio are rejected. We recommend that the link backhaul check feature be enabled on the access radios within a ports and terminal deployment.

The following figure shows that the link between the infrastructure radio and the HMLP switch is down. Assuming that the radio is not powered using PoE but instead is powered with by an external power source, 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.

Figure 24: Link Backhaul Check: Handoff Inhibition

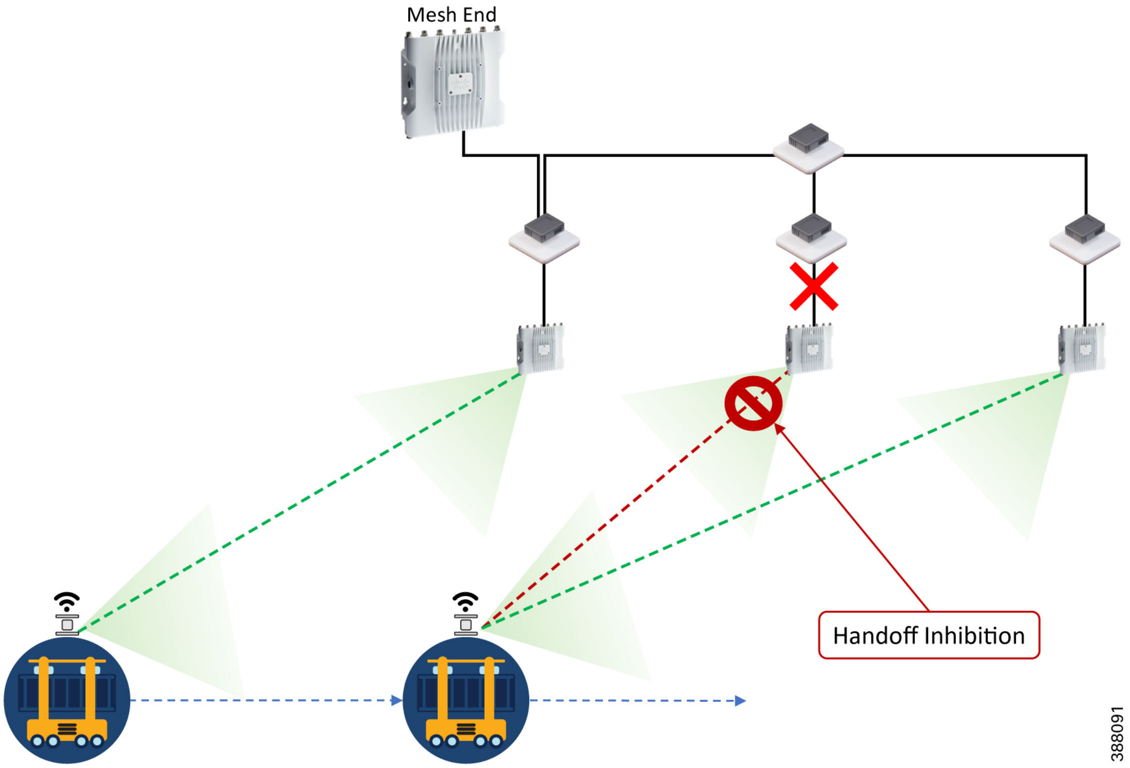


Mesh End Backhaul Check: Handoff Inhibition

Using the link backhaul check feature, an access radio unit detects a carrier loss on its Ethernet or fiber port, which stops its ability to deliver mobility traffic to the mesh end. 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, mobile radios that are connected to this radio unit search for another access radio to connect to. All mobile radio units that are connected to this unavailable access radio find and connect to an alternative access radio unit within a few hundred ms, typically within less than 400 ms. Also, any handoff attempts from any other mobile radios to this access radio are rejected. We recommend that the link backhaul check feature be enabled on access radios within a ports and terminal deployment.

The following figure shows that the link between the infrastructure radio and the HMLP switch is down. Assuming that the radio is not powered using PoE but instead is powered by an external power source, the radio is still up and providing good wireless connectivity to the 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.

Figure 25: Mesh End Backhaul Check: Handoff Inhibition

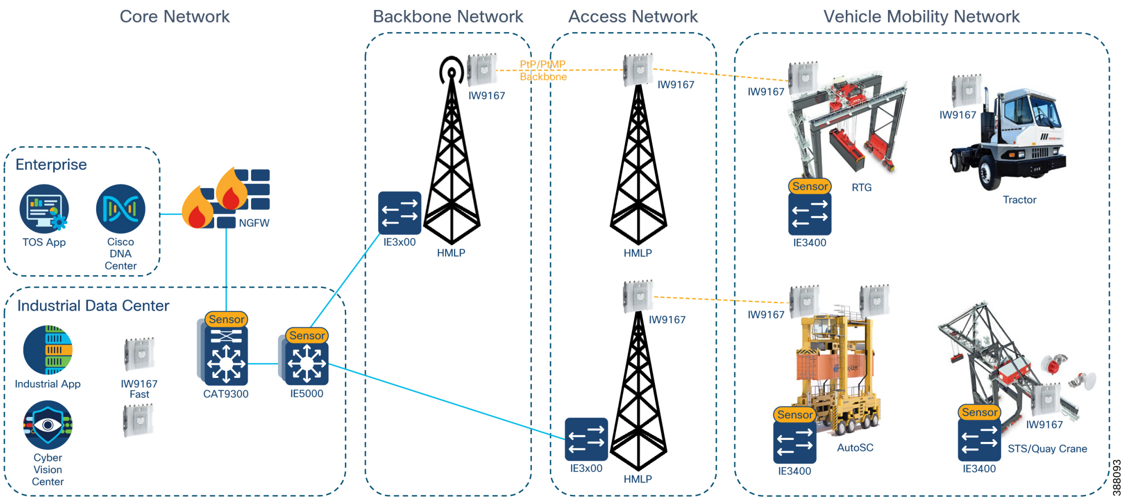


CURWB Mobility Radio Redundancy and High Availability

For deployments that include dual radios on board vehicles, we recommend the use of MPLS fast failover on the pair of radios. Both radios need to be connected to the same switch on board the vehicle. After fast failover is configured, both radios exchange high frequency keepalives between them to enable failure detection and fast failover within 500 ms.

CURWB L2 Fluidity Deployment for Ports and Terminals

Figure 26: Fluidity L2 High-Level Network Architecture for Ports and Terminals



The preceding figure depicts the CURWB fluidity L2 high-level network architecture with four zones:

- Vehicle mobility network
- Access network
- Backbone network
- Core network

CURWB systems for port and terminal operations are compatible with all terminal operating systems. CURWB network applications include, but are not limited to, optical character recognition (OCR) for cranes; easy retrofits of existing terminal vehicles (including STS/quay cranes, RTG cranes, AGVs, reach stackers, and stacking cranes); wireless tele-remote crane control; real-time video pan-tilt-zoom and CCTV feeds for vehicle operation and security; safety and telemetry inputs and outputs; failover networks for fiber spools; GPS correction data for automated guided vehicles and automated stacking cranes; and Wi-Fi network backbones.

In this reference design, the focus is on the CURWB architecture and deployment best practices to enable TOS. TOS usually needs lower bandwidth than other ports and terminals applications—typically a maximum of 1 Mb per second per vehicle. Wireless coverage of the full operations area is mandatory to support the TOS application. Network latency requirements are generally very lenient, although latency requirements may depend on specifications given by the TOS vendor.

It is likely that there are other types of traffic on the network along with TOS traffic. This traffic can include Webex or Skype for audio communications, Anydesk for maintenance, Syslog messages from RTGs, and so on. It is important to apply the appropriate QoS and traffic shaping policies for the different types of traffic and always to prioritize TOS application traffic over all other kinds of traffic to ensure the smooth operation of the port or terminal.

It also is important to ensure that only traffic that is intended to be on the wireless network be allowed. If the CURWB wireless network has been designed for a TOS application, only the Network Advantage license has been applied on the radios, and high-bandwidth video should be restricted from the wireless network to avoid severe degradation of the TOS application.

If the requirement and expectation is to use the CURWB wireless network for traffic other than TOS, a different RF design and a higher license tier for the CURWB radios might be needed.

CURWB L2 Fluidity: Network Zones

Vehicle Mobility Network

The vehicle mobility network consists of vehicles with either a single or dual CURWB radio installed on board. The onboard radios connect wirelessly to the access network radios and perform handoffs as the vehicle moves about the terminal. Some larger vehicles have a ruggedized Cisco Catalyst IE3x00 switch on board. Each vehicle has an onboard ruggedized tablet for TOS, which is either connected by wire directly to the second port of the CURWB radio, or to one of the switchports on the Cisco Catalyst IE3x00 switch, if available. VLAN tagging can be done on the CURWB radio in the absence of an onboard switch, however there only one client VLAN tag can be supported using the native VLAN.

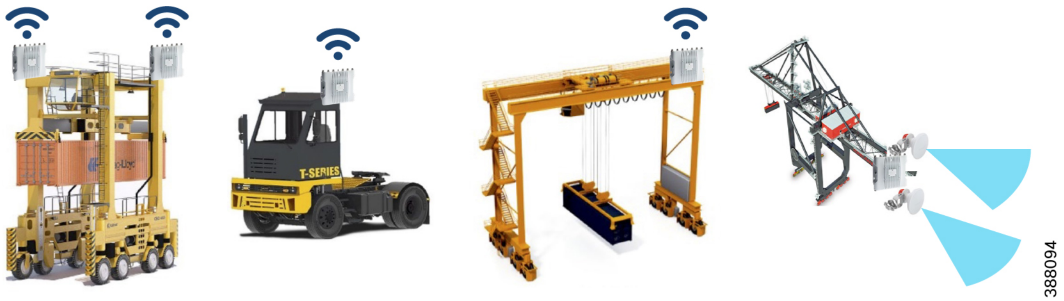
Vehicle Radio Deployment

All mobile units in a terminal are called *vehicles* and make up the vehicle mobility network.

Typical vehicles in a container terminal include STS cranes, reach stackers, terminal tractors, AutoSCs, and RTG cranes. A vehicle mobility network can be equipped with:

- Single radios (no redundancy) or dual radios (hardware redundancy and fast failover)
- Omnidirectional or directional antennas, depending on the operational area, angle of movement of vehicles, and the type of application running on vehicles

Figure 27: Vehicle Onboard Radio deployment Examples



Access Network

The access layer network consists of:

- CURWB access radios installed on HMLPs to provide wireless coverage to low-height ground vehicles that move around a terminal.
- CURWB access radios installed on HMLPs to provide wireless coverage to high-height STS/quay cranes.

Note It is mandatory that all infrastructure radios be connected to the infrastructure backbone network using either a wired or wireless backhaul link.

In both deployment scenarios listed above, the predominant antenna type used is the 90 degree horn antenna. In the first scenario providing RF coverage for lower height ground vehicles, which move about the entire terminal and in between piles of high containers, the 90 degree horn antenna is tilted toward the ground, providing coverage in the aisles created by the stacked high metal containers. In the second scenario, the 90 degree horn antenna for the access radio is pointed directly toward the 90 degree horn antenna for the radio that is installed on the STS/quay crane.

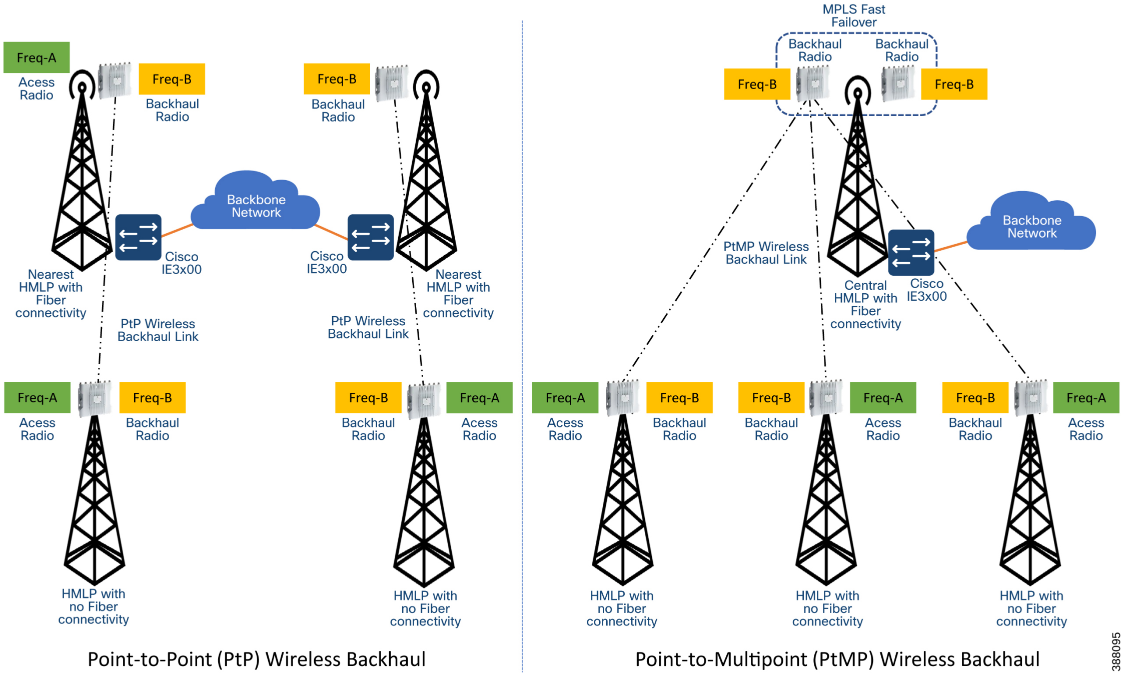
Note Because all STS/quay cranes are higher than the HMLPs, we recommend that the STS/quay cranes network be separate from the rest of the wireless network and that it be deployed on a separate channel.

CURWB Fixed Infrastructure: Wireless Backhaul

When fiber is not available at a HMLP for the access radios, we recomment requesting that fiber be installed to maintain the highest throughput and lowest latency. If this option is not possible and the throughput and latency requirements are minimal, a CURWB radio can be be used for a fixed infrastructure. In this configuration, one of the 5 GHz radios on the IW9167 is used for fluidity and the other 5 GHz radio is used for the fixed infrastructure. We recommend that the wirelessly connected poles be no more than one radio hop away.

It is important to use different frequencies for the fixed infrastructure radio and that the frequencies do not overlap with the radio configured for fluidity mode. The input power must also be verified because if the IW9167 is POE powered using 802.3at, the second 5 GHz radio is disabled. The following figure shows examples of a point-to-point and a point-to-multipoint deployment.

Figure 28: Examples of Point-to-Point and Point-to-Multipoint Wireless Backhaul


Freq-A
Acess Radio
Freq-B
Backhaul Radio
Freq-B
Backhaul Radio
Backbone Network
Cisco IE3x00
Cisco IE3x00
Nearest HMLP with Fiber connectivity
Nearest HMLP with Fiber connectivity
PtP Wireless Backhaul Link
PtP Wireless Backhaul Link
Freq-A
Acess Radio
Freq-B
Backhaul Radio
Freq-B
Backhaul Radio
Freq-A
Acess Radio
HMLP with no Fiber connectivity
HMLP with no Fiber connectivity
Point-to-Point (PtP) Wireless Backhaul
MPLS Fast Failover
Backhaul Radio
Backhaul Radio
Freq-B
Freq-B
Backbone Network
PtMP Wireless Backhaul Link
Central HMLP with Fiber connectivity
Cisco IE3x00
Freq-A
Acess Radio
Freq-B
Backhaul Radio
Freq-B
Backhaul Radio
Freq-A
Acess Radio
Freq-B
Backhaul Radio
Freq-A
Acess Radio
HMLP with no Fiber connectivity
HMLP with no Fiber connectivity
HMLP with no Fiber connectivity
Point-to-Multipoint (PtMP) Wireless Backhaul
388095

Note To avoid RF interference and high channel utilization, elect a different nonoverlapping RF channel for each of the wireless backhaul links (unless they are far apart and cannot interfere with each other). Also, the RF channels that are used for the fixed infrastructure should be different than the RF channel used within the access layer.

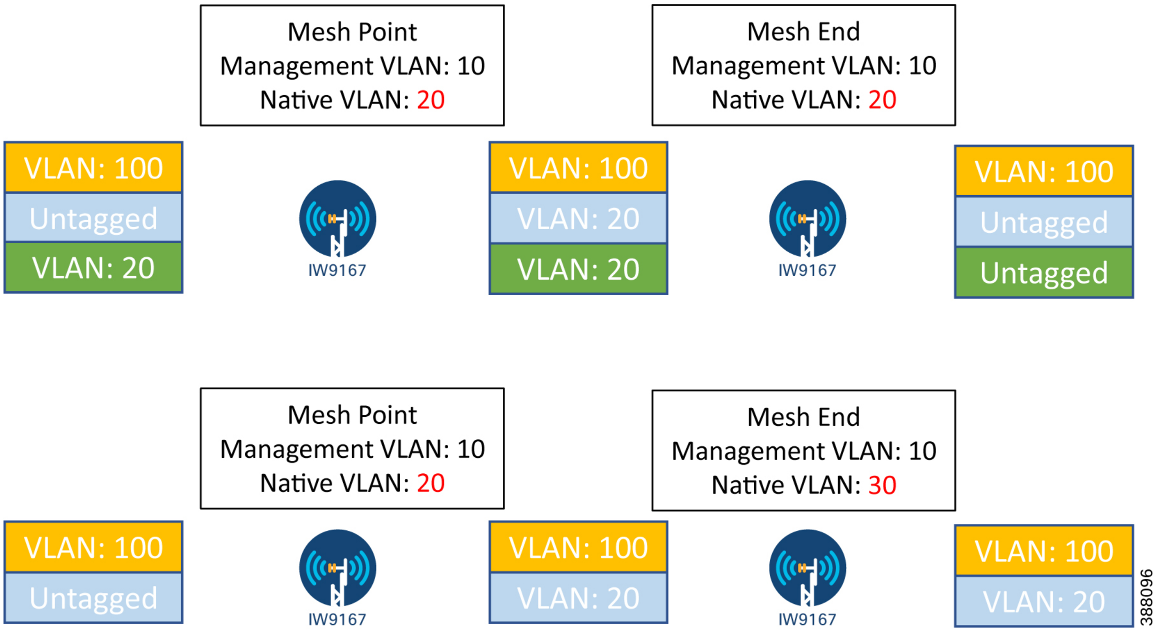
VLAN Design

On CURWB radios, VLAN support is optional and controls how tagged and untagged traffic is propagated through the network. When enabled, two VLANs are configurable in the radio user interface, one for management and the other for the native traffic. The management VLAN is used for control plane communication between the radios. The native VLAN determines how untagged traffic is tagged as it passes through the radio. Setting the native VLAN to 0 is a special case where all untagged traffic is dropped and only tagged traffic can pass.

The ability to control the VLAN tags is important in the ports and terminal context because a radio may not always be connected to a managed switch with the ability to segment traffic into different VLANs. In this scenario, all end device traffic would normally be untagged when put onto the switched network. The radio could be installed on an access port, but this approach forces all untagged traffic into a single VLAN. Using the CURWB solution, any radio connected to an end device could configure a native VLAN matching the type of device connected.

For instance, if a crane has numerous devices segmented behind a network switch using multiple VLANs, the radio connected to that switch passes traffic without modifying the VLANs. If another vehicle has one of those devices connected directly to a radio, the native VLAN can be used to put that untagged traffic into the correct VLAN to maintain consistency on the switched network. Because the native VLAN is for untagged traffic, using different native VLANs on the mesh points from the mesh end enables the initially untagged traffic to exit the mesh end with the VLAN intact. See the following figure for examples of this behavior.

Figure 29: Native VLAN Options on Mesh Point and Mesh End



We recommend using on the mesh end a native VLAN that is not used for any other traffic in the network. This approach enables the mesh point to control which VLAN the connected device is placed into.

When installing a switch behind a CURWB radio, the interface that is connected to the radio should be in trunk mode. The native VLAN on the switch should also match the native VLAN on the radio for consistency. In this scenario, the switch ports are configured for the correct VLANs that are necessary for the end devices and all traffic is tagged or untagged by the switch.

QoS

CURWB implements DiffServ inspired quality of servie (QoS) to provide end-to-end classification of user traffic. When enabled, the CURWB radio inspects every packet and looks for DSCP or COS markings. This value is then translated into one of eight priority levels based on that marking. When traffic is transmitted over the wireless interface, the eight priority levels are further mapped into four access categories based on IEEE 802.11e as shown in the following table.

Note CURWB radios cannot perform any QoS marking. The radios only inspect the user traffic QoS marking and schedule based on those values.

Table 3: Mapping Between Packet Priority and Access Category

Priority	Access Category
0	BEST EFFORT (BE)

Priority	Access Category
1	BACKGROUND (BK)
2	BACKGROUND (BK)
3	BEST EFFORT (BE)
4	VIDEO (VI)
5	VIDEO (VI)
6	VOICE (VO)
7	VOICE (VO)

We recommend that, if the wireless network has been deployed to enable a TOS application, only TOS traffic is transported over the CURWB wireless network. If there is a need to transfer other traffic over the CURWB wireless network, ensure that the TOS traffic is marked with the highest priority so that it gets preference over all other traffic contending for the CURWB resources.

For vehicles that have the Cisco Catalyst IE3x00 switches on board, the switch should perform the QoS classification and marking closest to the edge device and scheduling on the port facing the CURWB radio. For vehicles that do not have a switch on board to classify and tag traffic with QoS, the radio's native VLAN can be used to identify and tag with QoS on the northbound access radio switch.

Cisco IE3x00 QoS

The Cisco IE3x00 Rugged Industrial Switches support QoS, which allows a certain type of traffic to be treated differently at the expense of others, so that the performance of high-priority traffic such as TOS can be assured. Classification and marking are the first steps to implement QoS. Classification differentiates traffic type by examining the packet header. A packet can be classified based on the DSCP, the COS, and the IP precedence value in the header. It also can be classified with a VLAN ID and an access control list (ACL).

Classification and marking are recommended at the entry point of the network. After the traffic is classified, certain QoS features can be applied in the policy map, depending on the ingress or egress direction of the traffic. In the case of input policy applied to ingress traffic, the Cisco IE3x00 can be configured to trust the marking from the client device or set it to a different value based on business requirements. For output policy that is applied to egress traffic, you can assign a percentage of bandwidth, shape transmission to certain rate, or set a queue limit for specific traffic types. The Cisco IE3x00 supports multiple queueing models, including class-based weighted fair queuing (CBWFQ), and priority queuing. We recommend using CBWFQ in this solution to allocate a percentage of bandwidth for a specific application.

For vehicles that have a Cisco IE3x00 switch on board, it is advisable to mark egress TOS traffic from the vehicle to the control room with the highest priority so that it gets precedence over other kinds of traffic.

Security

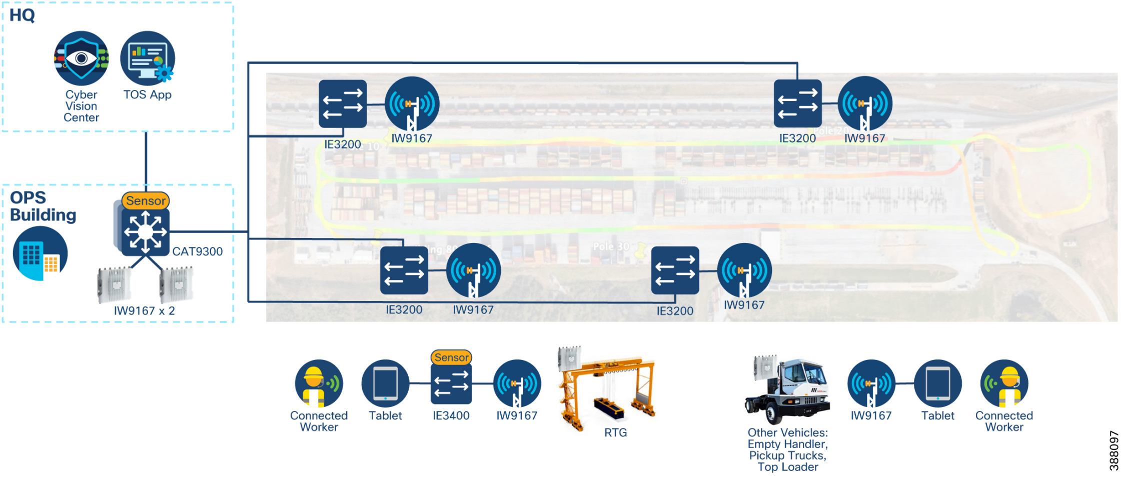
All client traffic within the MPLS tunnel is kept private using the system passphrase. However, for additional security, the CURWB solution also supports enabling AES encryption to encrypt all traffic over the wireless medium. For extra security, AES key rotation also is supported with a user-defined rotation timeout.

When configuring AES encryption, you must enable AES encryption on all radios within the system. Enabling AES only for a subsection of the system is not supported and causes a breakage.

CURWB for TOS Reference Architecture

Based on the reference architecture that is described previously, the following figure shows a reference architecture that can be used to support TOS.

Figure 30: TOS Reference Architecture



As shown in this figure, the design consists of IW9167 radios that are installed on HMLPs. Each HMLP consists of a Cisco IE3x00 switch that provides PoE+ (or uPOE) power to the radio, and provides fiber connectivity to the backbone network. The radios that are installed on the HMLPs provide RF coverage to the different ground vehicles and to the RTG cranes. Depending on the vehicle density and the amount of traffic traversing the wireless system along with TOS application traffic, a single frequency design can be used for a small deployment, or a dual or multifrequency design can be used for larger ports with a high vehicle density.

On smaller ground vehicles, another IW9167 radio is installed with the tri-band omnidirectional antenna. There is no need for a Cisco IE3x00 switch to be installed on smaller vehicles. Therefore, the TOS tablet is plugged into the second port of the radio directly. Also, because there is no Cisco IE3x00 switch on board to provide power to a radio, it must be powered by using DC power.

On larger vehicles such as RTGs, there can either be a single or dual IW9167 radio deployment with the tri-band omnidirectional antenna. The RTG has a Cisco IE3x00 switch installed on board, which can provide PoE power to the radios, depending on the power needed. In this case, the TOS tablet can be connected to the switch.

Note In some ports RTGs move only in the left and right direction and do not make 360 degree turns (especially within tele-remote and automation applications). In these cases, it is better to use directional antennas because having omnidirectional antennas adds more interference.

Note We recommend that you install the Cisco IE3400 on all ports and terminal vehicles that have a PLC on board. The IE3400 supports Cisco Cyber Vision, which provides visibility into the PLC communication traffic and can detect any anomalous behavior.

CHAPTER 4

Ports and Terminals: RF Planning, Design, and Installation

Wireless Site Survey

A wireless radio frequency (RF) site survey is highly recommended before the permanent installation of any radio equipment. The purpose of an RF site survey is to conduct a detailed engineering study to create a competent wireless network design that, after installed, addresses the needs of the individual use cases that have been identified for a particular operating environment. At the same time, the site survey gathers site-specific information that aids in the deployment of support infrastructure, including network and RF cabling, electrical, antenna selection and mounting, and AP hardware installation.

A proper site survey involves the temporary setup of suitable AP and antenna combinations in specific static locations to test and measure the RF propagation characteristics within a given environment or area. Several parameters and key metrics are collected during the wireless survey, such as overall coverage area, signal strength and quality, supported data rates, signal overlap, potential sources and existence of RFI and EMI, and environmental conditions that can affect RF behavior and performance. This data is analyzed to determine the correct hardware, antennas, and installation locations before undertaking the larger project costs of drilling holes, routing cables and conduit, and mounting equipment.

Without a proper RF site survey or wireless design study, equipment might be installed in suboptimal locations. Not only could this greatly reduce equipment performance, resulting in coverage gaps and therefore application issues, but the resolution to such a scenario would require additional time and engineering resources to identify and address any coverage gaps. This situation leads to an increase in overall project costs, prolonged project timelines, unplanned downtime, and disruptions to production, which would likely far outweigh the cost of simply conducting a proper RF site survey.

Pre-Survey Data Collection

Before conducting a site survey, ascertain the customer's requirements. This step ensures that the applications and use cases that ultimately need to be supported by the wireless deployment are well understood. Integrating these requirements into the survey process ensures that the resulting design accommodates the proposed performance criteria as stated by the customer's equipment and application vendors.

The requirements gathering process and key considerations include:

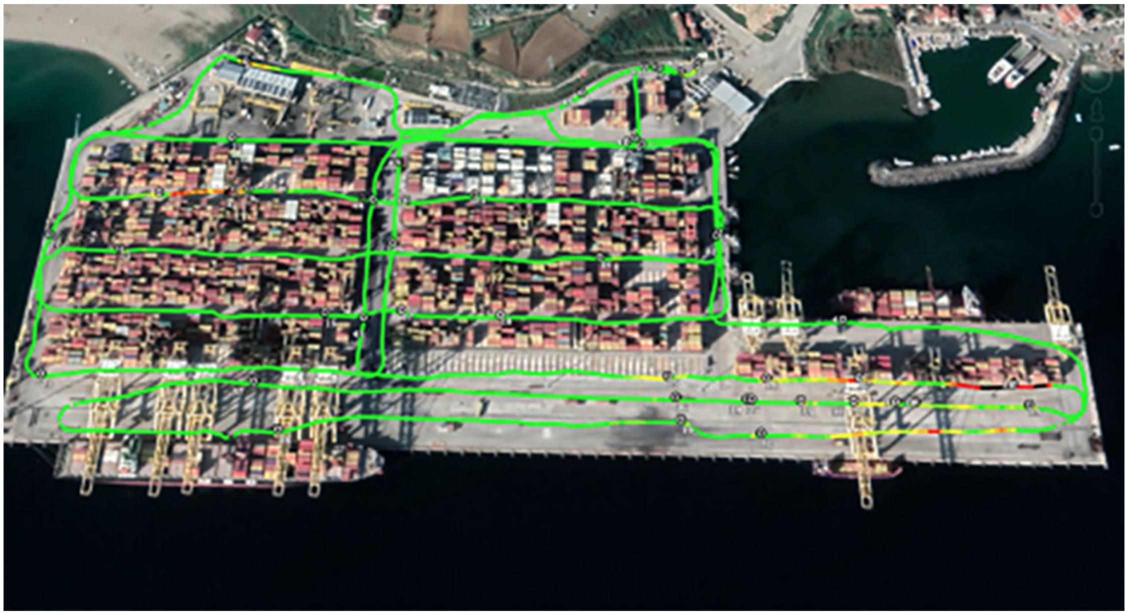
- Map of the terminal with locations of all HMLPs with fiber drops.
- Map of terminal showing the types of vehicles (with their heights) and their operating locations.
- Tye of light poles. It is critical to understand what type of light poles are available in the terminal to select proper antennas for different types of vehicles to provide the best coverage. Can any equipment be installed in the middle of the light pole or does it have to be on top of the pole? Any other mounting restrictions?
- Application requirements (latency, jitter, packet loss, out-of-order packets). The types of traffic that will traverse the wireless network need to be known. For example, if the wireless network is primarily being designed for TOS traffic, will there be any traffic other than TOS that will use the same wireless infrastructure?
- Bandwidth requirements for the applications (TOS, OCR, AGVs/IGVs, tele-remote, and so on).
- Location and concentration of vehicles (RTGs, STSs, reach stackers, ground vehicles) requiring wireless connectivity.
- Specific areas that require wireless coverage to support specific applications, and areas that do not require coverage.
- Contiguous RF coverage to facilitate fast roam times to support real-time applications.
- Support for future applications (excess capacity and performance).
- Endpoint and application transmission characteristics (constant bit rate vs. traffic bursts).

RF Site Survey

A thorough RF site survey consists of multiple activities to achieve the desired outcome. One, as mentioned previously, is the actual site survey, which involves the placement of APs in different locations within a defined area to understand RF coverage and potential performance characteristics.

Another is an RF spectrum analysis. While it is imperative to validate that the wireless design and the resulting deployment can meet the application requirements, it is equally important to understand what other RF devices might be operating in close proximity that can end up adversely affecting the wireless deployment.

Figure 31: RF Site Survey to Ascertain any Wireless Coverage Gaps



RF Spectrum Analysis

An RF spectrum analysis is used to thoroughly inspect the localized radio spectrum. This analysis is commonly conducted to identify sources of radio frequency interference (RFI) where suspected communication interference can be of concern. The analysis data can be helpful for equipment channelization and interference avoidance.

The principal goal of a spectrum analysis is to search for and locate potential sources of RF interference and to find clean RF channels that can be used for the CURWB deployment.

An RF spectrum analysis needs to be performed at the beginning of a project to help determine which clean frequencies and channels are available in the port or terminal. An estimate of the application throughput is needed and the vehicle density also is extremely useful for selecting an appropriate channel width. It is also important to determine the exact frequencies and channels and channel width because this information needs to be provided within IoT-OD to configure the radios.

A spectrum analysis should be performed multiple times at various operational times of a day or week. Often overlooked are incoming trucks that have cellular hotspots, where they turn on Wi-Fi to connect to wireless devices inside each truck. Experience shows that frequency usage varies throughout a standard operational day. For this reason, we recommend using a professional spectrum analyzer, as it can be set up to scan over a period of time, whereas a radio scan is a one-time scan so requires multiple manual scans.

Implementation Considerations

As previously mentioned, consider many factors when designing and deploying a wireless network. Each of the following topics has a unique ability to affect wireless communications and must be considered or uncovered during the site survey and installation process.

Ultimately, these considerations and their handling need to harmonize with the overall solution requirements to provide more assurances that both the design and subsequent resulting deployment meet service level expectations and application requirements.

Common RF installation Considerations

- Fresnel zone
- Knife-edge diffraction
- Obstruction shadowing
- Environmental attenuation
- Reflection and scattering
- Multipath, which is a 100% guarantee in container terminals, due to large steel walls of container stacks going up and down daily
- Delay spread values
- Antenna polarization, isolation
- Reactive near-field, radiating near-field
- In-band RFI and out-of-band RFI and harmonics
- EMI
- RF noise floor
- Equipment specifications
- Antenna field of view
- Antenna E and H planes
- Antenna type (omnidirectional, directional-sector, 30, 60, 90 degree horn, panel, and so on)
- Antenna gain
- Antenna beamwidth
- Antenna horizontal and vertical polarization

Survey characteristic

- Coverage
- RSSI
- SNR
- Data rate
- Retries and loss
- Overlap and redundancy
- High installation costs

RF Planning

During high-level frequency planning for a port or terminal site, it may be decided that part or all the system may use only a single radio channel or may use two or more radio channels. These stipulations are based on connectivity needs and the result of spectrum analysis of the port environment.

The minimum height value assumes that there are no obstacles in the Fresnel zone and that the link is parallel to a flat surface, such as the sea. If there are obstacles in the middle of the Fresnel zone, such as trees or buildings, you must add the height of the obstacles to the minimum height of an antenna.

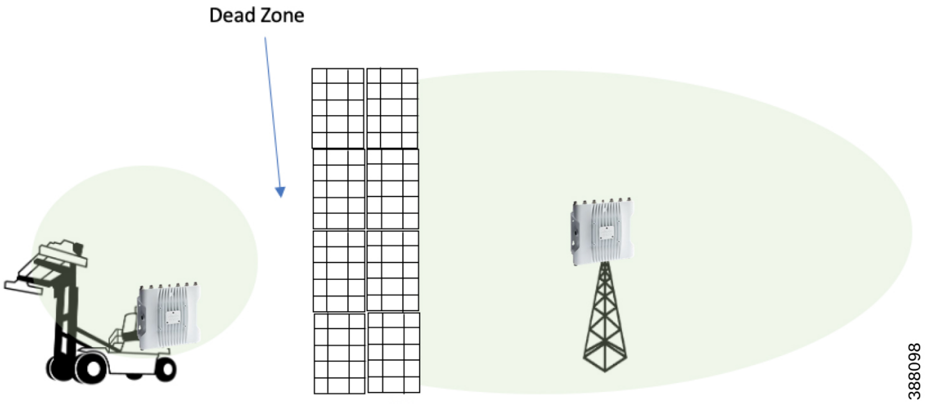
For TOS application within ports, the following types of vehicles and their RF coverage need to be considered:

- Small vehicles operating at a height of approximately 7 ft (2 m), such as terminal tractors and reach stackers
- RTGs operating at a height of approximately 82 ft (25 m)
- Tall STS/quay cranes with a height of approximately 131 ft (40 m), where the antennas can be installed at different locations either on the legs of the crane or on top of the crane

It is important to note that the height of installation of the antennas must be above the maximum height of the container stacks within the terminal.

Align each antenna with care, referring to the link profile diagrams that were generated during the high-level system design. Always maintain clear line-of-sight, making sure there are no physical obstacles, especially metallic obstacles, between radios that are connected using a wireless peer link. At least 60% of the Fresnel zone between the two radios must be clear and free of any physical obstacles.

Figure 32: Beware of Dead Zones Created Due to a Tall Stack of Containers Between a Ground Vehicle and the Access Radio



DFS Considerations

Dynamic Frequency Selection (DFS) is a reserved services detection and avoidance function where selected 5 GHz frequencies are scanned for generally reserved radar, satellite, and weather radar. DFS is a major concern within any port and terminal deployment. The DFS operation within CURWB is different from typical Wi-Fi deployments. While Wi-Fi based solutions use multiple channels dynamically within the entire port, including DFS frequencies (if selected within the controller), CURWB uses fixed channels with a minimum use of spectrum to deploy critical applications.

Deploying CURWB using multiple channels is possible (vehicle radios configured in autoscanning mode). If only one of the infrastructure radios that is operating in the DFS frequency band detects the radar signal (there is no capability for vehicle radios to detect DFS), only that particular radio disables itself for 30 minutes, even if other infrastructure radios are configured within the DFS range. Radios that have not detected the radar signal continue to operate normally.

Post Installation: RF Tuning and Optimization

While the output from the survey work is critical for the planning and design phase of a project, there is additional work that needs to be performed after deployment and installation. To validate that the installed solution aligns with the specifications of the design and meets application requirements, conduct another survey after the wireless equipment has been deployed within the port or terminal.

This validation may be done over time in phases, which align with a phased construction and implementation schedule. However, the fundamental purpose is to conduct an RF survey, using previously described tools and techniques, to tune and optimize the wireless system, ensuring that it provides the necessary coverage and meets the design requirements. Due to the dynamic nature of a container terminal, RF tuning is an ongoing requirement and cannot be ignored.

Ports and Terminals: Specific RF Considerations

In the case of a greenfield port, the initial site survey and installation might have been done with just a few stacks of containers at the port. As the port starts getting busy, loads of containers and vehicles might block the RF LoS and Fresnel zone. An area that previously had good RSSI might become an RF dead zone due to a stack of tall containers between the area and the access radio. Therefore, it would be prudent to redo the RF site survey and adjust the following to address any gaps in RF coverage:

- Number and location of infrastructure radios
- Add radios to provide coverage to RF dead zones due to a new obstruction that popped up
- Infrastructure radio and antenna placements, height, direction, angle, power, gain
- Vehicle radio and antenna height, power gain

The port needs to be designed so that loads of container do not affect the RF environment. The RTGs and STS/quay cranes always operate above the maximum container stack height, so all antennas are going to be installed above the maximum container stack height. For small vehicles, as mentioned before, consider the maximum container stack of the terminal and make sure that all antennas are above that level. Also ensure that the the alignment of antennas is proper and covering the interested area.

Ports and terminals are dynamic environments, and the RF environment can change quite a bit from day to day. For existing brownfield ports, we recommend taking at least a couple of site surveys on different days and times to assess any gaps in RF coverage due to the dynamic nature of the RF environment at a port. Again, any coverage gaps can be addressed by modifying some or all the items listed above.

After the design phase and system deployment, further testing and heat map generation should occur. Based on the results further tuning should happen. The tuning steps are as follows:

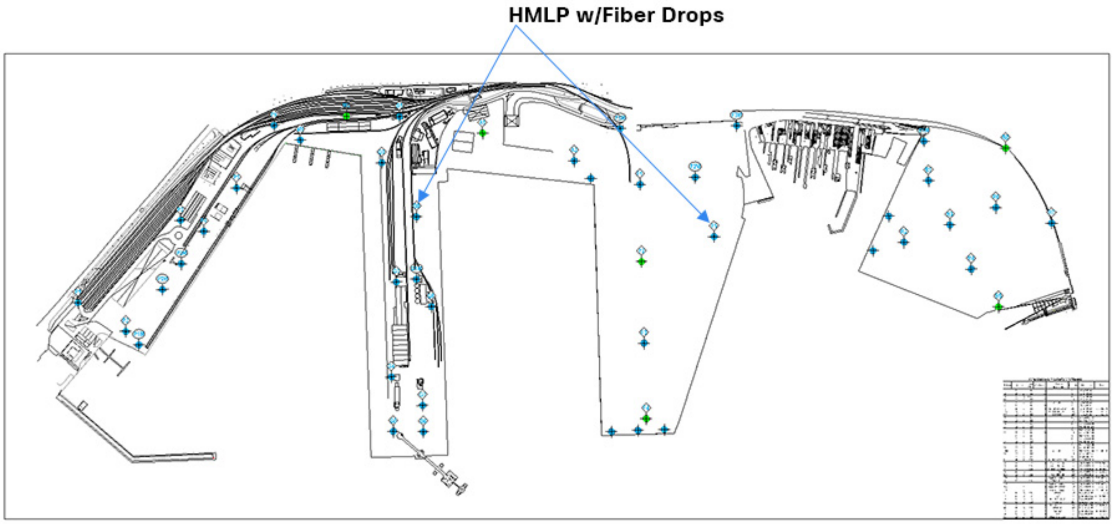
1. Add more radios to locations with poor performance (some radios need to be kept to add to the system in this step).
2. Align the antennas if the RSSI level is lower than expected.

3. Implement static multifrequency and load balance vehicles across different frequencies if congestion is more than expected (or increase the channel width on the system).

Terminal Map with Locations of all HMLPs with Fiber Connectivity

The following figure shows a typical comprehensive map of a container terminal with the locations of all available HMLPs equipped with fiber drops. Remember, the greater the number of available fiber drops, the smaller the number of radio-based backbone links that are needed.

Figure 33: Terminal Map with Locations of all HMLPs with Fiber drops



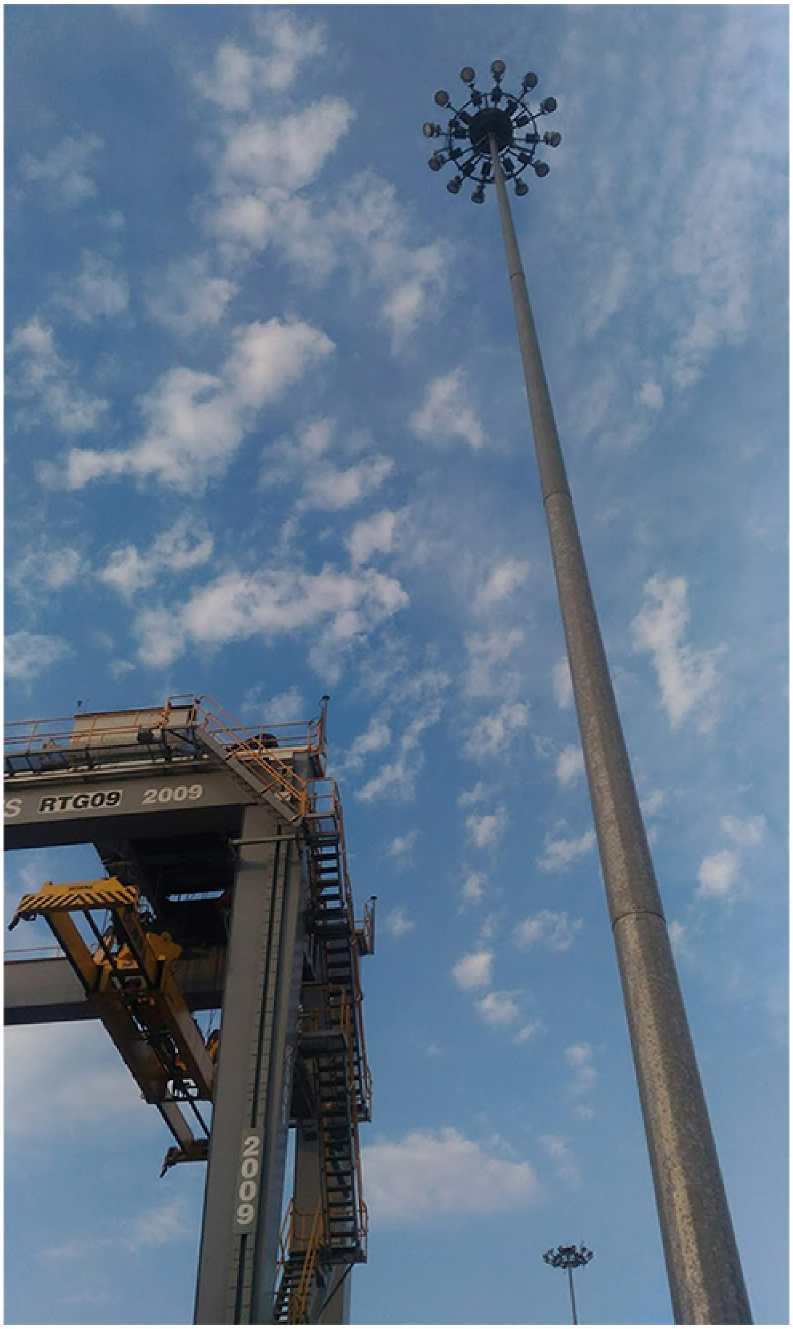
Type of Light Pole

Evaluate what kind of light poles are available within a terminal. Most terminals have circular light poles on which nothing can be installed on the pole itself. Different sets of radios and antennas are used here, one providing coverage to the high STS/quay cranes and the second radio or directional antenna pointing down toward the lower ground vehicles.

Radios can be installed only on the top of the HMLP on a circular metal rod. On these light poles, it is possible to install the radios or antennas at a height of 115 ft (35m).

Different sets of radios and antennas are used here, one providing coverage to the high STS/quay cranes and the second radio or directional antenna pointing down toward the lower ground vehicles.

Figure 34: HMLP where Radios and Antennas can be Installed Only on the Metal ring at the Top of the pole



The second type of light pole seen within ports and terminals is a tower on which you can install radios or antennas at various heights, providing deployment flexibility. On such light poles, one radio and antenna set can be installed at a height of approximately 10 to 13 ft (3 to 4 m) for smaller height vehicles such as terminal tractors and reach stackers. The next radio and antenna set can be installed at a height of approximately 82 ft (25 m) for RTGs. The third radio and antenna set can be installed at a height of approximately 130 to 150 ft (40 to 46 m) to provide coverage to STS/quay cranes.

Providing Wi-Fi Connectivity Within Ports

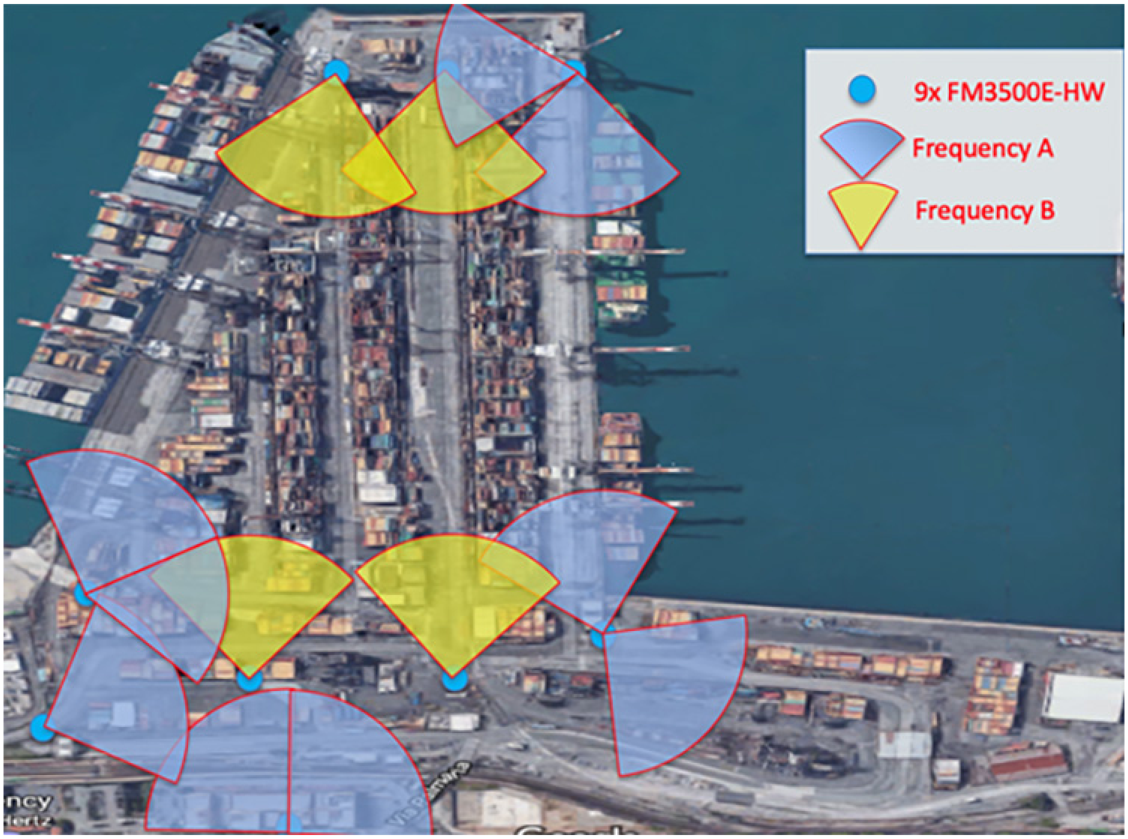
There are some areas within a port or terminal where Wi-Fi connectivity for handheld devices needs to be provided. For example, under STS/quay cranes, there are some workers carrying tablets for which Wi-Fi connectivity is needed. In this case, service cars can be used. A service car is a normal vehicles in a port or terminal that is equipped with a CURWB radio operating in the 5 GHz spectrum and a Cisco Wi-Fi access point operating in the 2.4 GHz spectrum. Service cars can move anywhere within a port or terminal and provide WiFi connectivity where needed.

Another deployment option is to use Cisco Wi-Fi access points operating in the 2.4 GHz spectrum and installed in a fixed location using CURWB fixed infrastructure to backhaul the Wi-Fi traffic.

Radio-Density Based RF Planning

Due to their requirements for uninterrupted connectivity, a multifrequency setup may be required for TTs and RSs in scenarios with a high vehicle density. The following figure shows an example CURWB multifrequency deployment at a port and terminal to support a high density of TTs and RSs.

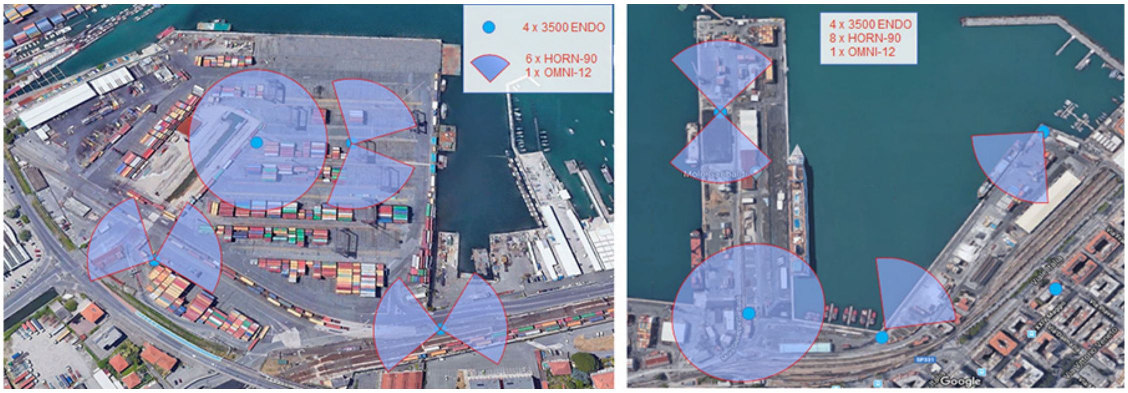
Figure 35: Radio-Density Based RF Planning



Radio Location and Antenna Type

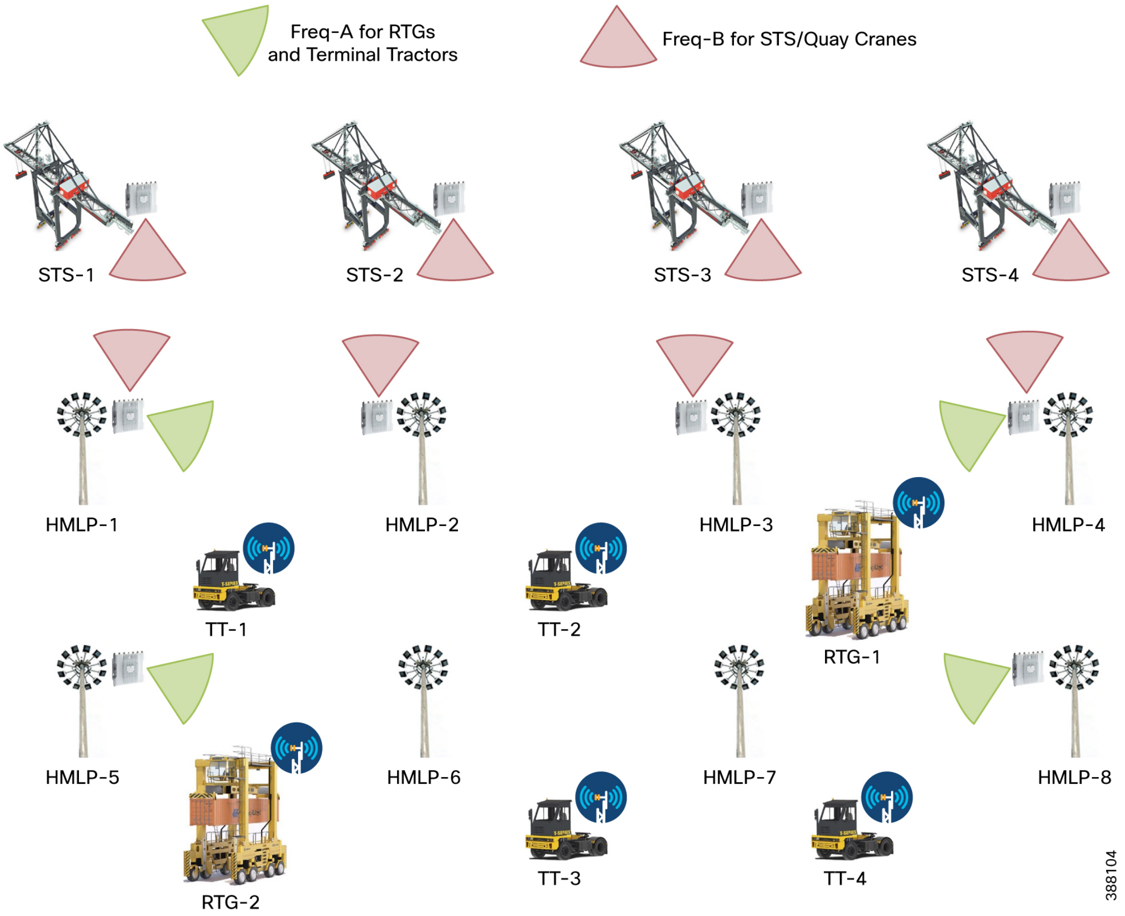
Pay close attention to the topography of the port or terminal site. Which areas are likely to cause line of sight issues or radio reflections? Are there any known "dead zones" on the site? These factors have a direct influence on the selection of omnidirectional and unidirectional antennas at every point in the backbone and access networks.

Figure 36: Location of Radios and Type of Antenna



Example CURWB Multifrequency Deployment for TOS

Figure 37: Example CURWB Multifrequency Deployment for TOS



The preceding figure depicts an example of a multifrequency CURWB deployment to enable TOS. The green radios are configured to operate on Freq-A and the red radios are configured to operate on Freq-B.

The green radios provide coverage to the RTGs and TTs. The red radios provide coverage to the STS/quay cranes. Because the IW9167 contains multiple radios, the red and green radios are considered to be one physical unit with different sets of antennas.

Because the height of the RTGs and TTs is much lower than the height at which the green radios are installed, the Horn-90 directional antennas are pointed down to provide appropriate coverage. The Horn-90 directional antennas for the red radios are pointed toward the radios that are installed on the STS/quay cranes.

Because RTGs and TTs typically move all around the port, make turns, and potentially move around 360 degrees, they are installed with omnidirectional antennas. The STS/quay cranes are deployed with the Horn-90 directional antennas directed toward the red infrastructure radios.

The solution is deployed in a way that redundant coverage is provided across the entire port if there is a failure of any of the infrastructure radios. For example, the red radio on HMLP-1 provides coverage to STS-1. If there is a failure of the red radio on HMLP-1, the red radio on HMLP-2 provides adequate coverage to STS-1. The same concept of overlapping coverage applies to the green radios providing coverage to the RTGs and

TTs. The green radio on HMLP-5 provides coverage down the entire aisle all the way until HMLP-8. Similarly, the green radio on HMLP-8 provides coverage down the entire aisle all the way until HMLP-5. If any radio at either end of the aisles fails, the radio at the other end of the aisle provides adequate coverage for the entire aisle.

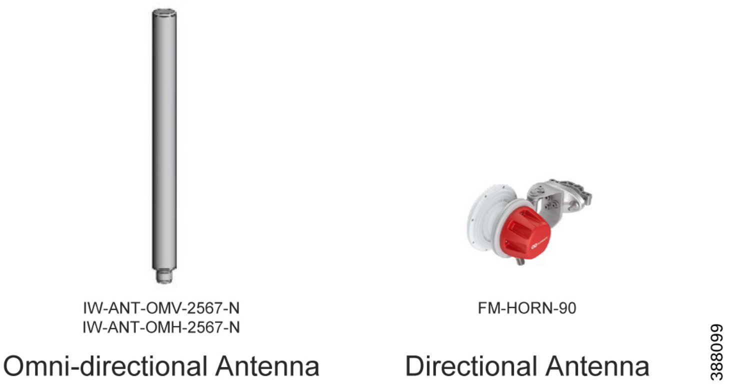
For small ports that have low vehicle density (fewer than 50 vehicles) a single-frequency deployment model can be adopted in which all the radios can be configured to operate on a single frequency. For large ports that have a high vehicle density (more than 200 vehicles), an additional infrastructure radio can be installed and configured to operate on a third frequency (Freq-C) to dedicate a separate set of radios providing coverage to RTGs vs. TTs. This configuration helps reduce the cochannel interference and channel utilization on each of the frequencies.

CURWB Radio and Antenna Installation Best Practices

Access Radio Installation: Access Radio Antenna Types and Application

It is worth examining the roles of different antennas in access and mobility networks.

Figure 38: Access and Mobility Network Antenna Types



Within an access network:

- Omnidirectional antennas are well suited for:
  - TOS and other applications with modest bandwidth needs
  - Vehicles that change their orientation through 360 degrees
- Directional antennas are well suited for:
  - OCR, automation, and other application that require connection reliability and thus reduced interference
  - Application in which the network may be vulnerable to radio interference, and in areas with relatively high levels of congestion across the radio frequency spectrum
  - Use on vehicles that do not move 360-degrees (for example, for STS/quay cranes)
  - Longer distance focused coverage

- Areas where omnidirectional antennas might cause radio interference

Note that ports and terminals are usually located within short distances of major population centers. For this reason, they typically feature higher levels of activity across all parts of the radio spectrum. This situation can cause the available RF spectrum within a port or terminal to be limited.

Access Radio Installation: Access Radio Deployment using 90-Degree Horn Antennas

Access radios within ports and terminals deployments typically are mounted on HMLPs. HMLPs with fiber connectivity always are preferred over HMLPs with no fiber connectivity. If certain HLMPs have no fiber connectivity, the design can incorporate having a wireless backhaul link.

The areas within a terminal that need uninterrupted radio coverage depend on what is taking place in each area. To establish whether uninterrupted radio coverage can be applied from a suitable height above the ground, a comprehensive map of the terminal showing the location and height of all available light poles and which of the poles have fiber drop links nearby is needed. Also required is information about the locations where vehicles are expected to moving and need coverage, and the number and types of moving vehicles that need connectivity. The greater the number of available fiber drop links, the smaller the number of wireless backbone links that are needed.

To ensure a proper design, data on the height of each vehicle must be considered. This information helps to determine at what height the access radio should be installed, the type of antennas to select, and at what angle the antennas need to be tilted.

Access radios can use one of the following 90 degree horn antenna configurations:

- Radio with one antenna design: offers long-range coverage in the intended direction
- Single 5 GHz radio with dual antenna design: offers coverage in two directions using all four ports on the 5 GHz radio
- Dual 5 GHz radio with dual antenna design: offers coverage in two directions using two ports on each 5 GHz radio

90 degree horn antennas are the preferred antenna type for use within a ports and terminal deployment due to their appropriate 90 degree horizontal and vertical beamwidth. These antennas can be tilted down to provide appropriate coverage within the aisles that are formed by tall stacks of containers. One radio with a 90 degree horn antenna tilted down can be installed at a height of approximately 50 ft (15 m) to provide coverage to ground vehicles moving about the port. A second radio with a 90 degree horn antenna can be installed higher, at an approximate height of 75 ft (23 m) to provide coverage to RTG cranes that have significantly higher heights than ground vehicles such as TTs or RSs. Note that installing radios and antennas at different heights is not possible on HMLPs where equipment can be installed only on the metal ring at the top of the pole, which is an approximate height of 115 ft (35 m).

Figure 39: Single and Dual 90 Degree Horn Antenna Design for Access Network

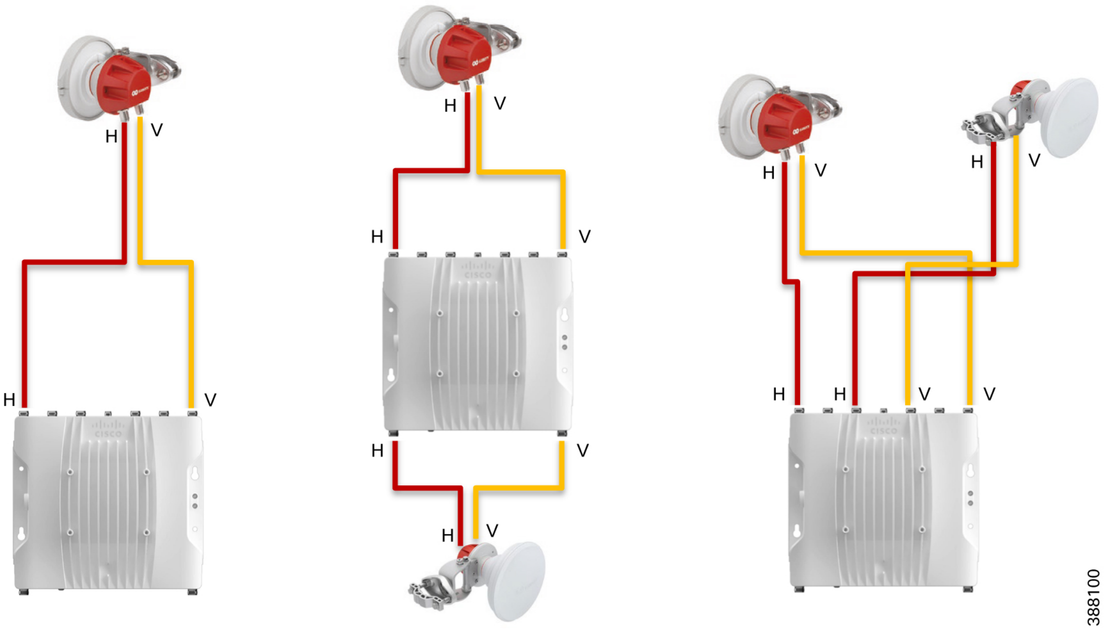
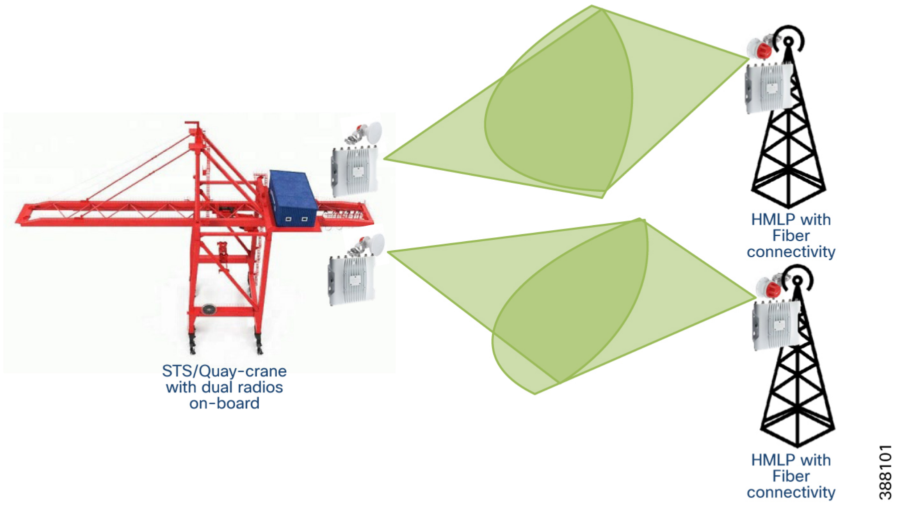


Figure 40: Highly Available Deployment for STS/Quay Crane



The preceding figure shows an example deployment of dual radios on board an STS/quay crane to provide redundancy at the mobility layer the vehicle. In this case, the HORN-90 directional antenna that is associated with each onboard radio points toward two separate infrastructure radios on neighboring HMLPs. This deployment model serves the dual purposes of providing hardware redundancy on board the vehicle and redundant coverage from two different infrastructure radios that provide resiliency against an HMLP power failure or fiber link breakage.

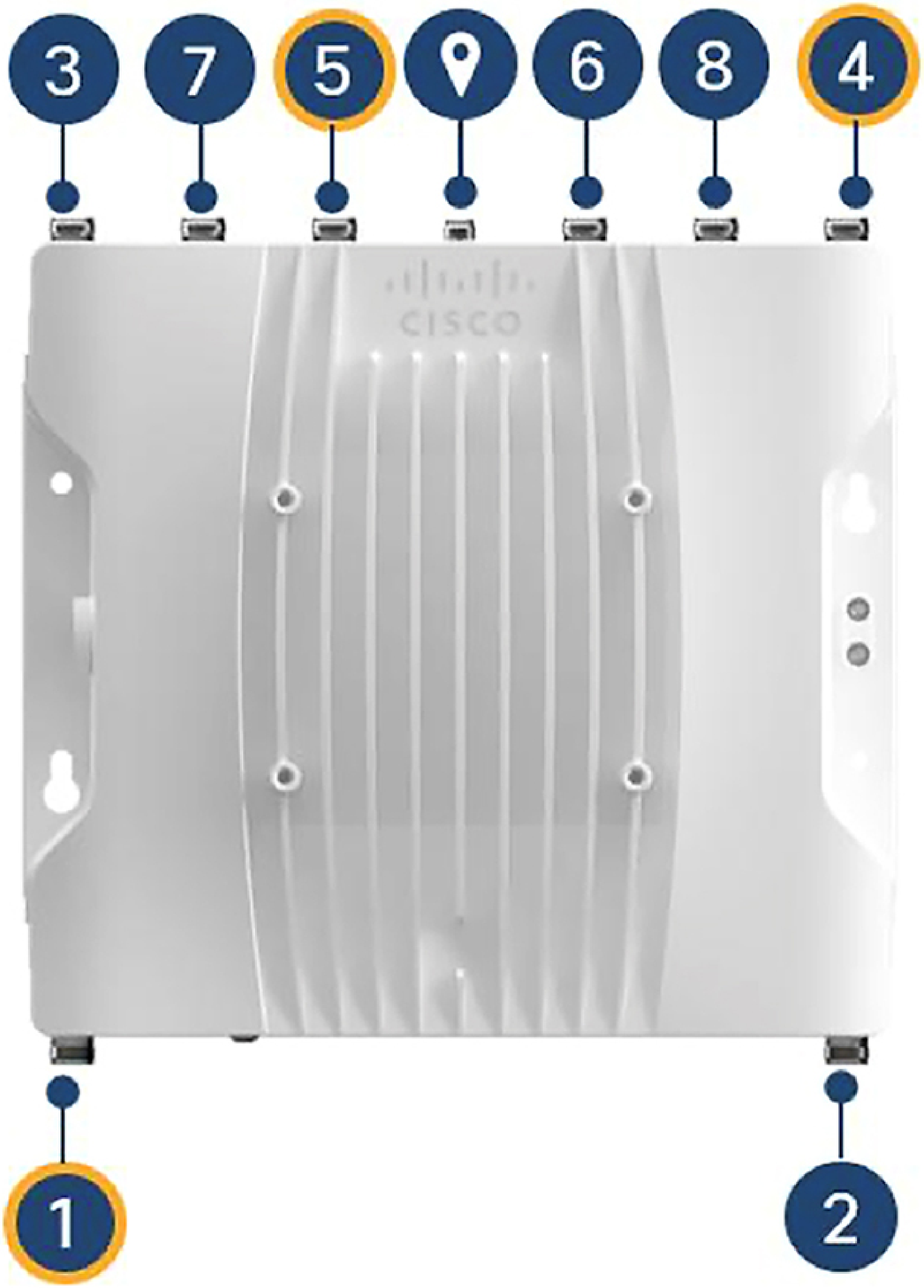
Vehicle Radio Installation: Antenna Cabling for Vehicle Radio

We recommend that tri-band omnidirectional antennas be installed on ground vehicles because these radios are able to receive and send signals in all directions. This functionality is needed as these vehicles move around a terminal and as they make turns.

The IW9167 has eight N-type antenna ports split between the 2.4 and 5 GHz radio and the other 5 and 6 GHz radio. Depending on the installation location on the vehicle, antennas can be directly connected to the radio ports or connected using RF cables. If both the 2.4 and 5 GHz and the 5 and 6 GHz radio are used, the omnidirectional antennas can’t all be connected directly to the radio. One set of antennas must be connected via RF cables in this case.

The IW9167 must also be powered keeping in mind the desired radio functionality. Full radio functionality requires DC power or a switch providing 802.3 bt power (uPOE).

Figure 41: IW9167E Antenna Numbering



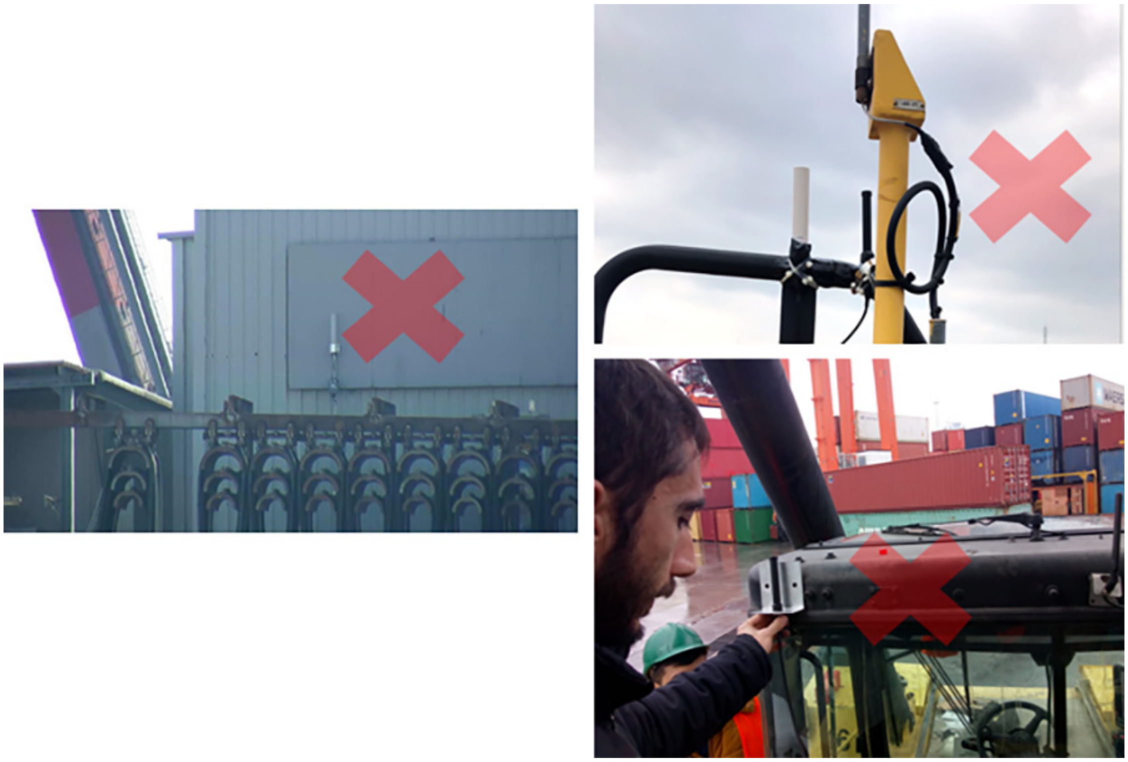
Antenna ports 1 through 4 are for the 2.4 and 5 GHz radio and ports 5 through 8 are for the 5 and 6GHz radio. Some antennas have circuitry that allows communication with the radio to automatically populate regulatory parameters. Called self-identifying antennas (SIA), they are supported on ports 1, 4, and 5 circled in yellow in the preceding figure.

Note Radios do not have knowledge about horizontal (H) and vertical (V) polarization. It is important to ensure that the same order for the H and V polarization is maintained across the entire deployment. If antenna port 1 is selected as H and antenna port 2 is selected as V, this convention should be followed across all radios in a given deployment. If not in cross-polarization and signal degradation occurs.

Clear Line-of-Sight and Fresnel Zone

This section shows examples in which the line-of-sight (LoS) and Fresnel zone have been blocked by metal obstructions around an antenna. Unidirectional antennas can also experience LoS and Fresnel zone blockages. Careful planning and logistics are needed to ensure that antennas are placed high enough to avoid any blockages.

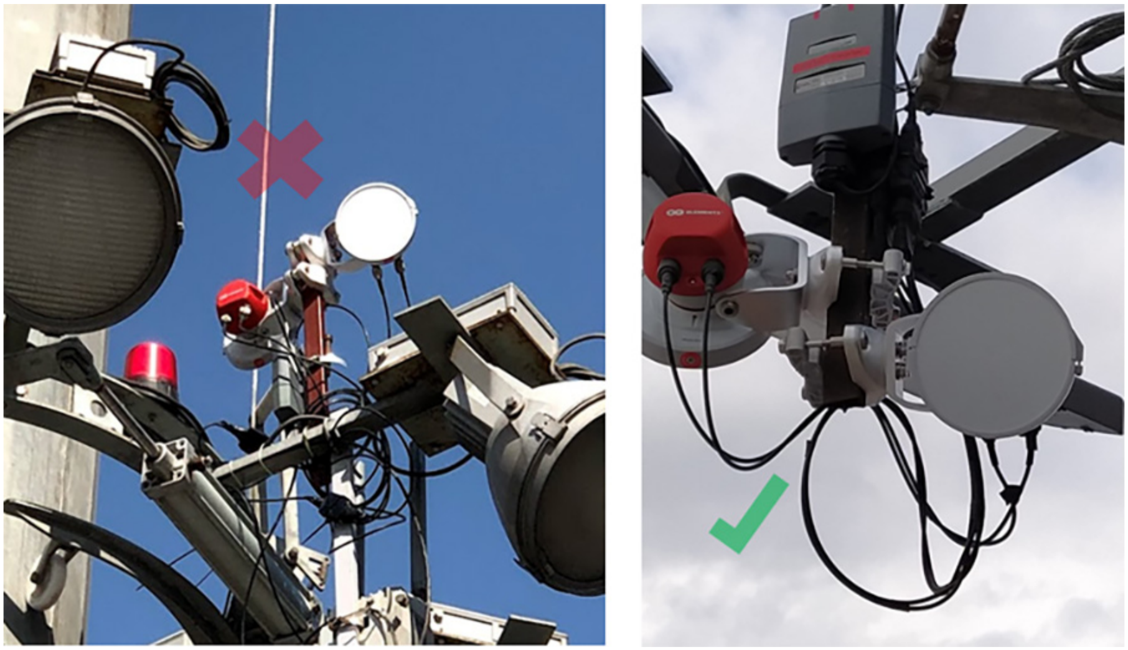
Figure 42: Roll-Out Best Practices: Avoid LoS and Fresnel Zone Blockages



Always take care to install each antenna in a way that takes full advantage of its radiation propagation pattern. This installation requires you to know the differences between each type of antenna within each antenna category. On some light poles, you may need accessories to mount antennas high or low enough to clear all obstacles that may interfere with the LoS.

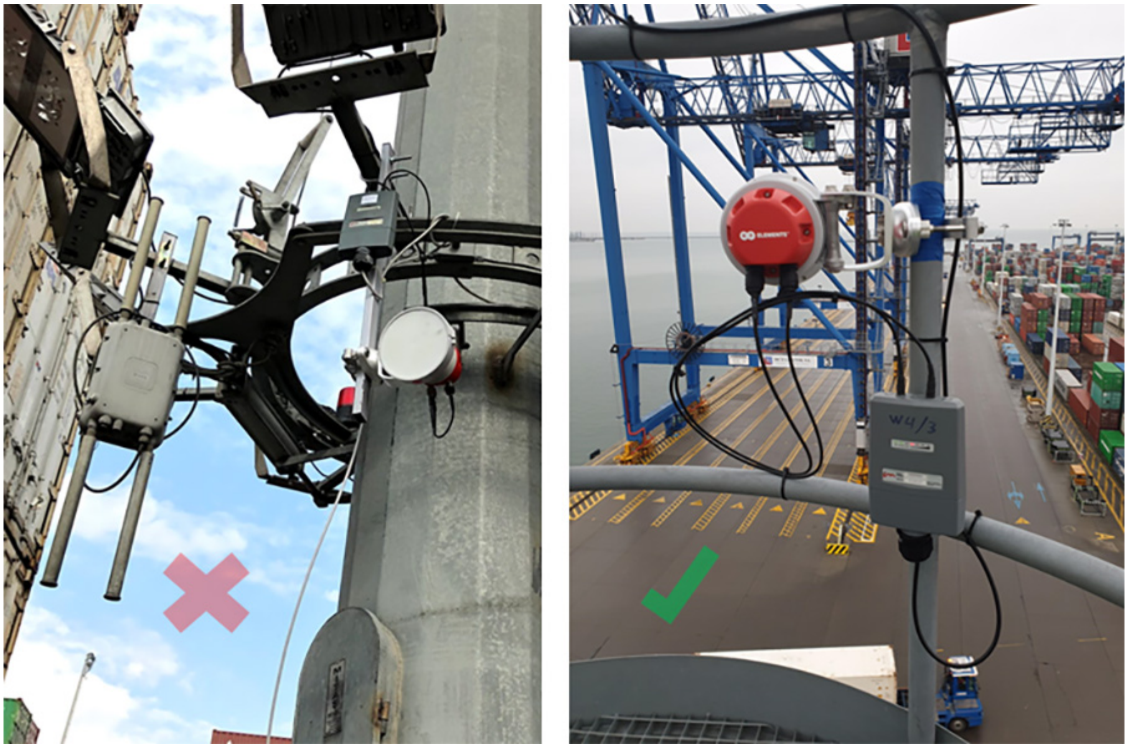
Do not install down-facing antennas above lights because the lights likely present physical obstacles to beam propagation. In these cases, it may be better to sacrifice a meter or two of height to guarantee freedom from LoS blockages.

Figure 43: Roll-Out Best Practices: Incorrect and Correct Antenna Installation



To avoid colocation interference, avoid installing radios and antennas close to any other wireless equipment, even if the other equipment operates on frequencies that are different than the CURWB equipment.

Figure 44: Roll-Out Best-Practices: Avoid Proximity to Other Wireless Gear



CHAPTER 5

Glossary

AGV	Automated guided vehicle
AIDC	Automatic identification and data collection
AutoSC	Automated straddle carrier
CPT	Connected ports and terminals
CRD	Cisco Reference Design
HMI	Human machine interface
HMLP	High mast lamp pole
IP	Internet protocol
IT	Information technology
LoS	Line of sight
MPLS	Multi protocol label switching
OCR	Optical character recognition
OT	Operations technology
PtMP	Point-to-multipoint
PtP	Point-to-point
QoS	Quality of service
RCS	Remote control station
RMG	Rail-mounted gantry crane
ROC	Remote operations center
RS	Reach stacker
RTG	Rubber-tired gantry crane

STS	Ship-to-shore
TT	Tractor trailer
VMT	Vehicle mounted terminal