Industrial Automation for Process Control and Refineries

Introduction

This design guide provides a comprehensive explanation of Industrial Automation for Process Control and Refineries system design. It includes information about the industry challenges, primary use cases, architecture, and guidelines for implementation. The guide also recommends best practices and potential issues when deploying the reference architecture. This document builds on the Connected Refineries and Processing Plant Cisco Reference Document (January 2016) available:
https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/connected-refineries-pocessing-plant.pdf

This release of this Cisco Validated Design (CVD):

- Aligns with the release of the new Cisco Hazloc Class1/Div 2/Zone2 hazardous location-certified industrial access point, the IW 6300. This guide provides best practices and design recommendations for:

    - Migrating from the 1552 access point to the IW 6300 in existing Brownfield deployments where the 1552 access points are currently installed.

    - Greenfield opportunities where wireless networking is being enabled in the process plants and refineries.

- Describes a secure, scalable, and robust wired and wireless architecture that addresses key challenges and use cases for refinery and processing plant environments. This architecture supports capabilities for both workforce-enabled use cases and wireless instrumentation use cases. The focus of this release is primarily on the design and implementation of the wireless network supporting refineries and processing plants.

- Provides architecture and design guidance for integrating wireless instrumentation 802.15.4 WiHART networks with the Emerson 1410 gateways and Rosemount instrumentation to the Cisco Wi-Fi Mesh networks.

- Includes Cyber Security architecture and guidance aligned with key industry standards such as NIST, IEC62443 Industrial Cybersecurity. This guide also introduces Cisco Cyber Vision for enhanced visibility of industrial devices and communication with anomaly detection for the OT assets and industrial protocols.

- Documents the suggested equipment and technologies, system level configurations, and recommendations. This document also includes descriptions of caveats and considerations that process control customers should understand as they implement best practices.

This document primarily focuses on addressing oil and gas refinery and processing plant issues though use cases and architectures. These solutions are applicable to other areas of the oil and gas value chain such as the oilfield, production platforms, and large pipeline stations in midstream including compressor or pump stations. The document includes:

- Process Plant and Refinery Overview provides an overview of the oil and gas value chain, industry challenges, and three areas of focus with high level use cases that address the challenges.

- Solution Overview and Use Cases addresses the high level design and low level use cases for the refinery and processing plant.

- Industrial Wireless Design provides low level design guidance for the wireless networks in the refinery.

- **Industrial Wireless Site Survey and Design Considerations** details challenges and site survey considerations for deploying wireless network in a refinery or processing plant.

Process Plant and Refinery Overview

This section describes the oil and gas value chain, industry challenges, and three high level use cases focused on addressing those challenges.

Oil and Gas Value Chain

At a high level, the oil and gas value chain starts with exploration to discover resources, then transitions through development, production, processing, transportation/storage, refining, and marketing/retail of hydrocarbons. This value chain is typically grouped into three areas:
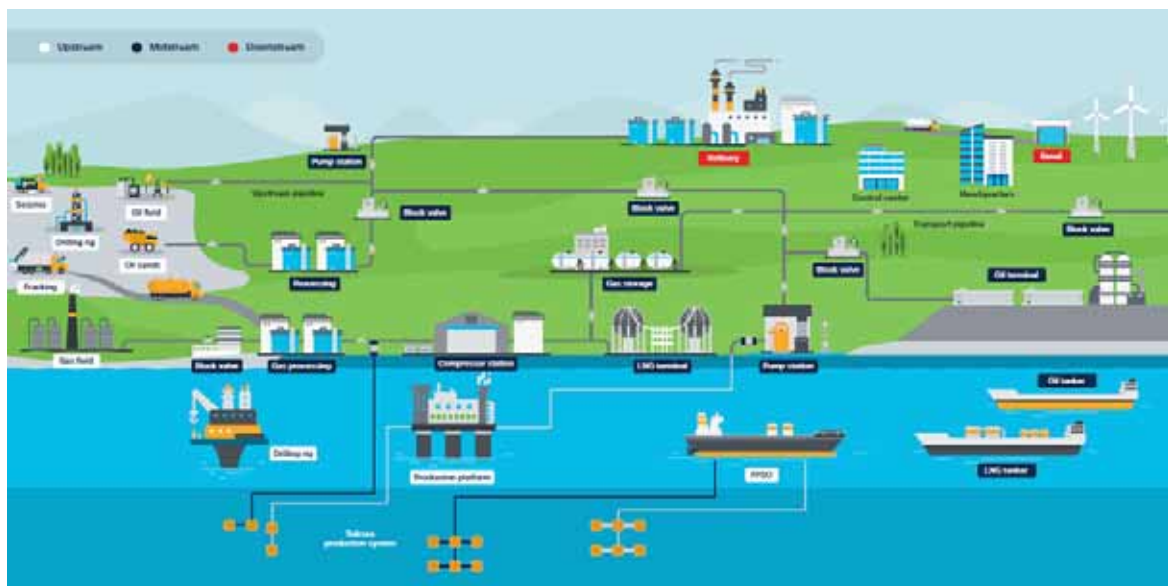
- **Upstream**—Includes the initial exploration, evaluation and appraisal, development, and production of oil and gas assets. This is referred to as Exploration and Production (E&P). These activities occur both onshore and offshore. Upstream focuses on wells and determining how to operate individual wells or entire basins to achieve the best return on investment.

- **Midstream**—Primarily focuses on the transport and storage of hydrocarbons via pipelines, tankers, tank farms, and terminals, providing links between production and processing facilities, and processing and the end customer. Crude oil is transported downstream to the refinery for processing into the final product.

  Midstream also includes the processing of natural gas. Although some of the processing occurs in the field near the source, the majority of gas processing takes place at a processing plant or facility, arriving there typically from the gathering pipeline network. For wholesale markets, natural gas must first be purified by removing Natural Gas Liquids (NGLs) such as butane, propane, ethane, and pentanes, before being transported via pipeline, or turned into Liquid Natural Gas (LNG) and shipped. The gas can be used immediately or stored. The NGLs are leveraged downstream for petrochemical or liquid fuels or turned into final products at the refinery. Processed natural gas is transported to gas distribution utilities for delivery to their commercial, industrial, and residential customers.

- **Downstream**—Concerned with the final processing and delivery of product to wholesale, retail, or direct industrial customers. The refinery treats crude oil and NGL and then converts them into consumer and industrial products through separation, conversion, and purification. Modern refinery and petrochemical technology can transform crude materials into thousands of useful products including gasoline, kerosene, diesel, lubricants, plastics, and asphalt.

Figure 1 highlights the value chain for oil and gas.

Figure 1   Value Chain for Oil and Gas

Refineries and processing plants are typically sprawling complexes with many piping systems running throughout, interconnecting the various processing and chemical units. Many large storage tanks also exist around the facility. The plant can cover multiple acres and many of the buildings and processing units on site are multi-stories high. The processing units and extensive piping networks are generally metal, spanning long distances between buildings or treatment areas. Plant equipment at the sites is continually being upgraded to ensure efficient operation. Some plant areas are potentially hazardous, handling highly-explosive gases from the chemical processes (see Industrial Wireless Site Survey and Design Considerations for details). Potential challenges from corrosion due to steam and cooling water around the site resulting in the possibility of deadly gas leaks are ever-present.

The refinery is a complicated working environment with complex equipment and extensive piping networks. Products are continuously being produced, requiring the system to be continuously monitored via pressure, temperature, vibration, and flow. At any one time, hundreds of workers including company employees, contractors, and external company support staff may be onsite. Plant operators ensure the entire process is working correctly, engineers monitor process efficiency and optimize or redesign where necessary, and maintenance staff ensure equipment is maintained, repaired, and safe. The transportation requirement to move raw materials or finished product in and out means that multiple vehicle types such as cars, trucks, oil tankers, and trains are also part of the refinery environment.

Management and safety systems keep all of the processes and people operating effectively, efficiently, and safely. To ensure these systems can operate in coordination across the refinery or processing facility, a comprehensive and reliable communications system must be implemented.

Industry Challenges

Oil and gas companies are facing distinct challenges across the industry: reduce costs, improve operational efficiency, productivity, and employee safety. The market downturn in 2014 forced oil and gas companies consider new and innovative ways to increase production, streamline operations across IT and OT, and explore new business and operating models. They found that "Digitalization" could be part of the answer. Many describe this as "Digital Transformation" or simply embracing "Digitization". New and existing data sources need to be accessed, regulations must be complied with, and the safety of employees must be ensured. Digital technology is now viewed by many as the enabler, particularly through the adoption of wireless-based technology. The following are broad challenges and trends facing the industry.

- **Worker Safety** is of the utmost importance—The ultimate goal is to achieve zero worker injuries, minimize the human factor, and provide a risk lens for plant or facility safety and security. New technologies are being used to provide visibility of worker location and life-safety wearables that are connected to the network, such as mobile detectors, can provide a near real-time view into risk across the plant.

- **Improve Productivity**—With greater visibility into operational workflows, the effort to improve average worker productivity (wrench time) in the field, whether for employees or contractors, has increased dramatically. With average wrench time estimates of around 18% in oil and gas, this means only two out of ten hours are spent on productive work. The industry is looking to technology and digitization to increase and perhaps double productive time.

- **Improve Operational Efficiency**—With greater agility to react to production-impacting failures, market trends, industry fluctuations, and shifting demand, operations are more efficient. Digitizing the oil and gas supply chain from upstream to downstream will be transformative. The adoption of Industry 4.0 and Internet of Things (IoT) sensor connectivity, wireless instrumentation, and leveraging digital technologies such as analytics, machine learning, and Artificial Intelligence (AI), will help enable oil and gas companies to make more informed decisions, improve productivity, and increase efficiency and safety.

- **Aging Workforce**—The oil and gas workforce is starting to age out and retire. The newer workforce is accustomed to connectivity and anywhere access to data, so companies need to innovate to help meet this expectation of mobile workers and improve visibility into operations.

- **Physical Security**—The more devices that are connect to the network, the wider the attack surface. With oil and gas companies adopting new technologies and use cases to help digitize and transform the business, new devices are connected to the network. This brings potential security attacks—intentional, unintentional, internal, and external—that can affect the business. In oil and gas this not only impacts production, but could affect worker safety or result in environmental incidents and hefty fines. Cyber security is not the only concern; physical security solutions such as video surveillance and access control are also needed.

Refinery and Processing Plant High Level Use Cases

A refinery or processing facility deploys several systems to ensure uptime, continuous operations, and safety of workers. Fundamentally a secure, robust, wired and wireless infrastructure must be implemented to keep all the systems, processes, and workers operating efficiently and safely across the entire plant.

Communications must support process control applications from the instrument or sensor to the control room application. Communications support the mobile worker with access to data and information to perform his or her role. The systems can be categorized as:

- Operational—Directly involved with supporting refinery operations such as the process control or safety systems.

- Non-operational—Such as multiservice applications that support the worker and operations within the refinery, but are not directly associated with process control. Examples of non-operational services include voice, video surveillance, condition-based monitoring, and remote expert services.

The operational and non-operational services fit into three core categories across the refinery and the oil and gas value chain (Figure 2).
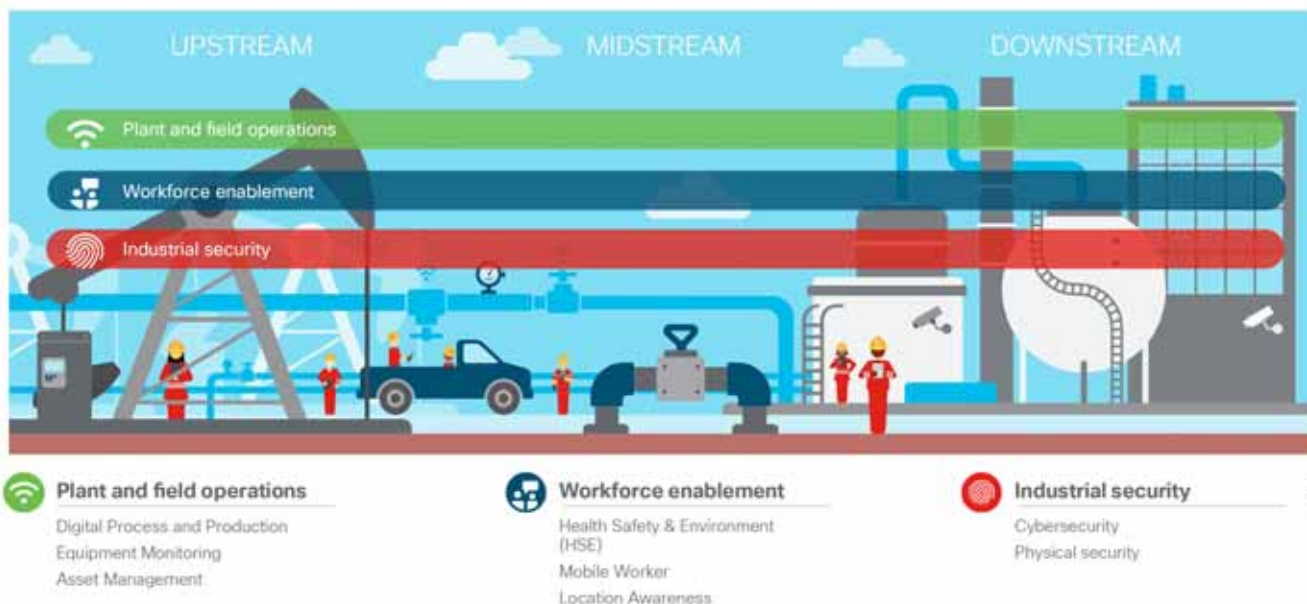
Figure 2   Core Categories

Table 1   Core Categories

Plant and Field Operations	Workforce Enablement	Industrial Security
Digital Process and Production	Health Safety and Environment (HSE)	Cybersecurity
Equipment Monitoring	Mobile Worker	Physical security
Production Asset Management	Location Services	

Plant and Field Operations

Plant and Field Operations provides operational and non-operational services supporting the process and equipment across oil and gas plants, facilities, or oil fields. The three high level use cases are described below. These use cases target uptime, operational efficiency and improved safety through continuous monitoring of the process, and equipment and assets within an oil and gas installation.

Digital Process and Production

This applies robust wired and wireless network communications with security and data management technologies to Industrial Automation and Control Systems (IACS) for real-time plant and field operations that are critical for production assets at the core of the business. Within the refinery this supports the Process Control Network (PCN), Safety and Power networks which at their core are focused on maintaining the stability, continuity, and integrity of industrial processes. Sensors, devices, controllers, and actuators must be available and managed to properly operate the industrial processes.

Equipment Monitoring

Collecting equipment data in near real-time provides the opportunity to optimize equipment performance and proactively detect issues before they occur. In most instances applications such as condition-based monitoring or predictive maintenance are not considered part of the critical process control. The data can be processed at the edge and then published to the cloud or on premise where it can be consumed. Predictive or proactive analytics can be leveraged in a facility to better manage asset maintenance on plant equipment such as motors, valves, and pumps. Typically the sensors are wireless *Wireless*HART or ISA 100 based. Depending on the criticality or location, the wireless sensor data is wired directly into control networks or backhauled over Wi-Fi networks.

Its worth noting that some instances of equipment monitoring may be part of critical process control. This then becomes part of the process or safety system under the scope of Digital Process and Production.

Asset Management

Across an oil and gas facility there are a number of non-critical assets that are not part of process control networks. Production Asset Management automates the collection of non-critical operational data and asset location using periodic, low-cost wireless communications. An example is non-process control related tank level monitoring or asset location awareness in parts of the refinery using LoRA Technology where regular 802.11 wireless is not deployed.

Workforce Enablement

There are several challenges within the oil and gas environments that affect worker productivity, efficiency, and safety. As noted earlier, attracting a younger workforce and retaining them is a major challenge facing the industry as the educated workforce retires. Enabling the worker with new technology such as wirelessly connected ruggedized tablets can provide them with real-time access to information to perform simple or complex operational tasks in the field regardless of location. Remote expert applications are another example. The expert is providing support services to the onsite field engineers for training and improved worker productivity. Near real time location services are key. They provide near real time visibility into assets and personnel throughout the workplace with the latter contributing to improved health and safety.

Health, Safety and Environment (HSE)

Health and safety is paramount throughout the oil and gas industry: upstream, midstream, and downstream. Protection of people, property, and infrastructure is key to preventing personnel loss and injury, and environmental incidents, ultimately providing a smart, safe, and secure workplace. Multiple high level and low level use cases contribute to HSE. Existing safety systems deployed in the plants can be enhanced with the ability to proactively view potential health and safety threats through equipment monitoring or pipeline integrity monitoring within a refinery. Providing mobile gas detectors with location awareness can provide data for real-time visibility of gas detection and personnel location in the refinery or processing plant. These use cases require a secure, robust wired and wireless infrastructure to enhance HSE within the oil and gas industry.

Mobility

Mobility is a major contributor to optimized operations and efficiency in oil and gas. Typically, field personnel perform work using information from unconnected ruggedized laptops in the field or from paper-based documents. As companies strive to improve operations, they have deployed wireless networks to enable the workforce and gain access to data on demand. Workers with safe tablets and devices can now gain access to data and update information in real time. Access to equipment manuals on demand, updating work orders remotely, and access to advanced applications such as remote expert while out in the field ultimately provide huge improvements in worker productivity.

Location

Keep workers safe and optimize productivity by always knowing who is where and what they are doing—in the field, along the pipeline, or in the refinery. Asset location tracking technologies such as RFID tags across an IEEE 802.11 wireless network or GPS-enabled sensors connected to the network enable other use cases described in this CVD (see Solution Overview and Use Cases). Plant administrators, security personnel, users, asset owners, and health and safety staff have all expressed interest in location-based services to help them address several issues in the plant. Managing the location of assets and personnel throughout the plant is key to improving operational efficiency and improving safety and regulatory compliance. Location-based services and tracking:

- Improves safety for personnel and property

- Provides visibility into personnel behavior or presence in risk-associated areas with geo-fencing

- Provides insights into worker efficiency for the business to streamline workforce tasks and schedule the workforce efficiently

- Reduces nonproductive time and helps locate correct machinery assets

- Contributes to improved turnaround and cost savings during Shutdown/Turnaround and Outage (STO) events

Industrial Security

Historically, a security-by-obscurity approach was adopted for the process control domain. Networks were seen as standalone with no public access, proprietary protocols were assumed as being difficult to understand and compromise, and security incidents were more likely to be accidental. As oil and gas companies continue to adopt new technologies and use cases, new and diverse devices are being connected to the network. This brings with it a potentially wider set of security attack challenges (intentional, unintentional, external, and internal). To address these, companies need to adopt a comprehensive cyber security framework. As the domains between Operational Technology (OT) and Information Technology (IT) converge, they must also align security strategies and coordinate to ensure end-to-end security. In addition to cyber security, physical safety and security solutions that include video surveillance, access control and analytics are required. A foundation for security must include both cyber and physical elements to best protect the process control environment.

Cyber Security

IoT devices in the oil and gas environment collect a wealth of real-time, real-world data that can be crucial to achieving goals around improving operational efficiency, optimizing equipment operation and maintenance, safeguarding workers, and addressing compliance requirements. Commercial off-the-shelf (COTS) products are increasingly used in oil and gas to perform tasks that were originally assigned to purpose-built equipment. COTS products come with more potential vulnerabilities, and therefore greater security risk; they dramatically increase the size of the potential attack surface. Oil and gas companies have varying degrees of cyber security maturity, so a staged approach to implementing cyber security in alignment with key security standards such as IEC 62443 and NIST should be considered.

Initially oil and gas companies can implement comprehensive visibility of the environment and create a baseline of connected assets. A risk assessment can then be made to measure and identify potential risks and establish a baseline of the environment. The company can further segment zones and conduits, develop and deploy consistent security policies to each segment, form mitigation strategies, and review the assessment regularly—making updates to reflect new equipment and new threats.

Physical Security

Physical security solutions provide broad capabilities for video surveillance, IP cameras, electronic physical access control, incident response and notifications, and personnel safety. Integrated solutions using connected cameras, electronic physical access control, geo-fencing perimeter protection solutions, and third-party intrusion can provide end-to-end support for safety and security detection, monitoring and management, and threat response across upstream, midstream, and downstream environments. Examples include video surveillance to provide perimeter security integrated with access control systems for an employee who swipes an access card to gain entry, and used for emergency incidents in the facility such as gas leaks or mandown to assist safety staff and first responders.
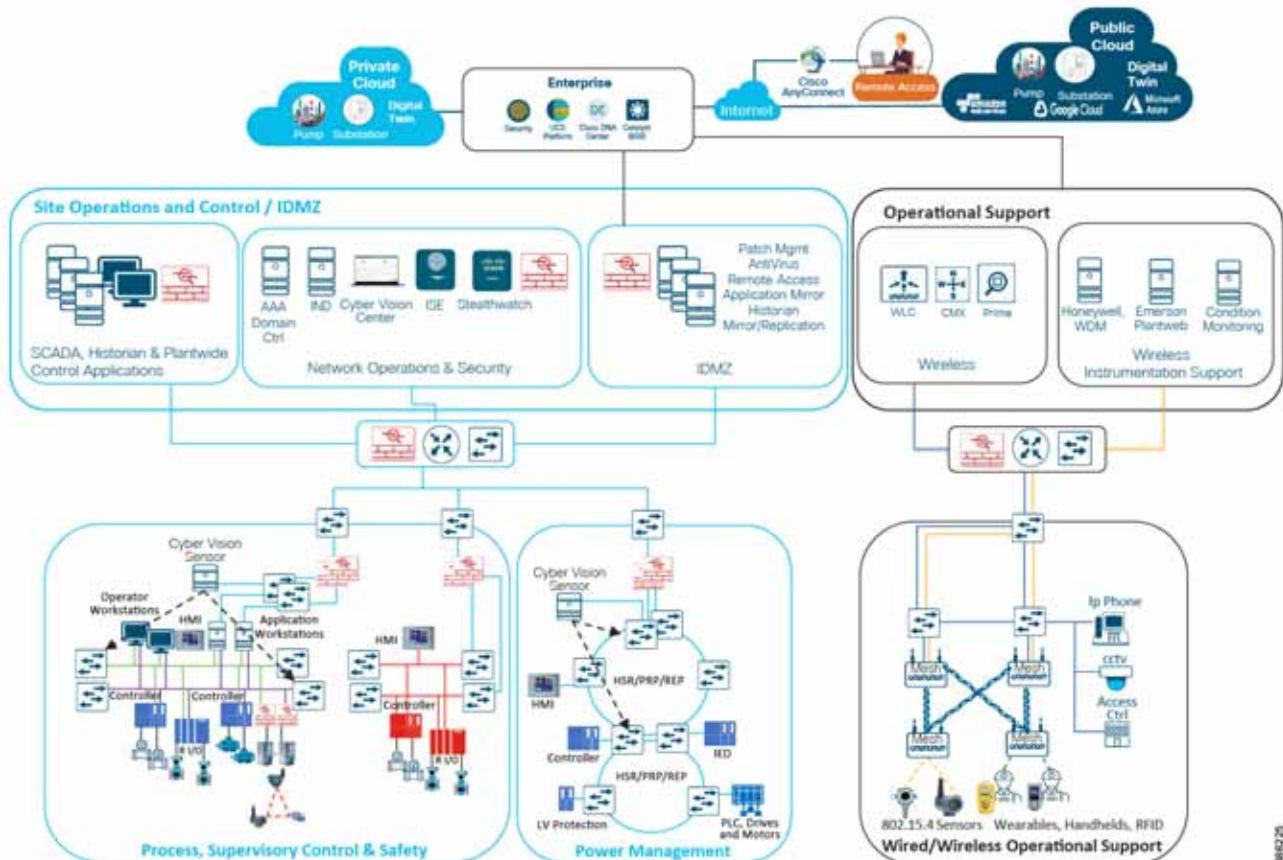
Solution Overview and Use Cases

Reference Architecture Overview

The Cisco oil and gas process control and refineries CVD defines a reference architecture to support multiple operational and non-operational services over a secure, robust communications infrastructure. The architecture applies wired and wireless network design, security, and data management technologies for process manufacturing environments. The reference architecture in Figure 3 is a blueprint for the security and connectivity building blocks required to deploy and implement digitized process control and refinery environments to significantly improve safety and business operation outcomes. The building blocks include:

- Wired process control networks with safety and energy management systems

- Industrial wireless network supporting the mobile worker and wireless instrumentation

- Industrial security throughout the plant including the Industrial DMZ

The use cases and building blocks described in this guide provide a complete end-to-end view of the reference architecture, although the focus of this guide is on the use cases and architecture enabled through 802.11 and 802.15.4 wireless technologies. The wired network and security architecture is built from the Industrial Automation CVD: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-Automation DG.html. The reader should be familiar with the architectural guidance and design principles in that guide, although there are some slight differences between the oil and gas process control environment and the industrial automation design which are highlighted in Oil and Gas Process Control and Refineries Reference Design—Wired.
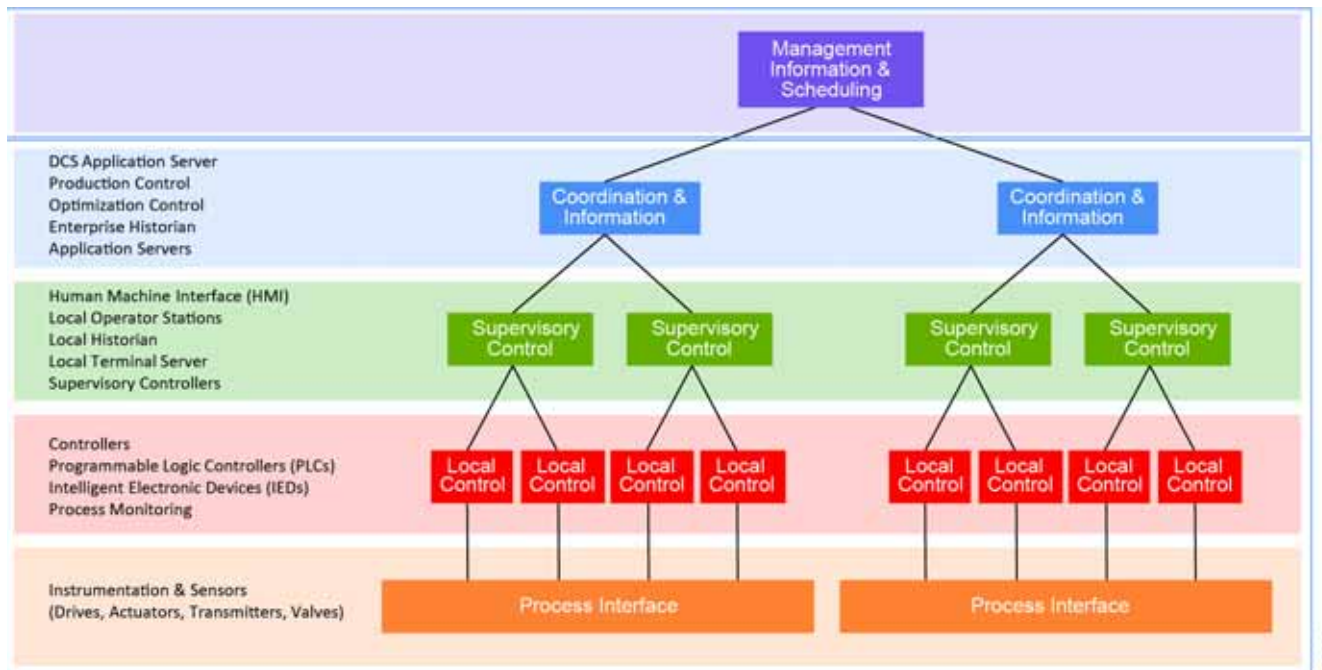
Figure 3   Reference Architecture

Process Control and Distributed Control Systems

A refinery or processing facility deploys many systems to ensure safety and reliability. Communications must support process control applications from the instrument or sensor to the control room applications. Historically, several of these systems would have been deployed independently; however, most process control vendors now offer integrated solutions incorporating many or all of the functions into common platforms. The typical plant will employ a Distributed Control System (DCS) that divides the control tasks into multiple distributed systems, so that if a part of the system fails, the other parts continue to operate independently. Figure 4 depicts the DCS model.

Figure 4   Distributed Control System Model

A DCS is process-driven rather than event-driven and typically produces a steady stream of process information with less reliance on determining the quality of data, as communication with control hardware is much more reliable. The DCS typically consists of multiple controllers or PLCs implementing multiple closed-loop controls. This makes them suitable for highly-interconnected local plants such as process facilities, refineries, and chemical plants.

Safety Systems

Ensuring safety and reducing risk in the production environment is key to any refinery operation, with priority on protecting workers and the surrounding environment from the accidental release of material. This is especially relevant in refineries and process manufacturing facilities where high temperatures and pressures, and hazardous materials are handled. Safety-instrumented systems are deployed across the plant to maintain safe operations when an anomalous or dangerous condition occurs. These systems are independent from the process control systems that control the same equipment or processes, ensuring that safety systems are not compromised. Because safety systems are so critical, a robust, secure, and redundant network is required to ensure high availability and integrity of these systems.
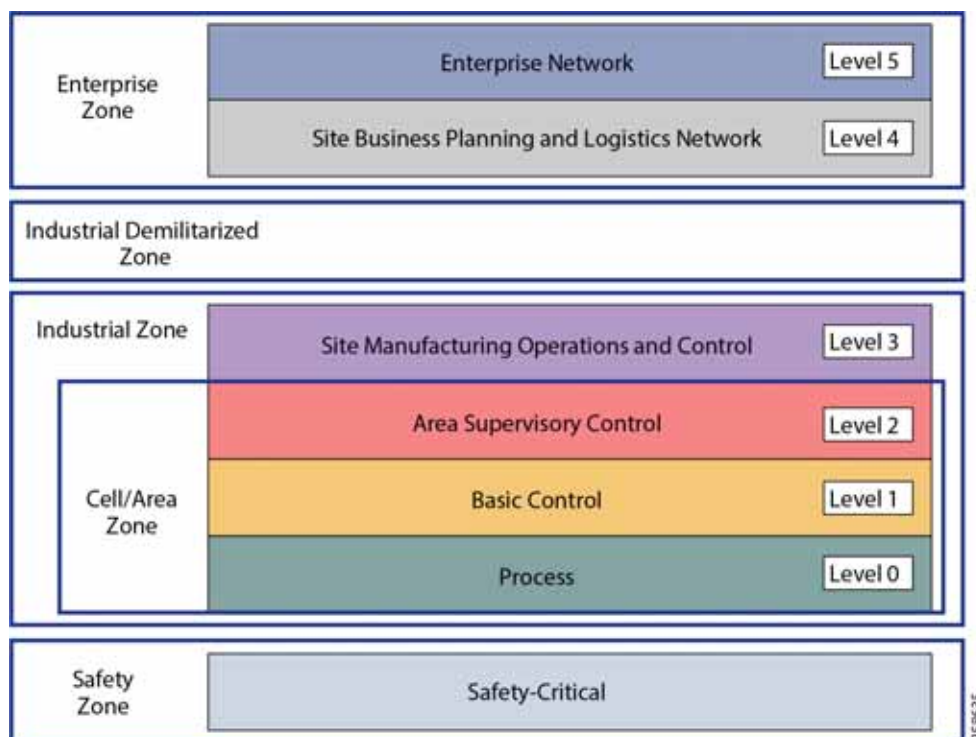
Energy Management and Non-process Systems

Within refineries and processing plants there are many non-process control related systems and facilities including power generation, energy monitoring systems, tank storage, flaring, and control rooms. Energy monitoring and control systems can play a substantial role within a refinery to manage and improve energy performance, energy re-use, and reduction in emissions. Most refineries and processing plants include energy-intensive processes with some form of

power generation and co-generation or combined heat and power generation (CHP). CHP uses internally-generated fuels for power production, which yields a significant cost savings and improved energy efficiency in a refinery. Networks are required for energy management, power generation, and non-process control related systems within refineries or processing plants. Mostly wired, these networks may have wireless instrumentation in the plants, such as 802.15.4 WiHART or ISA100.11A sensors that relay equipment metrics like vibration and temperature.

Plant Logical Framework

To understand the security and network system requirements of a PCN, this guide uses a logical framework to describe the basic functions and composition of an industrial system. The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the industry that segments devices and equipment into hierarchical functions.

Figure 5   Plant Logical Framework

The model shown in Figure 5 identifies levels of operations and subsequent sections highlight their functions. More information about the model can be found in the Industrial Automation CVD:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

Safety Zone

Safety in process control systems is so important that not only are safety networks isolated from the rest of the process control, they typically have color-coded hardware and are subject to more stringent standards. In addition, Personal Protection Equipment (PPE) and physical barriers are required to promote safety.

Cell Area/Zone

The Cell/Area Zone is a functional area within a plant facility; many plants have multiple Cell/Area Zones. Larger plants can have zones designated for fairly broad processes that have smaller subsets of control within them where the process is broken down into multiple distributed subsets. This is typical of a distributed control system as defined earlier.

Level 0 Process

Level 0 consists of a wide variety of sensors and actuators involved in the basic industrial process. These devices perform the basic functions of the IACS as part of the physical process, such as driving a motor, measuring variables such as temperature and pressure, and setting an output.

Level 1 Basic Control

Level 1 consists of controllers that direct and manipulate the local process, primarily interfacing with the Level 0 devices (for example, I/O, sensors and actuators).

IACS controllers are the intelligence of the industrial control system, making decisions based on feedback from the devices found at Level 0. Controllers act alone or in conjunction with other controllers to manage the devices and the industrial process.

Level 2 Supervisory Control

Level 2 represents the applications and functions associated with the Cell/Area Zone runtime supervision and operation, including DCS, HMI, and supervisory and data acquisition (SCADA) software. Depending on the size of the plant, some of these functions may reside at the site level (Level 3). An example could be control room workstations monitoring processes site wide.

Industrial Zone

The industrial zone comprises the Cell/Area Zones (Levels 0 to 2) and site-level (Level 3) activities. The industrial zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone. To preserve smooth plant operations and functioning of the IACS applications and IACS network in alignment with standards such as IEC 62443, this zone requires clear logical segmentation and protection from Levels 4 and 5.

Level 3 Site Operations and Control

Level 3 is where the applications and systems reside that support plant-wide control and monitoring. A centralized control room with operator stations monitoring and controlling many systems within the plant is at this level. The Level 3 IACS network may communicate with Level 1 controllers and Level 0 devices, function as a staging area for changes into the industrial zone, and share data with the enterprise (Levels 4 and 5) systems and applications via the DMZ. Examples of services at this level are historians, control applications, network and IACS management software, and network security services. Control applications will vary greatly depending on the plant.

Enterprise Zone

Level 4 Site Business Planning and Logistics

Level 4 is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. Although important, these services are not considered critical to the IACS and the plant floor operations. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the IACS network. Examples of applications would include Internet access, email, non-critical plant systems such as Manufacturing Execution Systems (MES), and access to enterprise applications such as SAP.

Level 5 Enterprise

Level 5 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. The IACS must communicate with the enterprise applications to exchange manufacturing and resource data. Direct access to the IACS is typically neither required nor recommended from this level.

Industrial DMZ

Although not part of Purdue reference model, the oil and gas process control and refineries solution includes a DMZ between the industrial and enterprise zones. New industrial security standards such as ISA-99 (also known as IEC-62443), NIST 800-82, and Department of Homeland Security INL/EXT-06-11478 include an Industrial DMZ as part of a security strategy. The IDMZ provides a buffer zone between the enterprise zone and the industrial/plant zone.
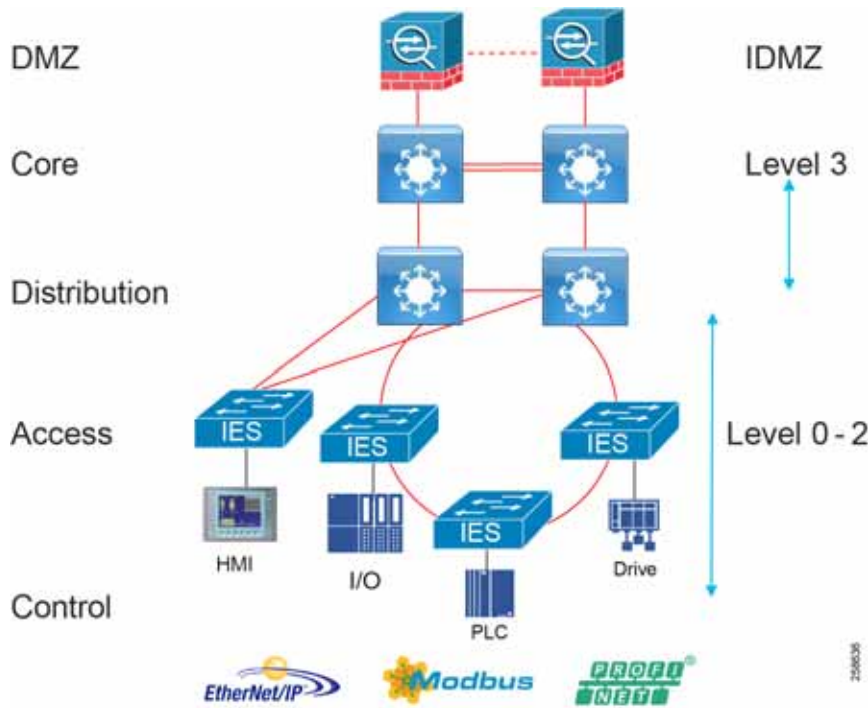
The Industrial DMZ is deployed within plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. Network access is not permitted directly between the enterprise and the plant, however, data and services are required to be shared between the zones, thus the industrial DMZ provides the architecture for the secure transport of data. This unofficial zone is crucial in securing and isolating the mission-critical operations network from the corporation own support services as well as from the outside world Typical services deployed in the DMZ include remote access servers and mirrored services.

Oil and Gas Process Control and Refineries Reference Design—Wired

The wired network design supporting process control, safety, and power networks is very much aligned with the Industrial Automation CVD. The reference wired design is built on the foundation described in this CVD, though there are some slight differences. This section provides a high-level view of the architecture and identifies differences from the Industrial Automation design.

The typical enterprise campus network design is ideal for providing resilient, highly scalable, and secure connectivity for all network assets. The campus model is a proven hierarchal design that consists of three main layers: core, distribution, and access. The DMZ layer is added to provide a security interface outside of the operational plant domain. Figure 6 highlights the alignment between the Purdue model and the enterprise campus model. Although detailed design and product guidance is out of scope for this document, the following sections outline the wired reference design for the oil and gas process control and refinery reference architecture.

Figure 6   Oil and Gas Process Control and Refineries Reference Design
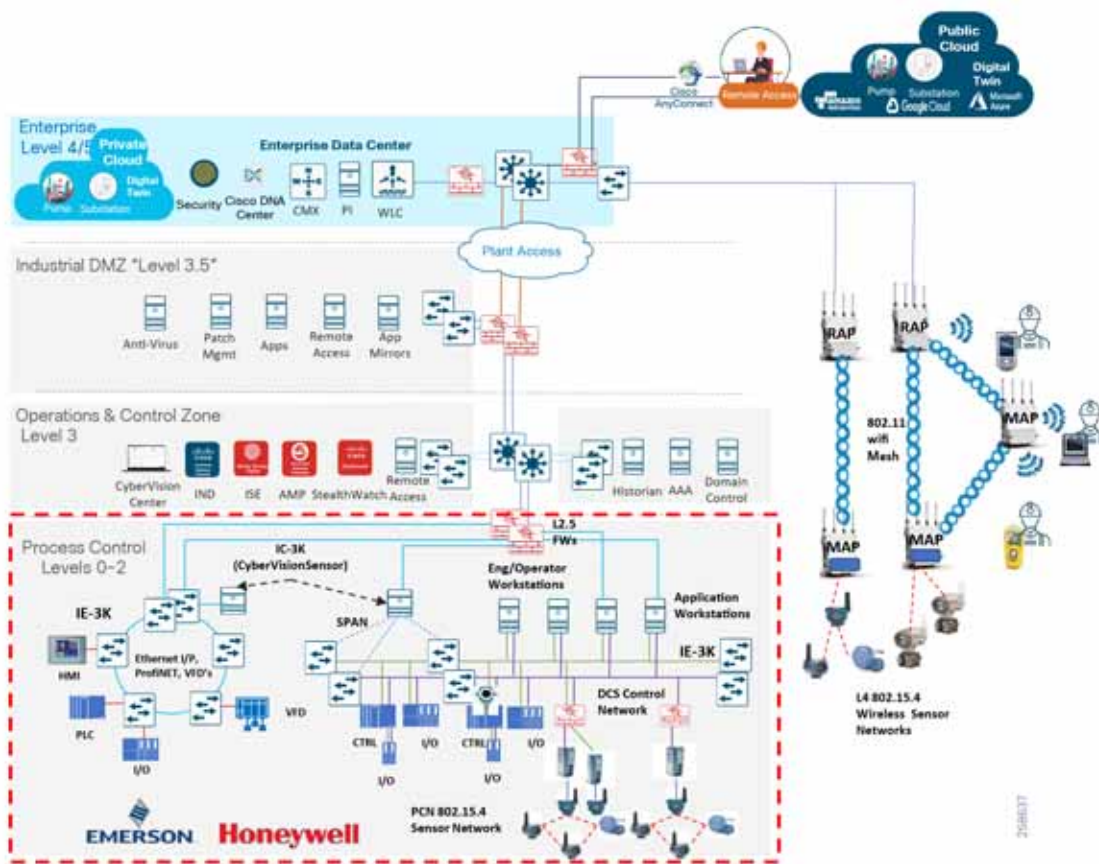
Process Control Levels 0-2

The process control network is where IACS devices and controllers are executing the real-time control of an industrial process. This network connects sensors, actuators, drives, controllers, and any other IACS devices that need to communicate in real-time I/O communication. It is essentially the major building block within the process control network architecture.

Within the process control levels 0-2, there are key requirements and industrial characteristics that the networking platforms must align with and support. This is very much aligned with the Cell/Area Zone design and recommendations in the Industrial automation CVD, in the section "Industrial Networking and Security Design for the Cell/Area Zone".

Environmental conditions such as temperature, humidity, and invasive materials require networking platforms with different physical attributes. In addition, continuous availability is critical to ensure the uptime of industrial processes to minimize impact to revenue. Finally, industrial networks also differ from IT in that they may need IACS protocol support to integrate with IACS systems.

Figure 7   Process Control Levels 0-2

Availability and Access Switching

Availability of the critical IACS communications is a key factor and consideration when designing process control networks. Network topologies and resiliency design choices, such as QoS and segmentation, are critical in helping maintain availability of IACS applications, reducing the impact of a failure or security breach.

Within process control networks there are a number of factors that define the layout of the access network. The physical layout of the plant, cost of cabling, and desired availability are three important factors in plants. There are some differences in networking access between industrial automation and the oil and gas process control network when looking at typical DCS deployments. Automation vendors have preferred deployment models to support a process control network or DCS. Emerson and Honeywell both support dual LAN architectures to provide availability of their DCS at levels 0-3. The following provides a quick overview of access topologies for process control networks.

Dual Lan

Within the classic dual LAN architecture in process environments the LANs are kept physically separate, essentially a LAN A and LAN B. The LANs do not converge at any point in the architecture from the controllers and I/O through to the workstations and application servers. Each end controller device will have two Network Interface Cards (NICs) or an A and B redundant pair of devices independently connected to each LAN. Redundancy and availability is provided through always having at least one LAN available.

Rings

The ring topology provides resiliency in that there is always a network path available even with a single link failure. Resilient Ethernet Protocol (REP) helps provide resiliency in rings. REP can offer a complete view of the state of the network ring, is deterministic and predictable during failures, is easy to configure, and can converge in under 200ms. Newer resiliency protocols for Ethernet rings such as High Availability Seamless Redundancy (HSR) are hitless and are supported on the industrial Ethernet line of switches. Rings can be used with the dual LAN if kept physically separate, again with no LAN A and LAN B convergence.

Star

In a redundant star architecture, there are only two hops in the path between devices and there is redundancy to provide fast convergence. The classic star topology has a switch connected to a redundant pair of switches upstream. The network has an element of predictability because of the consistent number of hops in the path. Star topologies may be less utilized in these environments if dual LANs are deployed, as in this topology it breaks the fundamental rule of the dual LAN where the LANS must not converge.

Resiliency protocols for the access layer are described in detail in the Industrial Automation CVD in the section "Industrial Networking and Security Design for the Cell/Area Zone". These include REP, HSR, Parallel Redundancy Protocol (rings or non-rings, dual LAN), and Media Redundancy Protocol (MRP-PROFINET deployments).

Note that a fair amount of wired instrumentation is connected over 4-20ma loops to marshaling I/O cabinets and into the controllers which are generally housed in controlled environments. The controllers are connected to Ethernet. For any harsher environments or where DIN rack mountable switches are mandated, the Cisco Industrial Ethernet (IE) series switches are recommended. Due to their ruggedized IP30-rated design. the Cisco IE switches are excellent access-layer switches for industrial applications.

Performance and QoS

Depending on the industrial application, a delay or variance and lack of determinism in the network can shut down an industrial process and impact its overall efficiency. Achieving predictable, reliable packet delivery is a fundamental requirement for a successful network design in process control networks. A design needs to factor the number of network hops, bandwidth requirements, and network QoS and prioritization to provide a greater degree of determinism and performance for process control network applications. The Industrial Automation CVD section on the Cell/Area Zone highlights QoS models, traffic types, and IACS application requirements in its design guidance and can be leveraged for process control networks.

Security

When implementing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. The Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95), and IEC 62443, NIST 800-82 are examples of such architectures. Key security requirements in the process control network are very much aligned with Industrial Automation. These include device and IACS asset visibility, secure access to the network, segmentation, group-based security policy, and Layer 2 hardening (control plane and data plane) to protect the infrastructure. Asset visibility, anomaly detection, and security policy and management are all provided with Cisco secure networking, Cyber Vision, ISE, and StealthWatch.

Management

Plant infrastructures are becoming more advanced and connected than ever before. Within the process control network there are two personas and skillsets taking on the responsibility of the network infrastructure, namely IT and OT staff. OT teams require an easy-to-use, lightweight, and intelligent platform that presents network information in the context of automation equipment. Key functions at this layer will include plug-and-play, easy switch replacement, and ease of use to maintain the network infrastructure. The Industrial Network Director supports this function. The management design and functions are aligned with Industrial Automation Cell/Area Zone design.

Recommended Cisco platforms for access and process control networks:

- Cisco IE 3200, Cisco IE 3300, Cisco IE 3400, Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000

- Carpeted access and with no industrial protocol support Cisco Catalyst 9300 and Cisco Catalyst 9200

- Security Cyber Vision, ISE, TrustSec, and StealthWatch

- Industrial Network Director providing OT network management support

Distribution Layer Switches

At the distribution layer in the architecture the process control and refinery architecture is very much aligned with the Industrial Automation CVD. The distribution layer facilitates connectivity between the access layer and other services. In smaller plants the distribution and core layer can converge onto the same platform. It may also provide site or plant wide connectivity. These switches are generally housed in controlled environments such as control rooms and so may be more aligned with traditional enterprise switching, unless certain industrial protocols are required such as in power networks, then industrial switches may be used at this layer.

Resiliency is provided by physically redundant components like redundant switches, power supplies, switch stacking, and redundant logical control planes HSRP, VRRP, and stateful switchover.

Distribution Layer Cisco Platforms

- Cisco Catalyst 9300 and Cisco Catalyst 9500

- Cisco IE 5000, Cisco IE 4000, Cisco IE 4010, and Cisco IE 3400

- Cisco Catalyst management through DNA-C

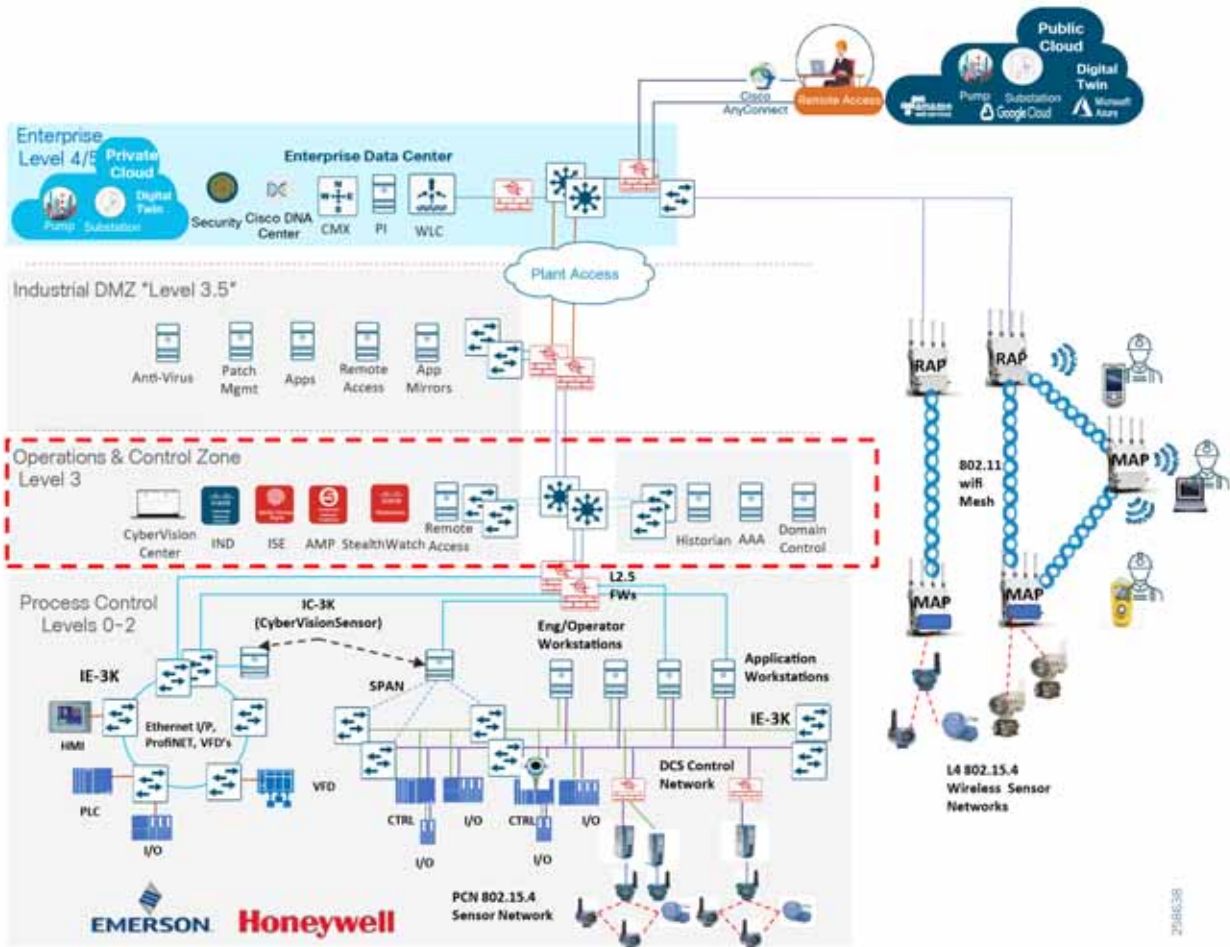- Security Cyber Vision, ISE, TrustSec, and StealthWatch

Level 2.5 Firewalls

Segmentation may be required between systems within level 0-2 and between level 0-2 and level 3. This firewall isolates the PCN from other level 0-2 networks across the plant such as power or other control systems not part of the DCS. It essentially provides access control for the DCS and is seen in some automation vendor reference architectures such as Emerson Delta-V.

Firewall Platforms

Cisco ISA 3000, Cisco ASA, and Cisco Firepower

Site Operations and Control Level 3

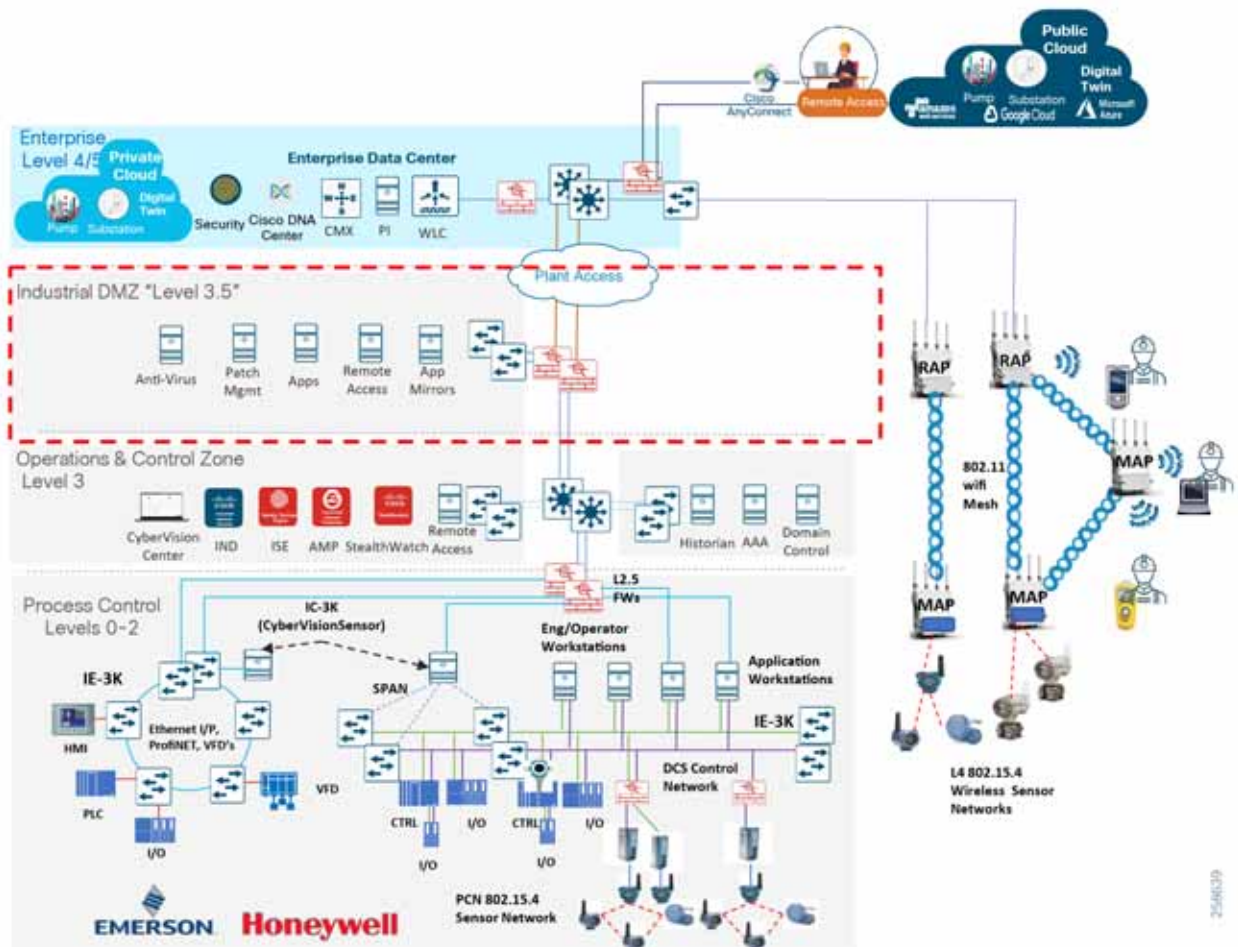**Figure 8   Site Operations and Control Level 3**

The majority of industrial plant facilities have a very different physical environment at this layer of the architecture compared to process control Level 2 and below. The networking characteristics are less intensive with respect to real time performance for the industrial protocols and equipment is physically situated in an environmentally controlled area, cabinet, or room. The core distribution networking platforms and data center are deployed at this layer. The data center houses the plantwide applications such as historians, asset management, plant floor visualization, monitoring, and reporting. Network management and plant security services are also housed here, including IND, Cyber Vision Center, ISE, and StealthWatch. This level provides the networking functions to route traffic between the process control area/zones and the applications within the site operations and control.

Core and Distribution Layer Cisco Platforms

- Cisco Catalyst 9300 and Cisco Catalyst 9500

- Cisco Catalyst management through DNA-C

- Security ISE, Cyber Vision, StealthWatch, and AMP for endpoints

- Cisco Hyperflex and Cisco UCS data center and compute platforms

Industrial DMZ Level 3.5

Figure 9   Industrial DMZ Level 3.5

The Industrial Zone (Levels 0-3) contains all IACS network and automation equipment that is critical to controlling and monitoring plant-wide operations. Industrial security standards including IEC-62443 recommend strict separation between the industrial zone (levels 0-3) and the enterprise/business domain and above (Levels 4-5). This segmentation and strict policy help to provide a secure industrial infrastructure and availability of the industrial processes. Though data, such as ERP data, is still required to be shared between the two entities, security networking services may be required to be managed and applied throughout the enterprise and industrial zones. A zone and infrastructure is required between the trusted industrial zone and the untrusted enterprise zone. The Industrial DMZ (IDMZ), commonly referred to as Level 3.5 provides a point of access and control for the access and exchange of data between these two entities.

The IDMZ architecture provides termination points for the enterprise and industrial domains and includes various servers, applications, and security policies to broker and police communications between the two domains. Key functions of the IDMZ include:

- Best practice is that no direct communications should occur between the enterprise and the industrial zone, although in some instances this may not be possible with enterprise systems being utilized in the industrial zone (ISE deployments).

- The IDMZ needs to provide secure communications between the enterprise and the industrial zone using mirrored or replicated servers and applications in the IDMZ.

- The IDMZ provides for remote access services from the external networks into the industrial zone.

- The IDMZ must provide a security barrier to prevent unauthorized communications into the industrial zone and therefore create security policies to explicitly allow authorized communications (ISE between enterprise and industrial zone).

- No IACS traffic will pass directly through the IDMZ (controller, I/O traffic).

The IDMZ design for process control is aligned with Industrial Automation. The design guidance is detailed in the Industrial DMZ reference section and detailed implementation can be found in the Converged Plantwide Ethernet CVD at: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

IDMZ Cisco Platforms

- Cisco ASA and Cisco Firepower Firewalls

- Cisco Catalyst 9200 and Cisco Catalyst 9300

- Cisco Hyperflex and Cisco UCS compute and data center platforms

Multiservice Traffic (Non-Operational Applications)—Wired

Multiple services can be deployed in plants to support plant operation communications. The services are not part of the operational systems and applications running within process control environment. These services typically include physical security badge access, video surveillance, and business-enabling applications such as email, telephony, and voice systems. Segmentation of the multi-service applications from the industrial application and process control environment is a common requirement. Regulatory demands, security concerns, risk management, and confidence of the business to maintain multi-service traffic on the same infrastructure as the IACS process and assets will drive the multi-service architecture. Generally, a separate physical infrastructure for the non-operational applications and services is acceptable. This is in essence an extended enterprise where the non-operational assets move into non-carpeted space. Hardened industrial switches are used in areas where more traditional enterprise switches cannot be deployed. Assets such as phones or video cameras may also require hardening as part of this architecture.
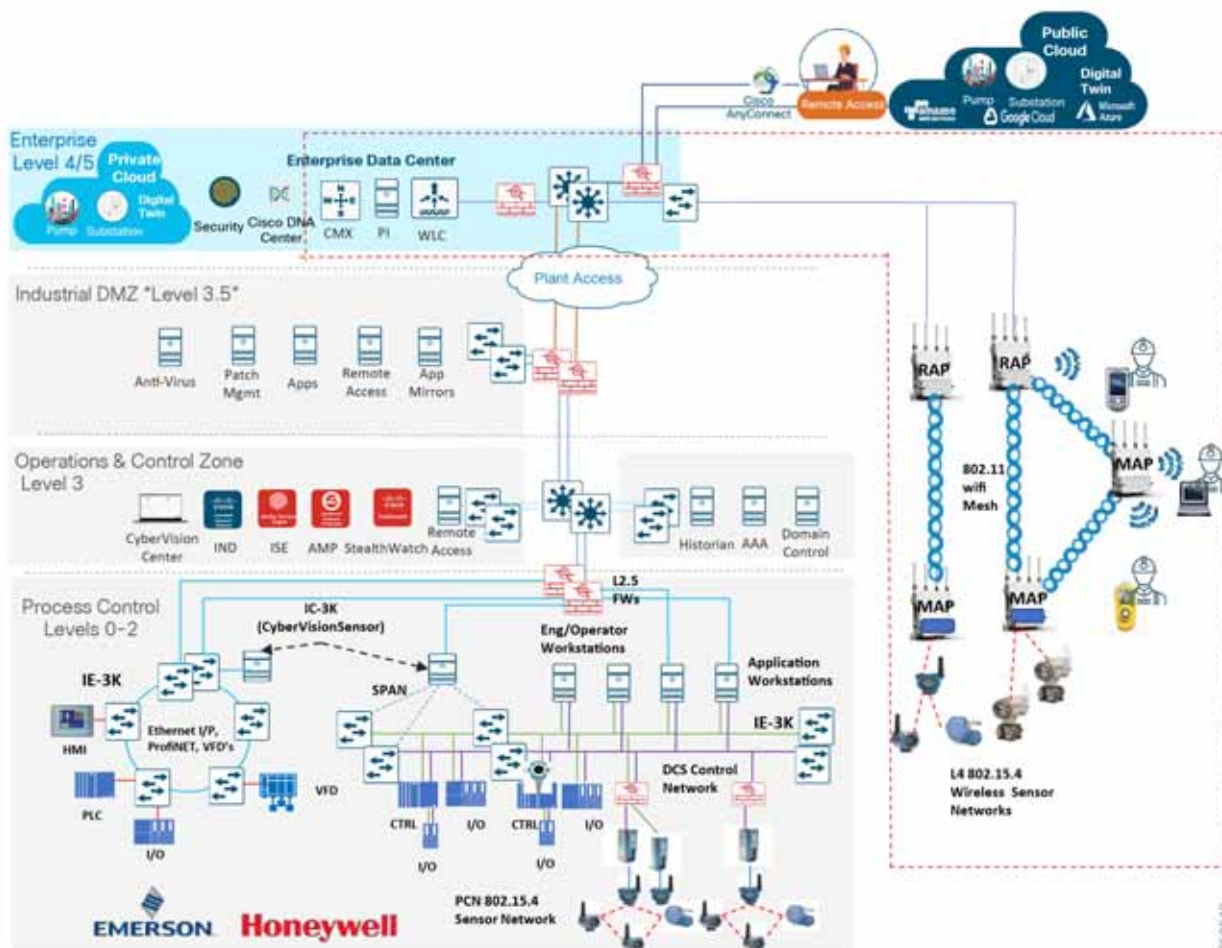
Oil and Gas Process Control and Refineries Design—Wireless

Industrial wireless and wireless instrumentation are the main focus for this version of the oil and gas process control and refinery guide. Detailed design guidance can be found in Industrial Wireless Design and Industrial Wireless Site Survey and Design Considerations. 802.11 Wireless networks in refineries support both plant/field operations and worker enablement. In supporting the plant field operations, 802.15.4 sensors and instrumentation data supporting equipment monitoring applications are backhauled over the 802.11 Wi-Fi mesh infrastructure. Mobility services are enabled to support the mobile worker with handheld devices providing near real time access to data with location services and also visibility into worker and asset location.

The wireless network provides:

- Mobile worker—A secure reliable Wi-Fi network built to enable the mobile worker within the process plant providing anywhere access to data improving the workers operational productivity and safety.

- Digital transformation—Improved productivity leveraging sensor data with built-in security enabling predictive maintenance and condition-monitoring applications.

- Worker safety—Visibility into worker location and enhance safety by enabling mobile safety devices such as mobile gas detection or hardened radio frequency identification (RFID) tags.

- Flexible implementation of advanced applications and reduced time to deployment of devices, avoiding expensive cabling with Cisco Mesh.

- Improved turnaround and location awareness to see into contractor productivity during STO events and improve worker safety.

- Remote expert—Provide access to centralized expert services to improve training and support to field engineers.

Solution Overview and Use Cases

Figure 10   Refinery and Process Control Wireless

The IW6300 is Cisco's new Class 1, Div 2/Zone 2 hazardous location-certified, designed specifically for hazardous environments like oil and gas refineries, chemical plants, and processing plants. It is an integral component to enabling 802.11 wireless and enabling the above use cases and outcomes in the process plant and refinery.

Figure 11   Cisco Catalyst IW6300 Heavy Duty Series Access Points

The reference architecture highlights the networks deployed outside of the Operations and Control Zone Level 3 and below. All supported services and data using Cisco wireless are not part of the critical process control. Equipment monitoring, predictive maintenance, mobile worker services, and location services are all non-process control applications. The other deployment model not evaluated in this version of the CVD is to place the wireless infrastructure at level 3.5 or as an isolated network rather than at Level 4. This wireless sensing data can be used as part of the process control. Both models have merits depending on the customer use cases and operating models - (IT/OT owned and supported). Further details are provided in the Wireless Instrumentation section.

The access points are set up to form a Cisco Mesh. The Cisco Mesh allows Mesh Access Points (MAPs) to wirelessly connect to the Root Access Points (RAPs) which are wired to the Cisco infrastructure. One of the advantages of using Cisco Mesh is the reduced cabling expense to provide wireless connection to areas of the plant that are not wired. The RAPs feed into the enterprise level 4/5 switch. This could be a Cisco Catalyst or a Cisco IE switch as part of the extended enterprise. Wireless LAN controllers provide system-wide operations and policies such as mobility, security, QoS, and RF frequency management. Cisco Prime Infrastructure provides a graphical platform for wireless mesh planning, configuration, and management. Network managers can use Cisco Prime Infrastructure to design, control, and monitor wireless mesh networks from a central location. Cisco wireless network promotes information and system security with next-generation encryption, interference and rogue access point-detection tools, intrusion detection, network management, client security with 802.1x, and Cisco ISE.

One of the major deliverables within the scope of this guide is to detail a path to migrate wireless networks from the existing 1552 hazardous location access point to the new IW6300 hazardous location access point. The design guide details 1552 and IW6300 mixed deployments for brownfield architectures and IW6300 only deployments with the new Cisco Catalyst 9800 WLC for greenfield deployments.

Figure 12   Wireless Migration

Cisco Wireless Platforms

- IW 6300 and 1552 Access points

- AireOS WLC and Cisco Catalyst 9800 IOS-XE WLC platforms

- Cisco Prime Infrastructure and Cisco CMX

Wireless Instrumentation

Refineries and processing facilities contain sensors, instrumentation, actuators, and other equipment associated with process monitoring and control systems. Historically, it has not been technically or economically feasible to connect all of these systems via a wired communications infrastructure and many of these devices therefore remain standalone. Deploying wired sensors would incur high costs and would not enable transient or intermittent monitoring. This means manual readings, non-real-time information, and a lack of integrated information on which systems can act.

The IEEE 802.15.4 wireless infrastructure connects instrumentation and sensors using industry standard ISA100.11a or Wireless Highway Addressable Remote Transducer Protocol (*Wireless*HART) protocols. The sensors are placed at the equipment or along pipes, transmit real-time process data over the 802.15.4 network to the sensor gateway, and then backhauled over the pervasive Cisco wireless 802.11 mesh. By deploying wireless technology for instrumentation, the process monitoring and control systems are able to gain real-time visibility and access to sensor-level information. This allows consistent condition-based monitoring from equipment at all times, delivering high performance, utilization, and reliability and reducing unplanned downtime.

There are two key partners supporting the wireless instrumentation infrastructure, Emerson and Honeywell Process Systems. The Cisco 1552 and IW6300 support the backhaul and integrate with both vendors wireless instrumentation solutions.

Emerson and Cisco work closely in a number of industries in oil and gas solutions, with an emphasis on integrated Industrial Wireless technologies and security for the refining and process control environments. An integral component of the Emerson Wireless plant solution is the wireless plant network. This leverages *pervasive sensing* for the instrumentation and sensor networks, and also for multi-service use cases to support operational activities.

In process control, Honeywell and Cisco work closely on converged Industrial Wireless solutions for processing facilities, refining, storage, and the oilfield. The joint work includes validated deployment architectures, proven use case solutions, product development, and an end-to-end communications strategy from instrument to application which securely brings together the Enterprise and the process control networks. Cisco wireless is a component of the Honeywell OneWireless Network architecture.

Historically both partners have developed joint products with Cisco and the 1552 wireless access points. This combines the Cisco Class 1 Div2 Intrinsically safe Access point with 802.15.4 Sensor gateways supporting Wireless Hart and ISA100.11A. This provides the connectivity of 802.15.4 networks and instruments, 802.11 wireless devices and 802.11
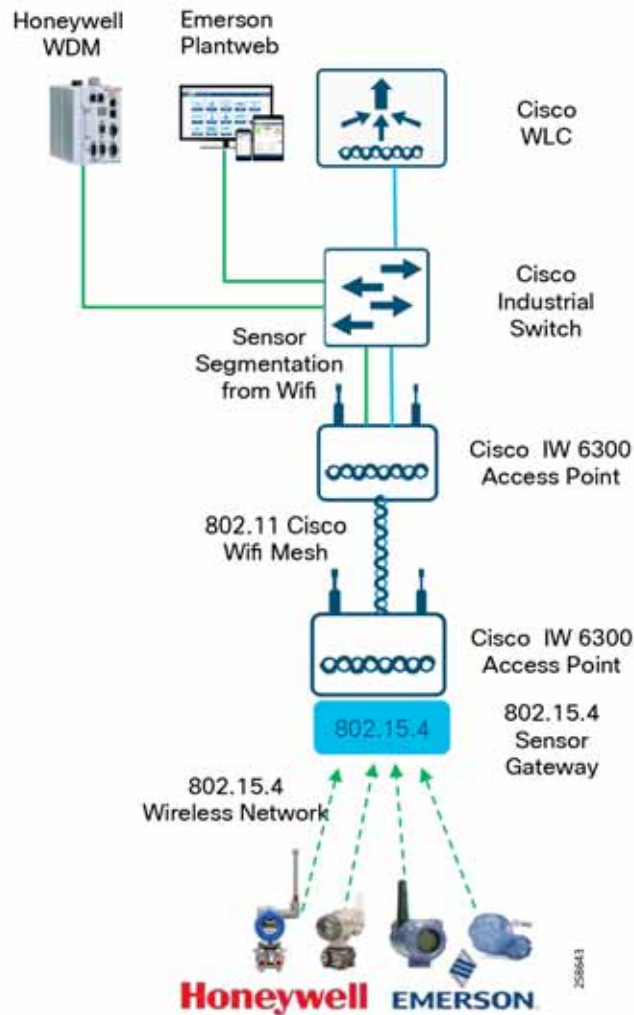
mesh backhaul all in a single device. The new IW6300 intrinsically safe Class 1/DIV 2 access point follows the same principles. Both Emerson and Honeywell have developed IoT modules which easily integrate into a single unit with the IW6300 access point.

As highlighted in the previous section, there are two modes for deploying wireless and wireless instrumentation in the refineries which have their respective merits. If deploying at Level-4, the Instrumentation gateways must carry non-process control sensing application data. There are additional guidelines that are recommended for example, the WiHART or instrumentation data cannot be accessible from the PCN, and cannot be used by an operator to make decisions in the DCS, i.e., you cannot write values in the DCS based on that data; you can output to an enterprise PI (in the DMZ for example), for data aggregation/collection, store the data in a historian DB. If instrumentation data is required from the DCS, then separate gateways need to be deployed and hardwired directly to the process control network as depicted in the reference architecture.

If sensing applications for process control are required to be backhauled over a Wi-Fi 802.11 Mesh and are essentially a component of the DCS then the WLC and infrastructure could be deployed and managed at the OT layer for example at L3.5 or below.

In the figure the Wireless instruments connect to the 802.15.4 Sensor gateway integrated with the IW6300. This is backhauled over the Wi-Fi mesh infrastructure and offloaded at the Root Access point over a switched infrastructure to either a Honeywell Wireless Device Manager or Emerson Plantweb instance.

Figure 13   Wireless Instrumentation

The Industrial Wireless Design describes design guidance for deployments of wireless instrumentation and the integration of 802.15.4 networks with the Cisco wireless infrastructure with a focus on Emerson for this initial release. Further releases will incorporate both Honeywell and Emerson architectures with design guidance.

Cisco Wireless Platforms

- IW 6300 and 1552 access points

- AireOS WLC and Cisco Catalyst 9800 IOS-XE WLC platforms

Partner Devices and Platforms

- 802.15.4 Sensor Gateway—Honeywell or Emerson IoT Module

- Honeywell or Emerson wireless instrumentation

- Emerson Plantweb

- Honeywell Wireless Device Manager (WDM)

- Sensor visualization platform

Oil and Gas Process Control and Refineries Reference Design – Industrial Security

When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. The Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95) and IEC 6244 and NIST 800-82 are examples of such guidelines. Key security requirements in the refinery networks include device and IACS asset visibility, secure access to the network, segmentation, group-based security policy, threat detection and mitigation to protect the infrastructure. As domains between Operational Technology (OT) and Information Technology (IT) converge, they must also align security strategies and work more closely together to ensure a truly end-to-end security architecture.

A Basic Security Strategy to securing any environment not just Industrial environments starts with Visibility and Baseline, Segment, Detect and then respond. This section and the highlights the security reference architecture for process control and refineries with an OT focus to securing the operational environment. This reference is built from the Industrial Automation for Network and Security CVD 2.0. This Industrial Automation for Network and Security CVD 2.0 contains deeper detail into the design and implementation supporting security in the OT process domain.

Visibility

Companies cannot secure the infrastructure without having a thorough understanding of the assets connected. Securing the OT infrastructure starts with having a precise view of the asset inventory, communication patterns, and network topologies. Plant security implementations require full visibility of their assets and application flows so they can implement security best practices, drive network segmentation, implement security policy with enforcement, and provide threat control, awareness and mitigation. Visibility is the first step in security, and the lack of visibility to assets and communication patterns in industrial control systems makes it a challenge to secure these environments. A security implementation generally starts with visibility such as implementing a security assessment. Cisco Cyber Vision, Cisco Industrial Network Director (IND) and StealthWatch can be used to provide visibility into the oil and gas and process plant connected assets.

Cisco Cyber Vision

Cisco Cyber Vision is a cybersecurity solution specifically designed for industrial organizations including oil and gas, manufacturing, power utilities and water distribution to ensure continuity, resilience, and safety of their industrial operations. It provides asset owners with full visibility into their IACS networks so they can ensure operational and process integrity, drive regulatory compliance, and enforce security policies through seamless integration with the IT Security Operations Center (SOC) and easy deployment within the industrial network. Cisco Cyber Vision leverages Cisco industrial network equipment to monitor industrial operations and feeds Cisco IT security platforms with OT context to build a unified IT/OT cybersecurity architecture. Cisco Cyber Vision provides three key value propositions:

- Visibility embedded in the Industrial Network-Know what to protect. Cisco Cyber Vision is embedded in the Cisco industrial network equipment so everything that connects to it can be seen, enabling customers to segment their network and deploy IoT security at scale.

- Security insights for IACS and OT-Continuously monitor IACS cybersecurity integrity to help maintain system integrity and production continuity. Cisco Cyber Vision understands proprietary industrial protocols and keeps track of process data, asset modifications, and variable changes.

- 360° threat detection-Detect threats before it is too late. Cisco Cyber Vision leverages Cisco threat intelligence and advanced behavioral analytics to identify known and emerging threats as well as process anomalies and unknown attacks. Fully integrated with Cisco security portfolio, it extends the IT SOC to the OT domain.

Cisco Cyber Vision has two primary components: Center and Sensor. The Sensor uses deep packet inspection (DPI) to filter the packets and extract metadata, which is sent to the Center for further analytics. Deep packet inspection is a sophisticated process of inspecting packets up to the application layer to discover any abnormal behavior occurring in the network. Primarily the sensors are deployed on industrial networks and protocols, Level 0-2 in the Purdue model.

Cisco Industrial Network Director (IND)

Cisco IND is a network management product for OT team that provides an easily-integrated system delivering increased operator and technician productivity through streamlined network monitoring and rapid troubleshooting. Cisco IND is part of a comprehensive IoT solution from Cisco and provides:

■ Easy-to-adopt network management system built specifically for industrial applications that leverages the full capabilities of the Cisco IE switches to make the network accessible to non-IT operations personnel

■ Creates a dynamic, integrated topology of automation and networking assets using discovery via industrial protocols (CIP, PROFINET) to provide a common framework for OT and IT personnel to monitor and troubleshoot the network and quickly recover from unplanned downtime. The device discovery also provides context details of the connected industrial devices (such as PLCs, I/O, Drives, HMI and so on).

■ Rich APIs allow for easy integration of network information into existing industrial asset management systems and allow customers and system integrators to build dashboards customized to meet specific monitoring and accounting needs.

Although IND is targeted as a network management tool for OT personnel, the asset visibility function is utilized in the Industrial Automation security architecture.

StealthWatch and NetFlow

Cisco StealthWatch provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, StealthWatch can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, distributed-denial-of-service (DDoS) attacks, illicit crypto-mining, unknown malware, and insider threats. Cisco StealthWatch collects and analyzes massive amounts of data to help security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network, so they can quickly and effectively respond to threats.

StealthWatch leverages NetFlow, IPFIX, and other types of flow data from existing infrastructure such as routers, switches, firewalls, proxy servers, endpoints, and other network infrastructure devices. The data is collected and analyzed to provide a complete picture of network activity. Focused on Enterprise IT networks. This would correspond to level 3 to 5 in the Purdue model. In the industrial domain Level 3 tends to have more COTS type applications and windows servers serving plantwide, therefore StealthWatch provides threat awareness and visibility and is impactful at this layer.

Segmentation, policy management and enforcement

Segmentation is a key component to creating zones of trust to help protect IACS networks and processes. IEC 62443 details restricted data flow recommendations to segment the control system into zones and conduits to limit the unnecessary flow of data between process networks or services. Network segmentation is one of the most effective controls implemented to mitigate propagation or lateral movement of an attack, Intentional or accidental between untrusted entities. With the visibility provided through Cisco CyberVision, IND and StealthWatch, segmentation can be implemented into the networks using basic methods such as vlan segmentation, firewalling and Cisco TrustSec with Cisco ISE administering the policies.

Firewalls

From a high-level segmentation perspective, the architecture leads with an IDMZ to provide segmentation and controlled access between the Industrial Level 3 and the business/enterprise levels 4 and 5. Further segmentation deeper into the Industrial Level 3 and below may be used such as with the Level 2.5 firewall in the architecture. This level 2.5 firewall is common in the DCS and process control networks to provide a further level of segmentation for controlled access and domain separation from the other site-wide plant systems.

Vlan Segmentation and ACLs

VLAN segmentation and ACLs have been the traditional way to provide restricted dataflow within IACS networks. While manageable for smaller plants, maintaining access policies can be cumbersome and difficult for larger plants. As more devices are added to a network, ACLs start to become large at policy enforcement points and are implemented at various places in the network, making it a distributed application of policy across an industrial plant. Continually updating ACLs poses a higher risk of misconfiguration and is generally not scalable.

TrustSec and Scalable Group Tags

Cisco TrustSec-enabled industrial switches provide scalable segmentation across the industrial automation architecture. Cisco TrustSec technology assigns SGTs to IACS assets, networking devices, and users when they attach to a network. By using these tags, an IT security architect can define an access policy and enforce that policy across the network.

Cisco ISE

Cisco ISE is a security administration product that enables an OT-IT security administrative team to create and enforce access level security policies. Cisco Cyber Vision or Cisco IND interfaces with Cisco ISE using Cisco pxGrid, which is an open, scalable, and IETF standards-driven data sharing and threat control platform to communicate device information through attributes to ISE. ISE can then utilize this information and apply the appropriate security policy.

The integration between the Cisco Cyber Vision/Cisco IND and ISE provides the following benefits

- Automatically enrolls IACS assets into the ISE endpoint database.

- Enables an OT-IT security administrative team to create granular profiling policies based on the attributes received from Cisco Cyber Vision or IND.

- Allows the OT engineers to leverage the integration between Cisco Cyber Vision/Cisco IND and ISE to automatically deploy new security policies in the network.
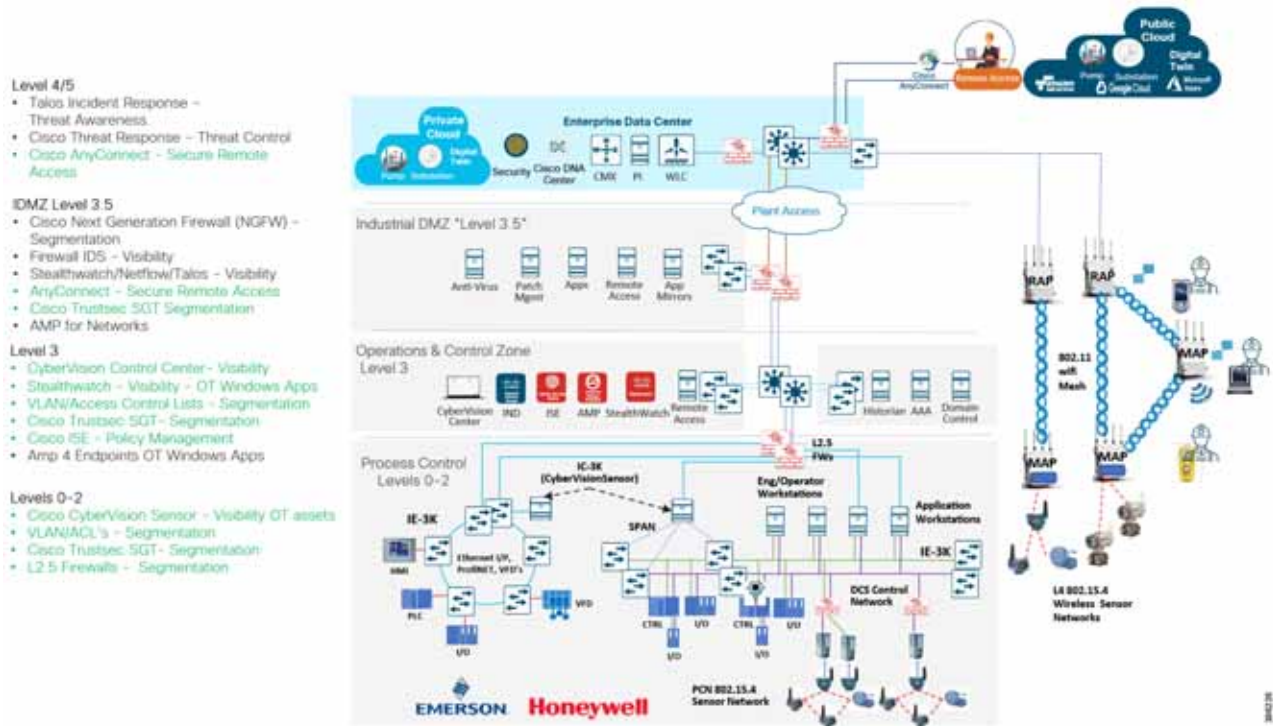
Threat awareness

As industrial networks are ever more connected to IT networks, they must be protected from the usual IT threats such as malware or intrusion. As attacks on industrial networks may look like legitimate instructions to assets, unwanted process modifications must also be detected. To secure an industrial network, a variety of threat detection mechanisms is required. Cisco Cyber Vision combines protocol analysis, intrusion detection, and behavioral analysis to detect any attack tactic. StealthWatch can detect threats such as command-and-control (C&C) attacks, ransomware, distributed-denial-of-service (DDoS) attacks, unknown malware and highlight traffic flows outside of the baseline.

Summary

The following figure highlights the Industrial Security reference architecture. Green items have been validated within the Industrial Automation CVD and those not highlighted are capabilities that can be applied in a true integrated IT/OT end to end architecture.

Figure 14   Industrial Security Reference Architecture

Low-Level Use Cases

Today's oil and gas industry is increasingly looking for new ways to enhance operations, reduce downtime, and improve worker safety and security. According to Deloitte, digitalization through IoT promises to help petroleum organizations directly meet these challenges as part of their key focus to:

- Improve reliability and manage risk—Minimizing the risks to health, safety, and the environment by reducing disruptions.

- Optimize operations—Increasing productivity and optimizing the supply chain through the cost and capital efficiency of business operations.

- Create new value—Exploring new sources of revenue and competitive advantage that drive business transformation.

The following use cases work across the three pillars described in Process Plant and Refinery Overview to help achieve digitalization that enhances business benefit through improved operational efficiency, productivity, and increased safety and security. The Cisco oil and gas process control and refinery solution provides a converged, standards-based architecture for supporting these use cases.

Plant and Field Operations

Enable digital operations by connecting machines, sensors, and other OT systems with secure and standards-based industrial wired and wireless networks.

ICS/DCS/SCADA Connectivity

The Distributed Control System and associated supporting industrial systems and production assets are core to the process plant and refinery. Millions of dollars can be lost due to a single outage within the network, so ensuring uptime and availability are key. Wired networking primarily supports the industrial control systems and producing assets within the process plant and refinery. A robust, secure, highly available network lays the foundation for continuous operations across the plants. The Industrial Automation CVD lays the foundation for supporting ICS/DCS/SCADA connectivity.

Predictive Maintenance

Predictive or proactive analytics can be leveraged in the facility to better manage asset maintenance on plant equipment, including heat exchangers, compressors, turbines, flare stacks, cokers, motors, pumps, and drives. Typically, equipment is assessed on a preventative time-based schedule or is reactive to issues. Equipment or parts may be replaced even if they do not need to be based on estimated lifetime use. Manual inspection can be expensive and as data is captured at a point in time, the lack of real-time information can lead to equipment failure, costly unplanned maintenance, non-productive time, and accidents or emergencies resulting from failing equipment.

Analytics can be leveraged to make equipment monitoring, management, and maintenance more effective. Models created for each equipment type help predict component failure and optimal performance characteristics. Wireless sensors monitoring equipment in the plant can provide temperature, vibration, and acoustic data that when compared with statistical models can access equipment performance and likelihood of failure. The wireless instrumentation architecture passes this data to high layer applications and AI/ML to create real outcomes. The plant is covered by a Cisco pervasive industrial wireless MESH infrastructure. The partner sensors from Honeywell and Emerson push the data over the 802.15.4 networks and then backhaul it over the Cisco Wi-Fi mesh.

Valve Alignment

Valve misalignments in tank fields and blending areas cause incorrect product mixes, resulting in financial losses from poor product quality, and pose environmental safety issues. Incidents of valve misalignment in a single plant cause millions of dollars in documented financial losses in a single year through poor product quality. These losses are due to tanks or deliveries being contaminated and operational issues affecting the performance of multiple process assets. The valve alignment status and monitoring in a plant is has been manual and verbally communicated.

Providing visibility into the valve status and ensuring the valves are correctly aligned for the passing of product has huge cost benefits. Wireless sensors are deployed on non-monitored valves throughout the plant, with the plant covered by a pervasive industrial wireless MESH infrastructure. The 802.15.4 wireless sensors transmit near real-time valve status process data to a 802.15.4 sensor gateway, which is backhauled across the wireless infrastructure. The data can then be passed to an application providing visibility into full product flow path status and indicators that operators can use to confirm it is safe to start the transfer or blending process.

Steam Trap Monitoring

Refineries and process plants use vast quantities of steam across their processes. Steam traps are deployed to recapture condensate and are invaluable. Condensate in the steam systems can impact equipment performance and processes resulting in safety concerns for workers and equipment and increased maintenance costs. Time-consuming manual audits are common practice, and are inadequate in that they only provide a snapshot of the operation and therefore are not a reliable indicator of trap condition. The time between these manual audits leaves the plant vulnerable to failed steam traps. Wired costs to monitor these systems is too costly. Enabling wireless acoustic sensors across the plant to monitor steam traps provides continuous monitoring into key assets. This is another wireless instrumentation use case where the 802.15.4 wireless sensors transmit near real-time process data to a 802.15.4 sensor gateway, which is then backhauled across the Cisco wireless infrastructure.

Workforce Enablement

Enabling a safe and efficient workforce using mobile technology to improve access to data from anywhere, improve interactions between field workers, remote colleagues, and experts is beneficial. Using data from mobile sensors provides continuous insight into location and plant environmental conditions.

Mobile Worker

Operations have requirements around personnel safety and operational efficiency. Typically, field personnel perform work using information from unconnected ruggedized laptops in the field or from paper documents containing useful data including asset information, maps and schematics, work orders, and manuals. Information is not always current in the field and centralized information is not updated until workers complete a task and provide updates. This lack of automated information exchange between field workers and centralized functions can lead to operating inefficiencies and outdated asset information.

Providing tools such as hazardous-certified or intrinsically safe mobile devices connected over the Cisco 802.11 wireless network enables workers to use current data to perform their work more efficiently regardless of location. Workers can perform operational tasks in the field, view and complete work orders remotely, access remote experts, and get data directly in the field improving overall worker productivity.

Shutdown Turnaround Outage Optimization

Shutdown Turnaround Outage (STO) events are scheduled periods during which a plant will stop production for inspections, maintenance, upgrades, and cleaning that would not be achievable during normal operation. STO is expensive for the company. During STO events a significant increase in workers and contractors are in the plant working to bring the plant operational as quickly and safely as possible. If the STO overruns, then this can cause significant negative financial impact. Ultimately millions of dollars can be saved in ensuring STO events do not overrun or complete ahead of time. Cost savings can be realized for STO optimization with a Cisco wireless implementation.

Cisco wireless infrastructure and wireless ruggedized phones, tablets, and laptops with engineering tools and applications for job tasks and job completion speed up completion and improve workflow, activity records, safety, and compliance. Visibility and business insights into contractor worker productivity can be realized also by tracking contractors to ultimately reconciling billed hours to work done.

Remote Expert

With a younger workforce and fewer workers who are experienced in older systems and infrastructure, it is not often possible to make the right resources available in the right place and at the right time.

Leveraging collaboration technologies over wireless to connect onsite plant workers with remote experts across an optimized Cisco wireless infrastructure provides expertise on demand. Skilled, experienced operators and staff can instantly help support tasks, training, and emergencies regardless of their location and be instantly connected to the control room or onsite worker.

PPE and Mobile Gas Detection

Previously, refineries had fixed wired gas sensors to provide limited visibility into gas leaks in the refinery. Before work could commence, a manual gas detection survey had to be completed in the location where the work would happen. Installing wired gas sensors in the plant to provide pervasive coverage is expensive due to high installation costs. Now engineers are equipped with mobile 4-way gas detectors, supplemented by fixed wireless gas detectors in key locations. The plant is covered by a pervasive industrial wireless MESH to provide plantwide connectivity for the sensors. Real-time gas monitoring measurements are sent from the mobile and fixed gas detectors across the wireless infrastructure, providing gas measurements and the location of the sensor and engineer in the plant. This enables improved productivity by decreasing the time taken to start work by eliminating gas testing activities, optimizing evacuation route planning, and improving safety. With near real time location especially during STO events, critical staff safety and compliance goals can be met.

Industrial Security

Cyber Security

Cyber-attacks are a huge threat to oil and gas companies given the huge attack surface across all of their connected assets. Risks from Cyber security for process plants and refineries include physical damage, facility downtime, and breaches of customer data and intellectual property. Cisco industrial security is aligned with key standards such as IEC62443 and NIST 800 and provides:

- Visibility into the operational domain to help baseline the environment and understand what is connected in order to apply policy.

- Define policy and provide segmentation and micro segmentation techniques to restrict data flows between critical, non-critical operational, and non-operational assets.

- Detect anomalous behavior based on threat awareness or that deviate from baselines and defined policy.

- Provide secure controlled remote access into the OT environment.

- Enable and inform Incident response on security incidents or anomalous behavior.

Risks can be reduced across the operational environment, ensuring uptime with improved security, availability, and safety.

Video Surveillance and Access Control

Video surveillance, IP cameras, electronic physical access control, incident response and notifications, and personnel safety provide end-to-end support for safety and security detection, monitoring and management, and threat response in the plants.

These enable:

- Video surveillance to monitor the perimeter, fences, gates, restricted areas, and emergency incidents that may occur.

- Video surveillance to increase situational awareness by automatically tagging video when an employee or contractor swipes an access card to gain entry.

- Increased identification checks of all persons entering facilities.

- Initiated detailed, visible checks of all vehicles and packages entering facilities.

- Verification of safety or emergency incidents such as a leak or man down and real-time video feeds to safety staff and first responders.

Cisco wired and wireless infrastructure can be used to connect cameras and access control gateways to the control room. PoE-enabled networking switches and access point can be used to power the cameras directly.

Industrial Wireless Design

Wireless Ethernet is fast becoming the preferred communication delivery system due to its excellent reliability, adaptability and affordability. Industrial architectures are increasingly using IEEE 802.11 wireless networks for critical Industrial Automation and Control System (IACS) applications and multi-service applications that require reliable data transmission with low levels of latency and jitter, asset and location tracking, condition and performance monitoring, video-surveillance, worker safety and worker mobility. Wireless networking provides the most cost efficient and effective means of monitoring the expansive operations within a refinery. By using wireless communications to interface well sites, operations centers and distribution centers along long distances helps save hundreds of man hours and millions of dollars over the life of the system because of avoiding high-cost of cable installation and maintenance. Also for certain scenarios within a refinery there might be some physical constraints of not being able to run physical cables in order to provide network connectivity. This is where a wireless solution comes in handy.

Through the elimination of cables, wireless technology greatly reduces the CAPEX associated with instrumentation. Mobile instruments and hand-held devices (video-cameras, PDAs, laptops) allow devices to be positioned both temporally and spatially, as required.

With the industrial internet of things (IIoT), businesses are able to improve productivity, effectiveness, and success via wireless sensor networks. These networks have become vital for oil & gas industry and also manufacturing. The power to improve productivity, control as well as monitor the process with automation and extensive information interaction comes from the evolution of IIoT. Smart industrial wireless technologies can have a significant effect on the oil and gas sector operations with wireless field networks for sensors, area gadget applications, and wireless plant networks.

Wireless sensing networks may consist of numerous different types of sensors, covering a large variety of applications measuring temperature, pressure, humidity levels, circulation, flow, tank levels, or simply relaying a contact closure with a discrete transmitter. Wireless sensor network applications generally cover monitoring of near real-time procedure control, safety and security, governance, and manufacturing efficiency.

Operating on increasingly thin margins and focused on maximizing output from existing resources, oil and gas companies are adopting wireless sensor instruments that provide up to 80% infrastructure savings compared with wired options. As oil prices continue to fall and exploration activity increases, wireless sensor network adoption is steadily growing for core applications such as wellhead automation and pipeline compressor/pump station monitoring as well as growing innovations for asset management, worker safety and environmental monitoring.

Wireless Local Area Networks (WLANs) differ significantly from traditional wired LANs in their use of shared radio frequencies, susceptibility to interference and coverage impairments. Deploying a plant-wide WLAN requires thoughtful planning and design as well as periodic monitoring to meet expectations for bandwidth, throughput, reliability and security.
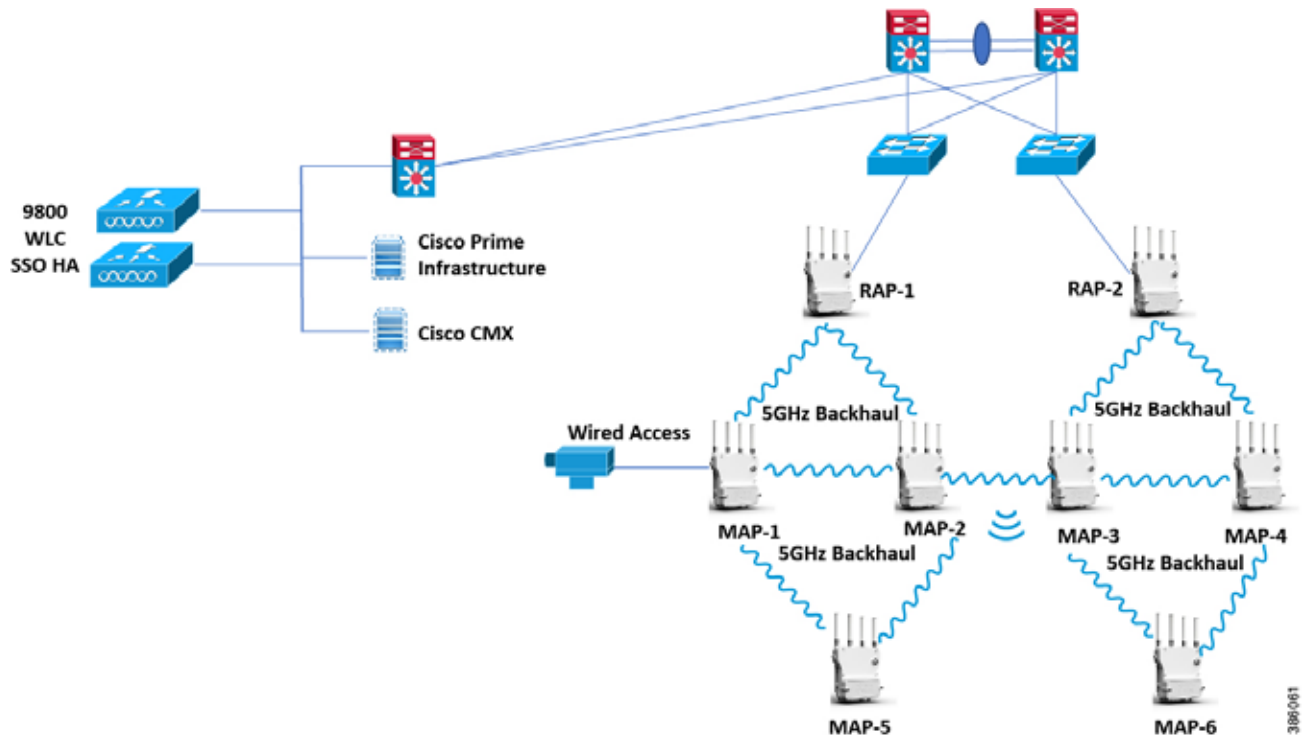
This chapter describes the Industrial Wireless Architecture and Design both for greenfield and brownfield deployments. This helps enable the target use cases around worker enablement, condition-based monitoring using Emerson WiHART gateways and sensors, Video Surveillance, Ethernet Bridging and Asset Tracking using active RFID tags. Design considerations around deployment of outdoor wireless mesh networks for greenfield scenarios, mixed mesh deployments for brownfield scenarios, high-availability, security and QoS are addressed. End-to-end integration with Emerson Rosemount WiHART gateways and sensors is also covered.

The greenfield deployment scenario covers architecture and design considerations around building a wireless mesh network consisting of Cisco's next-generation Catalyst 9800 WLCs and the newly announced IW6300 heavy-duty APs.

For the brownfield deployment scenario, architecture and design considerations around expanding wireless coverage to a newer area of the refinery is explained. Integration and seamless mobility between the existing deployment of Cisco AireOS WLCs and 1552 APs and the new deployment consisting of Cisco's next generation Catalyst 9800 WLCs and the newly release IW6300 Heavy-Duty outdoor wireless APs to form a mixed mesh deployment is described. Considerations surrounding the replacement of an existing 1552AP with the newer IW6300 AP are also discussed.

Overview of Industrial Wireless Architecture

Figure 15   Cisco Outdoor Industrial Wireless Architecture

The figure above depicts the reference architecture and components of Cisco's Outdoor Industrial Wireless deployment. The recommended topology to support the use-cases described above is to deploy a wireless mesh network registered to a redundant pair of Wireless LAN Controllers to provide high-availability. Cisco Prime Infrastructure is used for wired and wireless management. Cisco CMX is used to enable location services and asset tracking. Cisco ISE is used as a user/device identity store, queried for IEEE 802.1X authentication and acts as the overall network policy server.

Redundant Root Access Points (RAPs) are deployed to provide redundancy. Multiple Mesh Access Points (MAPs) are distributed throughout the plant floor wherever wireless coverage is deemed necessary. The 2.4GHz radio band is configured to provide wireless client access. The 5GHz radio band is configured to exclusively carry the wireless mesh backhaul traffic. Keeping in mind application performance and throughput requirements it's recommended not to deploy the mesh network more than 2-levels deep.

Wired Ethernet bridged traffic can be carried over the mesh backhaul if needed. For this, the device needs to be plugged into the Ethernet port of either the RAP or MAP access point. This is applicable to scenarios like video-surveillance and wireless (WiHART or ISA.100) sensors used for condition and performance monitoring. IP cameras used for video surveillance within the plant are plugged into the PoE out port of the AP. The video traffic is Ethernet bridged and transported over the mesh backhaul to its intended destination (video surveillance system within the control room). For condition-based monitoring the Wireless HART or ISA.100 gateway can be plugged into the PoE out port of the AP. The WiHART or ISA.100 sensors communicate with their respective gateways using their own wireless transport. The sensor traffic is Ethernet bridged and transported over the mesh backhaul to its intended destination. Any QoS markings applied by the wireless instrumentation gateway are preserved all the way over the mesh backhaul.

WiFi clients communicate with the access-points over the 2.4GHz radio band and are authenticated using the IEEE 802.1X protocol. Active RFID tags can be used for asset location tracking for stationary and mobile devices. The exact location of these tags are visible within the Cisco CMX UI.

Note: Location services accuracy and scalability were not tested as part of this validation effort. For this kind of outdoor wireless mesh network its highly recommended to perform a site-survey and also work with either Cisco CX or an accredited Cisco partner to tune the deployment to support location services.

Dynamic Frequency Selection

Previously, devices employing radar operated in frequency sub-bands without other competing services. However, controlling regulatory bodies are attempting to open and share these bands with new services like wireless mesh LANs (IEEE 802.11).

To protect existing radar services, the regulatory bodies require that devices wishing to share the newly opened frequency sub-band behave in accordance with the Dynamic Frequency Selection (DFS) protocol. DFS dictates that to be compliant, a radio device must be capable of detecting the presence of radar signals. When a radio detects a radar signal, it is required to stop transmitting to for at least 30 minutes to protect that service. The radio then selects a different channel to transmit on but only after monitoring it. If no radar is detected on the projected channel for at least one minute, then the new radio service device may begin transmissions on that channel.

The AP performs a DFS scan on the new DFS channel for 60 seconds. However, if a neighboring AP is already using that new DFS channel, the AP does not perform the DFS scan.

The process for a radio to detect and identify a radar signal is a complicated task that sometimes leads to incorrect detects. Incorrect radar detections can occur due to a large number of factors, including due to uncertainties of the RF environment and the ability of the access point to reliably detect actual on-channel radar.

Using 2.4GHz as the Mesh backhaul to avoid DFS interruptions in 5GHz band

For certain scenarios where-in the refinery is located next to a port, ships roll into the port with their radar enabled. This will trigger a DFS event if the APs are using a DFS channel within the 5GHz band.

In most regulatory domains, 802.11 stations are required to use Dynamic Frequency Selection (DFS) when using some or all of the channels in the 5GHz band. 802.11 stations, before transmitting in a DFS channel, must validate (by first listening for 60 seconds) that there is no radar activity on it. And, if an 802.11 radio should detect radar while using the DFS channel, it must vacate that channel quickly. Thus, if a radio should detect radar in its serving channel, then switch to another DFS channel, this will impose (at least) a one-minute outage.

This outage might not be acceptable to certain applications such as condition and performance based monitoring, video-surveillance traffic etc. If this is the case, then we suggest using the 2.4GHz band for mesh backhaul and the 5GHz band for WiFi client access. When adopting this model, the mesh backhaul can be up and running even under DFS scenarios and be able to transport condition-based monitoring (WiHART or ISA.100) and video surveillance traffic which is Ethernet bridged over the mesh backhaul. There will still be some interruption to the client access which uses 5GHz band due to DFS interruptions.

The pros and cons for using 2.4GHz for the mesh backhaul are shown below.

Pros:

- Mesh backhaul stays up and running even when radar signal detected

- 2.4GHz signal travels further than 5GHz signal, so we can provide similar coverage with less number of APs deployed

Cons:

- 2.4GHz provides less bandwidth as compared to 5GHz. This is a significant especially within a mesh deployment. One of the ways we can avoid degraded performance over the mesh backhaul might be to just deploy a 1-hop deep mesh network where-in a MAP node is just a leaf node and has no children nodes under it.

Cisco Industrial Wireless Network Components

This section highlights the individual component products that make up the Industrial Wireless network.

The table below highlights the Cisco component products needed to deploy the Outdoor Industrial Wireless Mesh network. Also listed are the individual software image versions that were validated within our labs.

Table 2   Industrial Wireless Mesh Components – Greenfield Deployment

Cisco Products	Version	Role
Cisco Catalyst 9800 Wireless Controller	IOS-XE 17.1.1s	Wireless LAN Controller for Greenfield and Brownfield Expansion/Migration scenarios.
Cisco IW6300 AP	IOS-XE 17.1.1s	Newly introduced ruggedized AP for outdoor environments. Can be used both for greenfield and brownfield expansion/migration/replacement.
Cisco Prime Infrastructure	3.7	Wired and Wireless Network Management
Cisco CMX	10.6.2	Location Services, Asset Tracking
Cisco Identity Services Engine (ISE)	2.6	Identity Store, IEEE 802.1X authentication, Network Policy Server
Cisco Catalyst 9300	IOS-XE 17.1.1s	PoE enabled access layer switch
Cisco IE 3400	IOS-XE 17.1.1	Ruggedized PoE-enabled access layer switch

Hazloc for Refineries

Operating in environments where flammable or explosive gases, vapors, or dust might be present requires communications equipment certified for use in a Hazardous Locations - often abbreviated as "HazLoc". Hazardous locations can be found in many industries, such as refineries, fuel storage facilities, chemical plants, grain elevators, and plastics processing plants. The National Electrical Code (NEC) NFPA 70 defines hazardous locations this way: "where fire or explosion hazards may exist due to flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers or flyings."

Equipment manufacturers do not determine the need for "hazloc" products, or evaluate the environment in which the communications equipment will be used. The Hazardous Location classification is determined by the Authorities Having Jurisdiction (AHJs) over the particular facility, for example the fire marshal, insurance provider or facility safety expert.

NATIONAL ELECTRICAL CODE (NEC) NFPA 70

Classes
- Class I: Flammable Gases, Vapors, or Liquids
- Class II: Combustible Dust
- Class III: Ignitable Fibers and Flyings

Division (Area Classification)
- Division 1: Locations where ignitable gas/vapor/liquid/dust are present continuously or some of the time under normal operating conditions
- Division 2: Locations where ignitable gas/vapor/liquid/dust are not likely to exist under normal operating conditions

Groups (Organized by Classes)

Class I Gas Groups
- Group A - Acetylene and equivalent gas groups
- Group B - Hydrogen and equivalent gas groups
- Group C - Ethylene and equivalent gas groups
- Group D - Methane and equivalent gas groups

Class II Dust Groups
- Group E - Conductive dust (mechanical — factories, recyclers)
- Group F - Combustible carbon dust (charcoal & coke dust) - above ground only
- Group G - Grain dust

Class III Fibers has no sub-groups

Refineries and process plants are environments which require intrinsically-certified communications systems to eliminate the potential of explosions from gases and chemicals. Communication systems must be ATEX and HAZLOC certified to assure safe operations in these potentially hazardous environments.

Cisco has recently announced the introduction of a new ruggedized heavy-duty outdoor AP - the IW6300, which has been specifically designed for ruggedized outdoor environments like oil and gas and mining. These mesh access points feature a Class I Division 2 enclosure and are designed to bring resilient Wi-Fi mesh that is scalable and secure to hazardous environments. The IW6300 APs are compatible with both Cisco AireOS WLCs and the newer Catalyst 9800 IOS-XE based WLCs.

Cisco WLAN Controllers

The industrial WLAN is a controller-based wireless design, which simplifies network management by using Cisco WLAN controllers (WLCs) to centralize the configuration and control of wireless APs. This approach allows the WLAN to operate as an intelligent information network and to support advanced services. The following are some of the benefits of the controller-based design:

- **Lower operational expenses**-Enables zero-touch configurations for lightweight APs; easy design of channel and power settings and real-time management, including identifying any RF holes in order to optimize the RF environment; seamless mobility across the various APs within the mobility group; and a holistic view of the network, supporting decisions about scale, security, and overall operations.

- **Optimized turn-up**-Enables streamlined configuration of WLAN controller and overall wireless network through the implementation of best practices during initial WLC configuration.

- **Improved return on investment**-Enables virtualized instances of the WLAN controller-for only the virtual wireless LAN controller (vWLC)-reducing the total cost of ownership by leveraging their existing investment in a virtualized infrastructure.

- **Easier way to scale with optimal design**-Enables the network to scale well, by supporting a centralized (local mode) design for industrial environments, and Cisco FlexConnect design for lean remote sites.

- **High availability stateful switchover**-Enables non-disruptive connectivity to wireless client devices during a WLAN controller failure.

Cisco WLAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, QoS, and mobility. They work in conjunction with Cisco lightweight APs in order to support business-critical wireless applications. From voice and data services to location tracking, Cisco WLAN controllers provide the control, scalability, security, and reliability that network managers need to build secure, scalable wireless networks.

Cisco Lightweight APs (LWAPs)

In the Cisco Unified Wireless Network architecture, APs are *lightweight*. This means they cannot act independently of a WLAN controller. When the AP communicates with the WLAN controller, it downloads its configuration and it synchronizes its software or firmware image. Cisco lightweight APs work in conjunction with a Cisco WLAN controller in order to connect wireless devices to the LAN while supporting simultaneous data-forwarding and air-monitoring functions.

Centralized (Local-Mode) Design Model

A centralized design model, also known as a local-mode design model, is recommended primarily for large site deployments. The benefits of a centralized design include IP address management, simplified configuration and troubleshooting, and roaming at scale. In a centralized design model, the WLAN controller and APs are both located within the same site. The WLAN controller can be connected to a data center services block, a separate services block off of the campus core, or a LAN distribution layer. Wireless traffic between WLAN clients and the LAN is tunneled by using the control and provisioning of wireless access points (CAPWAP) protocol between the controller and the AP.

A centralized architecture uses the controller as a single point for managing Layer 2 security and wireless network policies. It also enables services to be applied to wired and wireless traffic in a consistent and coordinated fashion.

In addition to providing the traditional benefits of a Cisco Unified Wireless Network approach, the local-mode design model meets the following customer demands:

- **Seamless mobility** - Enables fast roaming, so that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets.

- **Ability to support rich media** - Enhances robustness of voice with call admission control and multicast with Cisco Video Stream technology.

- **Centralized policy** - Enables intelligent inspection through the use of firewalls, as well as application inspection, network access control, policy enforcement, and accurate traffic classification.

Cisco Prime Infrastructure

Cisco Prime Infrastructure is used for day-0/1 provisioning and day-N assurance and management of the wired and wireless infrastructure.

Cisco CMX

Cisco CMX is primarily used to provide location services for use-cases like asset tracking. Both Wi-Fi client location and the location of active RFID tags is displayed within Cisco CMX.

Cisco Identity Services Engine (ISE)

Cisco ISE is used as the centralized server for policy definition and enforcement within the network. Cisco ISE can be used as a user/device identity store or can integrate with 3rd-party identity stores such as Microsoft Active Directory (AD). Cisco ISE is used to define user/device authentication/authorization policies. The WLC queries Cisco ISE to authenticate/authorize users using IEEE 802.1X.

802.11 Mesh Networks

A mesh is a network topology that allows all the nodes (devices) on the network to communicate with each other. A wireless mesh network is a multi-hop wireless network formed using a number of stationary wireless mesh APs. The APs are connected using a wireless backhaul to form a mesh-like backbone structure. Some of the APs within the mesh are connected to the wired network using a wired connection and these APs are designated as Root Access Points (RAPs). Other APs that connect to each other and the RAP(s) using a wireless backhaul connection are known as Mesh Access Points (MAPs).

Using IEEE 802.11 (Wi-Fi) to build a wireless mesh infrastructure makes it possible for companies to extend the network coverage to certain areas where otherwise it would be cost-prohibitive and complex to run physical Ethernet or Fiber cables. This flexibility enables the ability to connect devices to the network which would not have been possible in the past.

Mesh Access Point Roles

Access points within a mesh network operate in one of the following two ways:

- Root access point (RAP)

- Mesh access point (MAP)

While the RAPs have wired connections to the controller, the MAPs have wireless connections to their controller. MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a/n radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

Adaptive Wireless Path Protocol (AWPP)

Wireless routing is a key technology enabling the deployment of large wireless mesh networks.The Adaptive Wireless Path Protocol (AWPP) is designed specifically for wireless mesh networking to provide ease of deployment, fast convergence, and minimal resource consumption.

AWPP establishes an optimal path through a mesh of wireless nodes to a wired gateway, creating a self-configuring, self-healing wireless mesh backhaul. AWPP addresses the challenges of routing packets over wireless links, which have very complex packet loss characteristics compared to wired networks. AWPP comes out of Cisco's long experience and leadership in routing protocols as well as indoor and outdoor wireless networks.

AWPP replaces the work done by RF engineers with a protocol that dynamically discovers neighboring radios and calculates the quality of all possible paths to the wired network. These calculations are continuously updated, allowing network connectivity and paths to change as the traffic patterns on wireless links change. The ability of AWPP to quickly adapt to changing links eliminates any single point of failure and dramatically boosts the network's reliability. Its compelling characteristics include fault tolerance, reliability, scalability and adaptability to a wide range of wireless environments.

Extensive RF engineering and analysis can be replaced by more efficient statistical analysis for AP placement. As AWPP constantly monitors the network, mesh nodes that fail are quickly bypassed through a list of alternative paths always maintained by AWPP. As coverage requirements change, the mesh adapts and forms a new topology optimized for the particular placement of APs and the RF characteristics of the aggregate wireless mesh.

AWPP enables a remote access point to dynamically find the best path back to a RAP for each MAP that is part of the RAP bridge group name (BGN). AWPP takes RF details into consideration when selecting the best path back to the RAP.

AWPP helps establish the best path for a MAP to reach a RAP. AWPP uses a "Parent Stickiness" value to mitigate Route Flaps. Preferred parent can be manually configured if needed. AWPP integrates with 802.11 DFS (Dynamic Frequency Selection) for radar detection and avoidance.

To find an optimal route back to the RAP, a MAP actively solicits neighboring MAPs. During the solicitation, a MAP learns about all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor. The path decisions of AWPP are based on the link quality and the number of hops. AWPP automatically determines the best path back to the CAPWAP controller by calculating the cost of each path in terms of the signal strength and number of hops. After the path is established, AWPP continuously monitors conditions and changes the route to reflect changes in conditions. AWPP also performs a smoothing function to signal condition information to ensure that the ephemeral nature of RF environments does not impact network stability.

The benefits of this self-configuring, wireless mesh solution are substantial.

Wireless Mesh Traffic Types

Wireless mesh networks can simultaneously carry two different traffic types:

- Wireless LAN client traffic, such as Wi-Fi traffic from a mobile worker's hardened tablet

- Ethernet Bridged Traffic for wired devices connected to the RAP/MAP, such as a Video Surveillance Camera Traffic, or WiHART Gateway/Sensor Traffic

Wireless LAN client traffic terminates on the controller, and the Ethernet bridged traffic is backhauled over the mesh network and dropped off at the RAP Ethernet switch port.

IEEE 802.15.4 Wireless Networks

IEEE 802.15.4 is a standard that has been developed to provide a framework and the lower layers in the OSI model for low cost, low power wireless connectivity networks. IEEE 802.15.4 provides the MAC and PHY layers, leaving the upper layers to be developed for specific higher later standards like Thread, Zigbee, 6LoWPAN and many others. Low power is one of the key elements of 802.15.4 as it is used in many areas where remote sensors need to operate on battery power, possibly for years without attention.

Technology advancements in measurement instruments and final control elements provide greater process insight, reduce engineering costs, and contribute to improving the overall operational performance of the plant. These instruments are often collectively referred to as smart devices. These smart devices include advanced diagnostics that can diagnose the health of the device and in many cases, the health of the process that the device is connected to. It is not uncommon for smart devices to include diagnostics that can detect plugged lines, burner flame instability, agitator loss, worn motor bearings, wet gas, orifice wear, leaks, and cavitation. These devices tell the user how well they are operating and when they need maintenance. Many customers have reported substantial savings when using smart devices. Getting this technology to the field has often been hampered by the high costs of installation as well as other factors.

To address these needs what has emerged is a whole new line of devices utilizing wireless technology. Although some of these devices contain the same technology as their wired counterparts, newer devices are emerging with innovative low powered sensors and mobile sensors. The most prominent wireless technology to-date utilizes IEEE 802.15.4 compatible DSSS radios and operates in the 2.4GHz ISM radio band (IEEE 802.15.4 supports multiple bands). Two standards based upon the IEEE 802.15.4 radio technology are IEC62591-1 (*Wireless*HART) and ANSI/ISA100.11a-2011 (ISA100.11a). The international standard, *Wireless*HART, and the US standard, ISA100.11a, both provide full descriptions of the communication stacks.

IEC62591-1 Wireless HART

*Wireless*HART is one of the IEEE 802.15.4 derived standard. *Wireless*HART is an open-standard wireless networking technology that has been developed by HART Communication Foundation for use in the 2.4 GHz ISM band. The system uses IEEE802.15.4 for the lower layers and provides a time synchronized, self-organizing, and self-healing mesh architecture.

*Wireless*HART is based on the HART Communication protocol. The HART application layer has been in existence since the late 1980s. In its initial release, the HART Field Communications Protocol was superimposed on a 4-20mA signal providing two-way communications with field instruments without compromising the integrity of the analog output. The HART protocol has evolved from a simple 4-20mA based signal to the current wired and wireless-based technology with extensive features supporting security, unsolicited data transfers, event notifications, block mode transfers, and advanced diagnostics. Diagnostics now include information about the device, the equipment the device is attached to, and in some cases, the actual process being monitored.

*Wireless*HART targets sensors and actuators, rotating equipment such as kiln dryers, environmental health and safety applications such as safety showers, condition monitoring, and flexible manufacturing in which a portion of the plant can be reconfigured for specific products. *Wireless*HART technology is secure, cost-effective, and delivers greater than 99% data reliability.

ISA100.11a

ISA100.11a (IEC 62734) is another IEEE 802.15.4 derived standard. This standard has been developed by ISA as an open-standard wireless networking technology and is targeted as a wireless system for industrial automation including process control and other related applications.

Just like WiHART, ISA100.11a is an open standard maintained by independent industry organizations and recognized by the IEC. ISA100.a also uses the 2.4GHz spectrum like WiHART. Like WiHART, ISA100.11a is also designed for communication of low data-rates over short distances with low power consumption. Both WiHART and ISA100.11a use AES-128 encryption and a secure network join mechanism.

Both WiHART and ISA100.11a have extensive catalogs of compatible process instruments, actuators and accessories provided by multiple vendors. Both provide multi-vendor interoperability and certified devices.

ISA100.11a implementations typically use a star topology where groups of individual end devices cluster around a router which collects their data and sends it to a central gateway. Multiple routers can communicate with a single gateway. Routers are normally externally powered and can therefore have more powerful transmitters than end devices. They are helpful for gateway communications over longer distances with greater bandwidth.
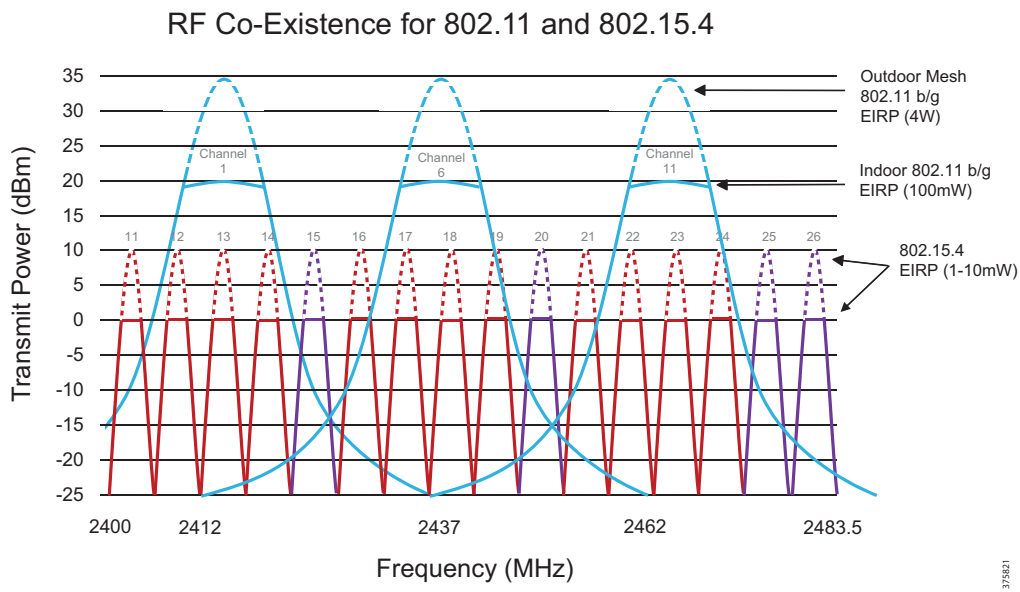
While this approach minimizes the need for meshing between end devices, there can be side effects. Due to typical ISA100.11a network topologies, communication is line-of-sight and devices need to be visible to a router. This means routers need to be mounted in relatively high locations where they can communicate with individual end devices while maintaining a clear path to the gateway.

Wireless Co-Existence

Multi-service wireless traffic using 802.11 protocols and operational wireless traffic using 802.15.4 protocols both share the same 2.4GHz frequency band. Thus, packets can interfere with each other when transmitted at the same time and frequency with sufficient energy. Both protocols use mechanisms to mitigate these issues including:

- Frequency Diversity-Channel hopping

- Time Diversity-Time Division Multiplexing

- Power Diversity-Low power output (<= 10dBm)

- Space Diversity-Mesh technology that allows for space coverage through multiple hops instead of using just output power

- Coding Diversity-Direct Sequence Spread Spectrum

Figure 16   Channel Interference for 802.11 and 802.15.4

The redundant paths offered by the meshing capabilities significantly increase reliability compared to solutions requiring direct line of site. If the network or environment changes, the self-healing, self-organizing networks find new, optimal paths for increased reliability. Combined, these features help mitigate problems not just from other RF devices, but also EM noise from other nearby sources typical in refinery and plant environments.

Based on joint testing between Cisco and Emerson conducted in a process facility with both 802.11 and 802.15.4 deployments, no significant degradation occurred in either the 802.11 network performance, due to features such as retries and path diversity or the 802.15.4 sensor network performance. The sensor network did exhibit some packet loss, but not enough to affect the overall data reliability as a direct result of robust features such as retries and path diversity. The baseline data reliability was 100% and the data reliability during the test period remained at 100%.

WiHART or ISA100 gateway/sensor Deployment Guidelines

Below are some deployment guidelines when installing WiHART or ISA100 gateways/sensors within your plant:

- Mounting the Wi-Fi and *Wireless*HART/ISA100.11a co-linear pattern, for example, vertically with one antenna directly above the other to maximize isolation is recommended. When mounted co-linearly each antennas is in a null of the other antenna radiation pattern. At least 3 feet of vertical antenna separation is recommended. The target radiated antenna isolation is 40 dB at 2.4 GHz.

- 40 dB isolation will result in no more than 6 dB desensitization to the Wi-Fi radio while the *Wireless*HART/ISA100.11a radio is transmitting. Desensitization is a degradation of the sensitivity of the receiver due to external interference, and results in dropped or interrupted wireless connections or a drop in throughput.

- If the antennas must be mounted at the same elevation, then they should be mounted at least 20 feet apart horizontally to reach 40 dB isolation. If there is less than 20 feet of separation, there may be interference that can degrade the throughput and decrease the maximum allowable range of both radios. The degree of the degradation will depend upon the amount of traffic loading and transmit duty cycles of each of the radios.

- If the 2.4 GHz Wi-Fi band is turned off and only 5 GHz Wi-Fi is used, then a minimum of 3 feet of horizontal separation is acceptable.

Greenfield Deployment Architecture

The figure below depicts the oil and gas connected refinery greenfield architecture. A greenfield deployment is where-in we are deploying wireless access within a newly deployed plant or a plant where-in there is no existing wireless coverage. The recommended WLC for greenfield deployments is the next-gen Cat-9800 IOS-XE based WLC and the IW6300 heavy-duty access point deployed within a wireless mesh topology.

Figure 17   Greenfield Topology

Cisco 9800 Wireless LAN Controller (WLC)

Cisco Catalyst® 9800 Series Wireless LAN Controllers (WLC) are the next generation of wireless controllers built from the ground-up for the Intent-based networking. The Catalyst 9800 Series Controllers are IOS XE-based and integrates the RF excellence from Aironet with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for the evolving and growing organization.

The Catalyst 9800 Series Wireless Controller Appliance comes in three form factors:

   – **Cisco Catalyst 9800**-L Wireless Controller - a compact controller appliance that is the perfect complement to the small to medium-sized network deployment. Data ports can operate in 1GE and 10 GE mode supporting different SFP/SFP+ transceivers and up to 5Gbps of throughput.

   – **Cisco Catalyst 9800**-40 Wireless Controller - Fixed wireless controller with seamless software updates. Data ports can operate in 1GE and 10 GE mode supporting different SFP/SFP+ transceivers and up to 40Gbps of throughput.

   – **Cisco Catalyst 9800**-80 Wireless Controller - Modular wireless controller with 100GE modular uplink and seamless software updates. Fixed data ports can operate in 1 GE and 10 GE mode supporting different SFP/SP+ transceivers and up-to 80 Gbps of throughput. Modular Uplink provides flexible connectivity options supporting 10GE, 40GE, 100GE QSFP hot-swappable transceivers.

Seamless software updates include Software Maintenance Update (SMU) for Hot and Cold patching on wireless controllers, AP Service Pack for maintenance update on access points, AP Device Pack for introduction of new AP hardware into the network and Intelligent Rolling AP Upgrade for hitless controller and access point upgrade.

Table 3

Platform	Deployment Mode	Preferred Topology	Maximum APs	Maximum Clients	Controller Throughput
Cisco Catalyst 9800-40	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Large Single or Multiple Site	2,000	32,000	40 Gbps
Cisco Catalyst 9800-80	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Large Single or Multiple Site	6,000	64,000	80 Gbps
Cisco Catalyst 9800-L	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Small Local Controller Site	250	5,000	5 Gbps
Cisco 9800-CL vWLC (Small)	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Small Enterprise	1,000	10,000	1.5 Gbps
Cisco 9800-CL vWLC (Medium)	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Mid-size Enterprise	3,000	32,000	1.5 Gbps
Cisco 9800-CL vWLC (Large)	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)	Large Enterprise	6,000	64,000	1.5 Gbps

Note: For additional details on the Catalyst 9800 WLCs please refer to:
https://www.cisco.com/c/en/us/products/wireless/catalyst-9800-series-wireless-controllers/index.html

Cisco IW6300 Heavy Duty Series Access Points

The Cisco Catalyst IW6300 Heavy Duty Series Access Points enable delivering a resilient wireless mesh network that is both secure and scalable. Designed specifically for hazardous locations, with Class-I Div-2 certification - protected by a sealed, corrosion-resistant enclosure, including IP67 dust and water resistance certification. Partner designed modules easily attach to enable Industrial Internet of Things (IIoT) with support for *Wireless*HART, ISA100, GPS, Bluetooth Low-Energy, Zigbee and much more. It provides certified and dependable Wireless AC Wave 2 with WPA3 encryption, 3 PoE ports and 1 SFP port.

Note: For more details on the IW6300 please refer to the product data sheet -
https://www.cisco.com/c/en/us/products/collateral/wireless/industrial-wireless-6300-series/datasheet-c78-742907.html

Greenfield Wireless Design

A multi-service wireless design provides the necessary infrastructure to support the mobile workforce, enhance plant turnaround time, provide access to a remote expert, and monitor the health and safety of refinery employees. It lays the critical foundation for subsequent services to be enabled.

To support these use cases, the Wireless LAN (WLAN) design is based on the Cisco Unified Wireless Network architecture. At the heart of this architecture is the Wireless LAN Controller (WLC) which handles all necessary functions related to system-wide operations and policies such as mobility, security, QoS, and radio frequency management. Wireless APs work in conjunction with the controller to connect wireless devices to the LAN and support lower level functions such as beacon handling, client handshakes, and media access layer control encryption. Two primary deployment models can be considered for a WLAN design: Centralized and FlexConnect.

■ In a Centralized deployment model, also known as local-mode, the WLAN controller and the APs are located within the same site (that is, there are no remote or branch locations). All client wireless traffic is tunneled between the AP and WLC using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. This model benefits by using one central location to manage IP addresses, configurations, and troubleshooting.

■ With a FlexConnect deployment, some traffic can be terminated directly at the AP, rather than being backhauled to the controller. Due to this bandwidth saving feature, this model is best suited for deployments containing multiple remote sites.

■ Due to the simplicity in configuration, greater control over traffic, and flexibility in access layer devices, a Centralized deployment model is recommended for refinery deployments.

■ Wireless APs in a centralized deployment are lightweight; they cannot operate without a WLC. Upon registering with the controller, the AP downloads the appropriate firmware or software image and its configuration. All communication between the AP and the controller takes place over an encrypted CAPWAP tunnel.

■ For greenfield scenarios, we recommend deploying the Cisco Catalyst 98XX WLCs along with the Cisco IW6300 Heavy Duty Access Points within a Mesh deployment. Multiple RAPs should be used for redundancy purposes.

■ For the video surveillance use-case, IP cameras can be attached to the PoE out port of the IW6300 MAP. For improved throughput and high resolution camera feeds one can also disable the 2.4GHz client access radio on that particular MAP so that only video traffic is carried over the backhaul link and it does not have to contend with any other Wi-Fi Client Traffic. In this design, the video stream will be Ethernet bridged and dropped off at the RAP Ethernet link. Any QoS markings from the video camera equipment will be preserved. It is recommended to segment the video stream traffic onto a separate VLAN from the Wi-Fi client traffic.

■ The Emerson IoT module which acts as a Wireless HART gateway plugs directly into the IW6300 and can communicate with the Emerson Rosemount Sensors to gather data and transmit it to industrial applications over the Cisco industrial wireless mesh network. Any QoS markings applied by the Emerson IoT module are preserved over the mesh backhaul network.

■ This mesh network can be managed using Cisco Prime Infrastructure. The mesh topology depicting the mesh parent child relationship can be viewed within Cisco Prime Infrastructure. Location services for Wi-Fi client location and RFID tag location for asset tracking is enabled using Cisco Prime Infrastructure and Cisco CMX.

■ For wireless IoT devices that are not able to be configured for IEEE 802.1X authentication an SSID with pre-shared key (PSK) can be advertised throughout the refinery plant. The traffic from IoT devices can be segmented into a separate VLAN. This VLAN can only be provided access to the IoT controller and to the Internet if needed.

■ For use-cases like worker mobility an SSID configured with 802.1X can be advertised throughout the refinery plant. This traffic can be separated into its own VLAN and provided more privileges. Access can be granted for the mobile worker to access the corporate servers and applications that he needs access to perform his duties.

Note: For more details on Cisco Mobility Design refer to:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.html
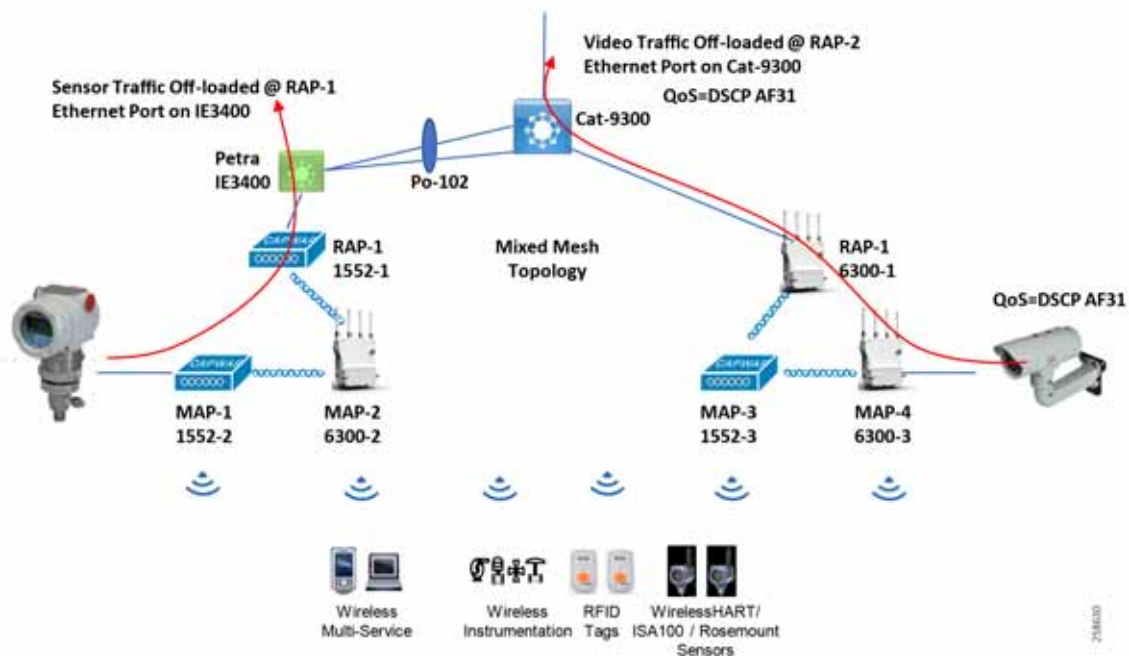
Note: For more details on Cisco Mesh Network Design refer to:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-8.html

Ethernet Bridging Over Mesh

Ethernet bridging technology helps bridge multiple wired network domains over a wireless mesh network. In Ethernet bridging devices such as IP-enabled video surveillance cameras are connected to one of the Ethernet ports on the wireless AP. Ethernet bridged traffic is carried over the mesh backbone and is offloaded on the first switch where the RAP is connected and not transported via the CAPWAP tunnel all the way to the WLC like regular wireless traffic. Any QoS markings on the Ethernet bridge traffic are preserved as they travel over the mesh backbone all the way to the switchport where the RAP is connected.

Figure 18   QoS Markings preserved for Ethernet Bridged Traffic

The figure above depicts a video surveillance camera connected to the Ethernet port of MAP-4. The video traffic is marked with a DSCP value of AF31. This video surveillance traffic stream is offloaded on the Cat-9300 switchport where RAP-2 is connected. The DSCP value of AF31 is preserved along the way.

On the other side we have a wired sensor that is connected to the Ethernet port of MAP-1. This traffic is offloaded on to the IE3400 switchport where RAP-1 is connected.

Within a refinery, Ethernet bridging is especially helpful for the following use-cases:

- Connecting video-surveillance cameras.

- Connecting IoT Wireless Instrumentation (WiHART or ISA100.11a) Gateways. The Emerson IoT modules plug-in to the PoE out port of the APs and this traffic is Ethernet bridged.

- Extending network services such as a remote office to an area of the refinery where there isn't any network cabling.

Ethernet bridging can be used with multiple VLANs. This feature is useful for trunking multiple VLANs to remote switches connected to MAP Ethernet ports. The RAP switchport native VLAN (untagged) functions as the mesh management network. This feature helps segment Ethernet bridged traffic into different L2 domains. Within a refinery environment we can use it to segment Video surveillance traffic onto its own VLAN. We can segment Wireless Instrumentation traffic into its own dedicated VLAN.

Depending on your use-case you might want to disable the client-side radio interface on the MAP that is being used for Ethernet bridging functionality so as not to overwhelm its backhaul link by having it to carry both the Ethernet bridged as well as the Wi-Fi client traffic. By disabling the Wi-Fi client radio interface the backhaul link between the MAP and its neighboring AP(s) only has to carry the Ethernet-bridged traffic.

Note: "VLAN Transparent" is a legacy method for Ethernet bridging. VLAN tags are not handled and packets are bridged as untagged packets. This is typically not used. It is enabled by default for backward compatibility reason.

Note: As a best practice it is recommended to have the Ethernet-bridged traffic going over a separate VLAN(s) from the wireless client traffic.

Redundancy and High-Availability (HA)

WLC Redundancy

High availability is a requirement for wireless controllers in order to minimize network downtime. In order to enable redundancy for the 98XX WLCs we recommend deploying the controllers as a High availability Stateful Switchover (SSO) pair.

The High availability SSO capability on the Cisco Catalyst 98XX wireless controller allows the access point to establish a CAPWAP tunnel with the Active wireless controller. The Active wireless controller in-turn shares a mirror copy of the AP and client database with the Standby wireless controller. The APs do not go into the Discovery state and clients do not disconnect when the Active wireless controller fails and the Standby wireless controller takes over the network as the Active wireless controller. There is only one CAPWAP tunnel maintained at a time between the APs and the wireless controller that is in an Active state.
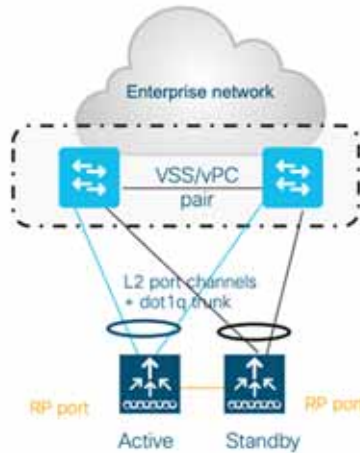
Release 16.10 and later supports full AP and Client Stateful Switch Over. Client SSO is supported for clients which have already completed the authentication and DHCP phase and have started passing traffic. With Client SSO, a client's information is synced to the Standby wireless controller when the client associates to the wireless controller or the client parameters change. Fully authenticated clients, for example, the ones in Run state, are synced to the Standby and thus, client re-association is avoided on switchover making the failover seamless for the APs as well as for the clients, resulting in zero client service downtime and zero SSID outage. With AP and Client SSO support on the Catalyst 9800 Wireless controller helps reduce major downtime in wireless networks due to failure conditions that may occur due to box failover, network failover or power outage for the primary controller.

The standby controller can be cost-effectively licensed, using the High Availability SKU, specifically as a standby controller with the AP license count automatically inherited from the paired primary WLAN controller.

When Link Aggregation (LAG) is enabled on the uplinks, the WLC can dynamically manage the port redundancy and can load-balance traffic on the APs. Furthermore, if any of the LAG ports fail, traffic is automatically transferred to one of the other ports. Thus, as at least one of the WLC uplinks is operational, the WLC and the APs will remain operational.
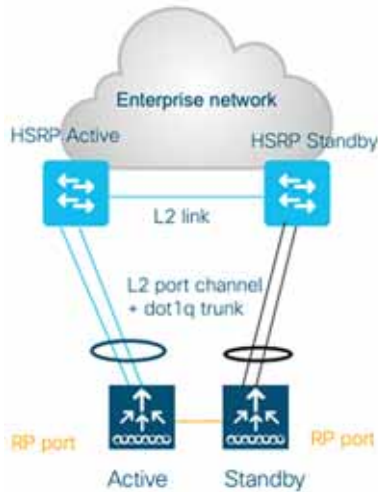
Further redundancy can be configured through the use of link aggregation between multiple switches in a VSS deployment as shown in the figure below. A VSS can also be referred to as multi-chassis EtherChannel. A single L2 port-channel on each box. Ports connected to Active and ports connected to Standby must be put in different port-channels. Enable dot1q to carry multiple VLANs. An important point to note here is that only LAG with mode ON is supported. Spread the WLC uplinks across the VSS pair and connect the RP link back to back with no L2 in between. One consideration to keep in mind is selecting a switch model that can scale in terms of ARP and MAC table entries.

Figure 19   WLC High-Availability using VSS/vPC

If your design incorporates HSRP then you can implement WLC redundancy as shown in the figure below. Configure a single L2 port-channel on each WLC. Ports connected to Active and ports connected to Standby must be put in different port-channels. The Cat-9800 WLC supports both PagP and LACP. Enable dot1q to carry multiple VLANs. One consideration to keep in mind is selecting a switch that can scale in terms of ARP and MAC table entries.

Figure 20   WLC High-Availability with HSRP Topology

Note: For a mesh topology, WLC failover is not stateful. The RAPs connected to the wired network failover pretty quickly, however it takes a couple of minutes for the MAPs to failover and for the mesh to re-converge and become stable.

Note: For details on how to deploy SSO HA for the Catalyst 9800 WLC please refer to: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_ha_sso_dg.html

Bridge Group Name (BGN)

Membership to the wireless LAN mesh network for mesh access points is controlled by the bridge group names (BGNs). Mesh access points can be placed in similar bridge groups to manage membership or provide network segmentation. Bridge group names (BGNs) help logically group APs and control the association of mesh access points.

BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string of 10 characters maximum. A BGN of NULL VALUE is assigned by default by manufacturing. Although not visible to you, it allows a mesh access point to join the network prior to your assignment of your network-specific BGN.

For adding capacity we recommend that you have more than one RAP in the same sector, with the same BGN, but on different channels. Having multiple RAPs with the same BGN in an area is good for redundancy – when a RAP goes down, its MAPs will join a different sector with the same name.

When Strict Match BGN is enabled on the mesh AP, it will scan ten times to find the matched BGN parent. After ten scans, if the AP does not find the parent with matched BGN, it will connect to the non-matched BGN and maintain the connection for 15 minutes. After 15 minutes the AP will again scan ten times and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled.

Note: BGN misconfigurations will cause network instability.

Preferred Parent

You can configure a preferred parent for a MAP. This feature enables more control and helps in enforcing a certain desired mesh network topology. We can bypass AWPP and force a MAP to go to a preferred parent.

Preferred Parent Selection Criteria

The child AP selects the preferred parent based on the following criteria:

- The preferred parent is the best parent.

- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).

- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.

- The preferred parent is not blacklisted.

- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).

- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

ISE HA Deployment

Deploying Cisco ISE in a large network requires an IT security architect to consider several factors such as scalability and high-availability. This design guide covers many factors related to deploying a large-scale Cisco ISE deployment. We encourage the reader to read the CPwE CVD to develop a good understanding of large-scale solution deployments. Some of the key recommendations given in the design guide are shown here as a quick reference.

In the distributed installation, the Cisco ISE system is divided into three discrete nodes (personas)-Administration, Policy Service, and Monitoring-which are described as follows:

- The Policy Administration Node (PAN) allows the Enterprise IT team to perform all administrative operations on the distributed Cisco ISE system. The PAN (located in the Enterprise Zone) handles all system configurations that are related to functionality such as authentication and authorization policies. A distributed Cisco ISE deployment can have one or a maximum of two nodes with the Administration persona that can take on the primary or secondary role for high availability.

- The Policy Service Node (PSN) provides client authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation. At least one node in a distributed setup should assume the Policy Service persona and usually more than one PSN exists in a large distributed deployment.

- The Monitoring Node (MnT) functions as the log collector and stores log messages and statistics from all the PAN and PSN devices in a network. The MnT (located in the Enterprise Zone) aggregates and correlates the data in meaningful reports for the IT and OT personnel. A distributed system can have at least one or a maximum of two nodes with the Monitoring persona that can take on primary or secondary roles for high availability.

For optimal performance and resiliency, this CVD provides these recommendations for the Industrial Automation Identity and Mobility Services architecture:
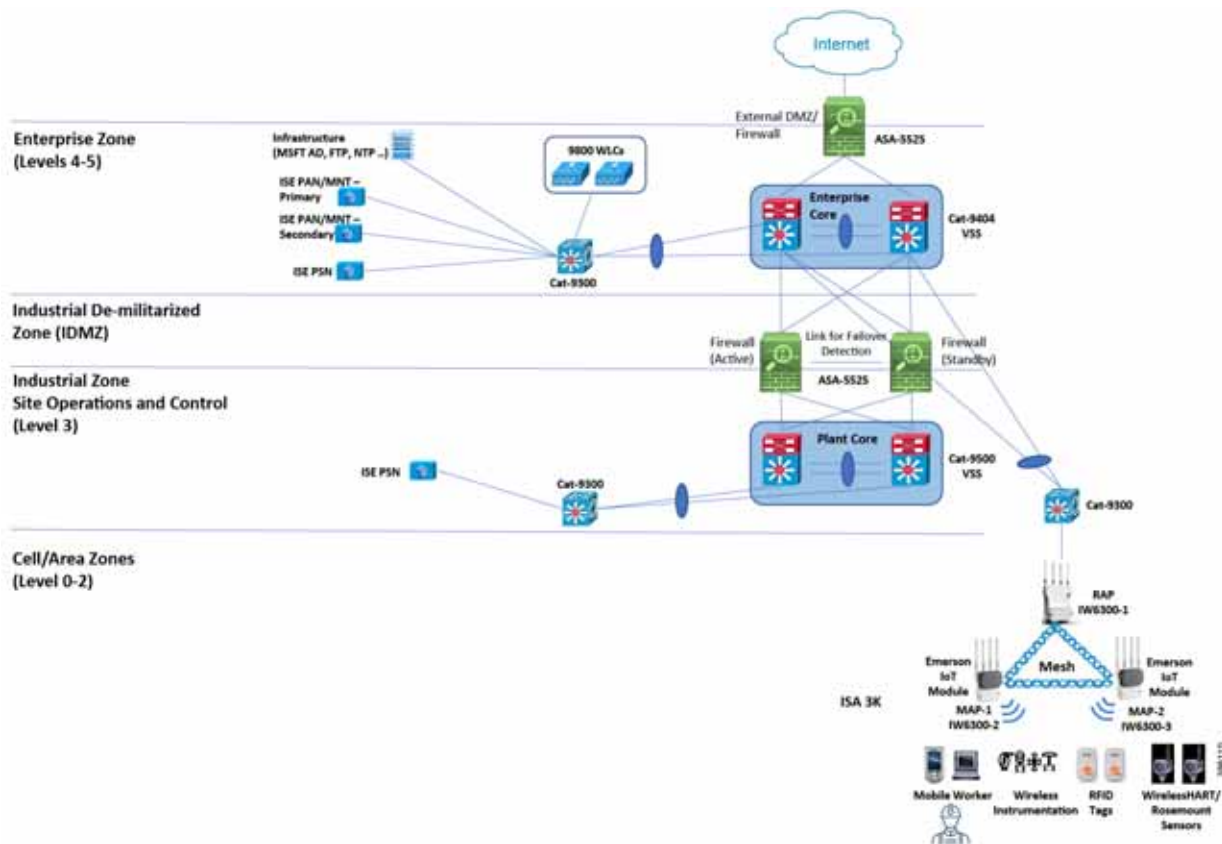
- Administration and Policy Service personas should be configured on different Cisco ISE nodes.

- Monitoring and Policy Service personas should not be enabled on the same Cisco ISE node. The Monitoring node should be dedicated solely to monitoring for optimum performance.

- A PSN should be placed in the Industrial Zone (Levels 0-3) to provide services for clients in the Industrial Zone. If the Enterprise and Industrial Zones become isolated, any existing clients will still be able to securely access the network. For best practices, see Previous and Related Documentation for links to the Industrial Automation IDMZ CVD DIG.

- A PSN should also be present in the Enterprise Zone to authenticate corporate mobile users who connect to the corporate network through the IDMZ in a secure data tunnel. This scenario is covered in detail later in the document.

Based on the recommendations above, a typical distributed Cisco ISE deployment in the Industrial Automation architecture consists of the following nodes (hardware appliances or VMs):

- One Primary Administration/Secondary Monitoring node

- One Secondary Administration/Primary Monitoring node

- One or several PSN in the Enterprise Zone

- One or several PSN in the Industrial Zone

Note: The number of PSN in the Enterprise and Industrial Zones may depend on the company size, the number of active clients, redundancy requirements, and geographical distribution (for example, one PSN per each plant).

Figure 21   Distributed ISE Deployment

Note: For additional details on deploying a distributed ISE deployment please refer to:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010.html

Security

Mesh AP Authentication

APs need to successfully authenticate with the WLCs in order to be able to join a mesh network. Two authentication methods are supported to enable this:

- MAC authentication – Mesh access points MAC addresses are added to a database on the WLC that can be referenced to ensure they are provided access to a given controller and mesh network.

- External RADIUS Authentication – Mesh access points can be externally authorized using a RADIUS server such as Cisco ISE that supports the client authentication type of Extensible Authentication Protocol-FAST (EAP-FAST) with certificates and WPA2/PSK on the WLCs.

Note: For our validation we used the MAC authentication method to authenticate APs with WLCs.

Wi-Fi Client Authentication

Wireless traffic between client endpoints and the APs should be secured using WPA2 with AES-CCMP encryption. Please note that WPA2 with AES-CCMP does not extend to management frames.

Clients connecting to the employee WLAN should be authenticated using 802.1X, which requires an AAA server such as the Cisco Identity Services Engine (ISE) that provides centralized policy-based management. Communication between the WLC and the AAA server uses the RADIUS protocol. Authentication of the end-user is accomplished using the Extensible Authentication Protocol (EAP). Multiple variants of EAP are available such as Protected Extensible Authentication Protocol (PEAP), EAP-TLS and EAP-FAST. PEAP makes use of standard user credentials (username and password) while EAP-TLS uses a digital certificate for authentication, which makes the process less painless for the end user but may not be supported on all devices.

The AAA server can authenticate the user against several different identity stores such as LDAP or Microsoft Active Directory (AD). When a service such as AD is used, further authorization status can be determined based on the groups to which the user belongs. For example, users in a contractor group may have a different set of access policies than a user belonging to the employee group. The use of an external identity store acts as a single point for granting or revoking credentials.

The AAA server can make further authorization decisions based on the type of device connecting (for example, an Apple iPad or Lenovo Laptop), the OS version running on the device, the level of anti-virus installed, the location of the end user, and time of day. All of these different parameters can be used to create differentiated access policies. Using a Mobile Device Manager (MDM) installed on the device (for example, on Android or iOS mobile devices), Cisco ISE can make even more granular decisions based on installed applications (or lack thereof) and security polices (such as passcode enforcement). With these measures in place, devices can also be blacklisted, if lost or stolen, or even remote-wiped, if deemed necessary for security reasons.

Once the appropriate policy is determined, an ACL, VLAN, or Cisco TrustSec Security Group Tag (SGT) can be pushed down to the WLC and applied to the client.

All multi-service wireless traffic is terminated at the WLC and must pass through an ASA firewall before proceeding to any other zone. Any access lists specific to the client, as pushed down from a policy node such as ISE, are enforced at the WLC or ASA. If the traffic is deemed appropriate, the ASA can be configured for analysis and inspection. Any suspicious traffic can be flagged or blocked, logged, and dealt with appropriately.
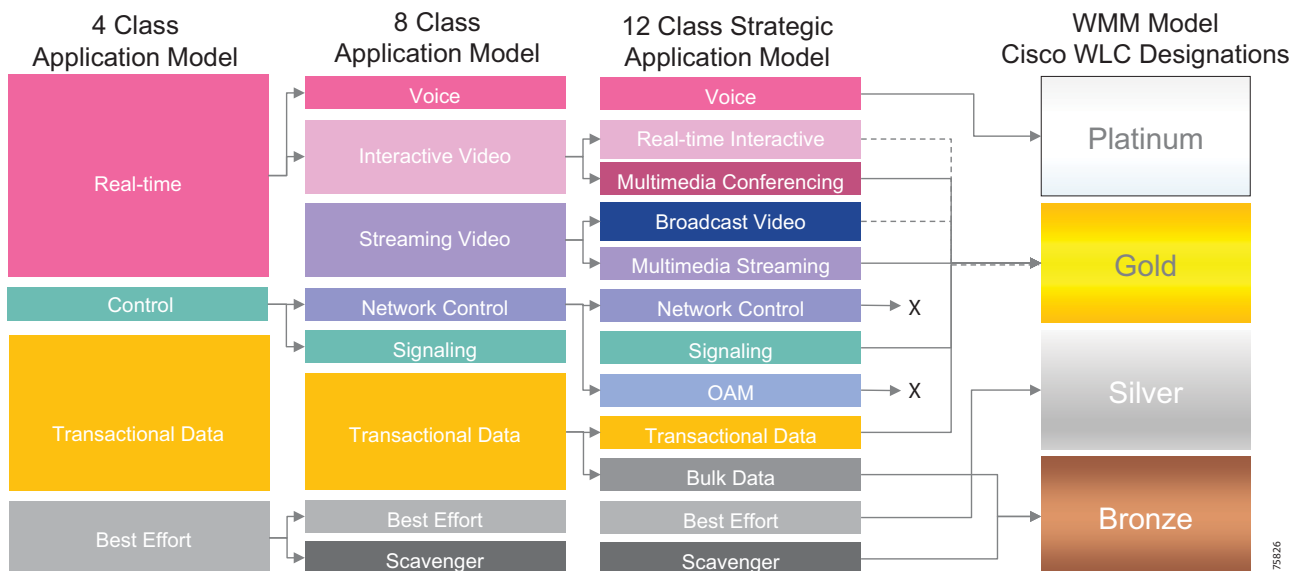
Quality of Service (QoS)

Due to the half-duplex nature and Layer 2 media access control (MAC) of 802.11 networks, QoS functions differently than it does in wired networks. Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification subset of 802.11e and defines four QoS classes: Voice, Video, Best Effort, and Background.

The Cisco WLC uses more generic terms for these classes with a designation based on precious metals: Platinum, Gold, Silver, and Bronze.

Although a WLAN only has four classes, that does not mean that the entire network cannot utilize more than these four classes. Rather the overall end-to-end QoS strategy should be based on the organizational requirements and then mapped into these four classes at the WLAN.

The figure below depicts various application models, including a complex 12-class application model and its fit in the WLC WMM categories.

Figure 22   Application Class Expansion Models Mapped to WMM

In the 12-class application model, Network Control and OAM traffic types are not typically generated by wireless clients and therefore are not mapped to a WMM category.

Once the traffic leaves the WLC and continues upstream to its wired destination, the corresponding VLAN onto which the WLC places the traffic must be configured for the same QoS policies.

By default, 6-bit DSCP values are mapped to 3-bit 802.1p CoS and 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as the CoS and/or UP values. For example, DSCP EF/46 (binary 101110) is mapped to CoS or UP 5 (binary 101) by default. For example, by default, the network switch that connects to the Cisco WLC will generate 802.1p CoS values (for the 802.1Q-trunked traffic) by setting these to match the three MSB of the DSCP values.

Table 4   Default Downstream DSCP to WMM Mapping

Application	DSCP	80211e UP	WMM Profile
Network Control	56 (CS7)	7	Platinum
Internetwork Control	48 (CS6)	7	Platinum
Voice	46 (EF)	6	Platinum
Multimedia Conferencing	34 (AF41)	5	Gold
Multimedia Streaming	26 (AF31)	4	Gold
Transactional Data	18 (AF21)	3	Silver
Bulk Data	10 (AF11)	2	Bronze
Best Effort	0 (BE)	0	Silver

Conversely, in the reverse direction, the CoS or UP values are simply multiplied by 8 (in order to shift these three binary bits to the left) to generate a DSCP value. Continuing the example, CoS or UP 5 (binary 101) would be mapped (that is, multiplied by 8) to DSCP 40 (binary 101000), also known as CS5.

Table 5   Default Upstream WMM to DSCP Mapping

WMM Profile	DSCP
Platinum	EF (DSCP 46)
Gold	AF41 (DSCP 34)
Silver	DF (DSCP 0)
Bronze	AF11 (DSCP 10)

In the examples in the table above, information is being truncated from 6-bits to 3-bits, marking details can get lost in translation. In this example, the original voice packet was sent with DSCP EF, but was received as DSCP CS5 (based solely on default Layer 3/Layer 2 mapping). This needs to be taken into account when mapping from wired-to-wireless and vice versa.

Note: It is critical to remember that QoS for wireless only offers a greater probability of one traffic type being differentiated or preferred over another; it is not a guarantee. Also, configuring a WLAN QoS level of say "Platinum", does not alter the original QoS marking of a frame, but sets the highest QoS allowed.

Radio Frequency Coverage and Capacity

The Connected Refinery wireless access design must provide sufficient coverage and capacity to support the previously described use cases. Coverage defines the ability of a client to connect to an AP with sufficient signal strength to overcome any radio frequency interference. The edge of the coverage for an AP is based on the signal strength and signal-to-noise ratio (SNR) measured as the client device moves away from the AP. The signal strength required for good coverage will vary depending on the specific type of client devices and applications that need to be supported by the network.

The Radio Resource Management (RRM) feature in the Cisco WLC acts as a built-in RF engineer to provide real-time RF management of the wireless network consistently to relieve frequent manual intervention. RRM enables Cisco WLCs to continually monitor their associated lightweight APs for the following information:

- Track load - The total bandwidth used for transmitting and receiving traffic to track and plan network growth ahead of client demand

- Interference - The amount of traffic coming from other 802.11 sources

- Noise - The amount of non-802.11 traffic that is interfering with the currently assigned channel

- Coverage - The RSSI and SNR for all connected clients

- Other - The number of nearby APs

Using this information, RRM can periodically reconfigure the RF network for best efficiency. RRM automatically detects and configures new lightweight APs as they are added to the network. It then automatically adjusts associated and nearby lightweight APs to optimize coverage and capacity. RRM produces a network with optimal capacity, performance, and reliability.

Overlapping cell coverage is just as important as cell boundaries. Excessive overlap of coverage can result in some channel interference, unnecessary AP-to-AP roaming (by client devices that have a limited roaming algorithm), and added expense because of more APs being required.

For data networks, a typical overlap in coverage is set to about 10 percent to 15 percent of the overall cell coverage area. In contrast, for voice networks, a higher overlap in coverage is recommended to ensure seamless call hand-off when roaming between APs. For voice networks, the recommended overlap is 15 to 20 percent of the overall cell coverage area.

Note: A wireless network should be designed based on the RF requirements of the most restrictive client that you intend to use. For example, if wireless voice clients will used on the wireless networks, then more than likely, these clients will have the most stringent RF requirements for RSSI, SNR, latency, etc. Refer to your client datasheets to determine their RF requirements and design your wireless network accordingly.

Access Point Deployment

Antenna selection and proper placement of each wireless AP should be determined by a wireless site survey (see Deployment Considerations). If location services will be deployed, such as Cisco Connected Mobile Experiences (CMX), it is important to document the MAC address as well as the physical location of each AP. This step is critical for accurate location triangulation.

Lightweight Wireless Access Points (LWAPs) must be associated and registered with a controller before being operational. Upon booting up, the AP will try to discover a controller in a variety of ways. Once a controller is discovered, the AP will request to join it.

In order to prevent any rogue APs from joining the network is to enable a MAC filtering list for APs on the WLC. The MAC address of every AP must be added to this list prior to the AP discovering the controller.

APs require power in addition to a wired connection to the LAN. This can be achieved using a dedicated power supply per AP. However, depending on the model of AP being deployed and location/ environment, this requirement can be simplified by deploying Power over Ethernet (PoE) capable access layer switches. With PoE-capable switches, supported APs can be powered over the same physical cable that enables data transport.

For more information regarding placement of APs for various traffic types, refer to the **Access Point Coverage and Placement** section.

Access Point Coverage and Placement

The Connected Refinery wireless network supports multi-service traffic, operational traffic, and location services for asset tracking. The placement of APs and their coverage affects the reliability and effectiveness of all services. Many refineries will include a mix of environments and thus have a variety of requirements in different areas of the refinery. The Control Room, for example, may require only a basic data grade network, with sufficient coverage for some workers and their laptops. However, in a different, larger, and more hazardous area of the refinery, the network must be capable of accurately tracking the locations of worker and equipment as they move around. Therefore, the network must be able to support a combination of AP deployments of varying densities.

Ultimately, AP placement will depend on customer requirements, plant design, and the RF environment. In general, the guidelines described in the following sections should be considered.

Note: Cisco highly recommends that a Wireless Site Survey be conducted in order to determine the best placement for APs for optimal coverage and application performance.

Network Management using Cisco Prime Infrastructure

As networks and the number of services they support continue to evolve, the responsibilities of network administrators to maintain and improve their efficiency and productivity also grow. Using a network management solution can enable and enhance the operational efficiency of network administrators.

Cisco Prime Infrastructure is a sophisticated network management tool that can help support the end-to-end management of network technologies and services that are critical to the operation of the organization. It aligns network management functionality with the way that network administrators do their jobs. Cisco Prime Infrastructure provides an intuitive, web-based GUI that can be accessed from anywhere from within the network and gives the user a full view of a network use and performance.

Cisco Prime Infrastructure provides a graphical platform for wireless mesh planning, configuration, and management. Network managers can use the Prime Infrastructure to design, control, and monitor wireless mesh networks from a central location.

With Prime Infrastructure, network administrators have a solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make the Prime Infrastructure vital to ongoing network operations.
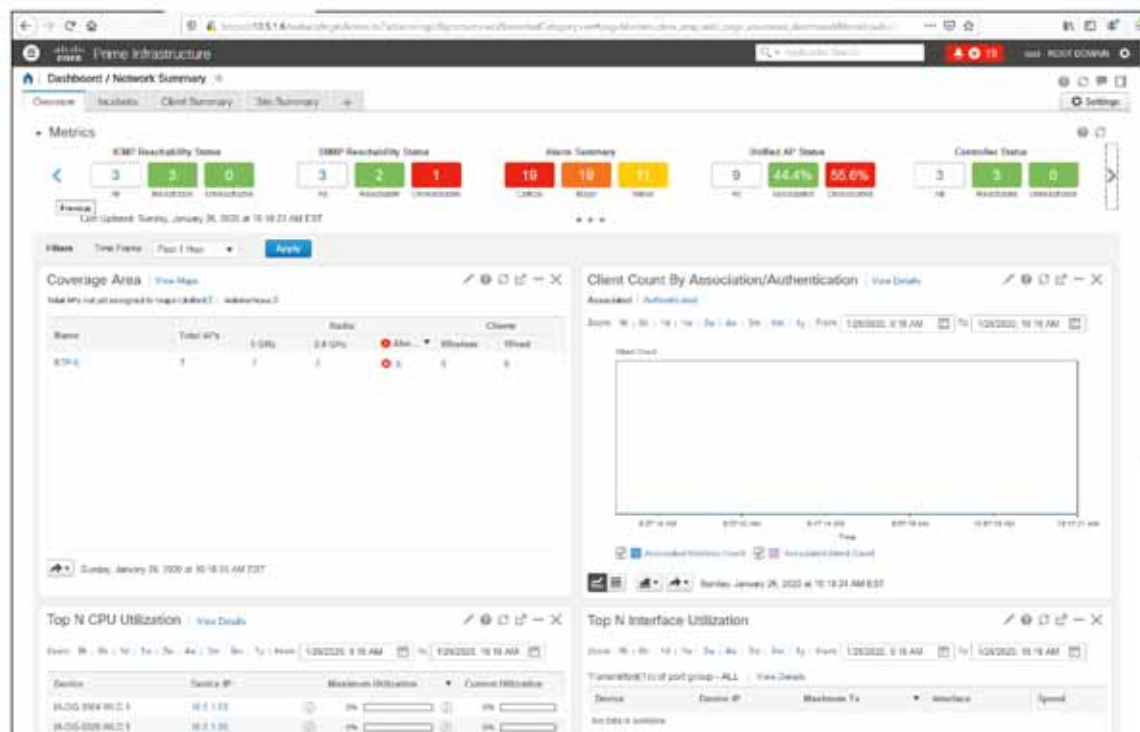
Prime Infrastructure runs on a server platform with an embedded database, which provides scalability that allows hundreds of controllers and thousands of Cisco mesh access points to be managed. Controllers can be located on the same LAN as the Prime Infrastructure, on separate routed subnets, or across a wide-area connection.

Cisco Prime Infrastructure can play a critical role in day-to-day network operations.

Monitoring Overall Network Health

As depicted in the figure below, Cisco PI can be used to monitor the overall health of your wireless deployment. The metrics and charts displayed on the dashboard are customizable and the entire dashboard can be exported as a CSV or PDF file for offline review.
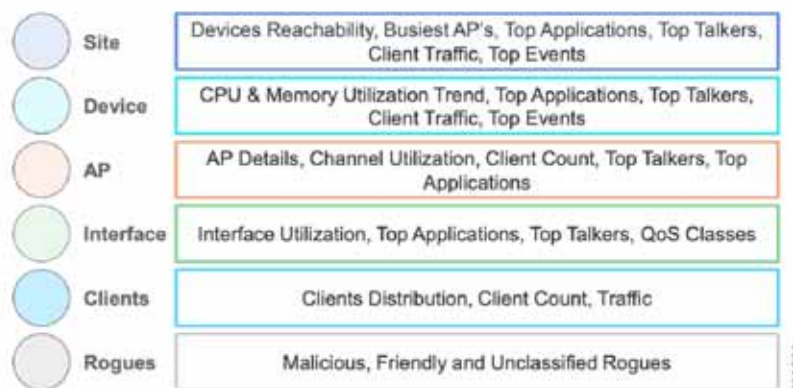
Figure 23   Cisco PI used to monitor Overall Network Health

Cisco PI Dashboard - What can you monitor?

Cisco PI is used to monitor different aspects of the wireless deployment as depicted in the figure below.

Figure 24   Monitoring using Cisco PI

Apart from the above, Cisco PI can be used to monitor the redundancy status of your WLC HA deployment, monitor AP and Client status and statistics and monitor Rouge APs in the network.

Alarms, Events, and Syslog Messages

Cisco Prime Infrastructure provides the Alarms and Events feature, which is a unified display with detailed forensics. The feature provides actionable information and the ability to automatically open service requests with the Cisco Technical Assistance Center.

Reporting

Cisco Prime Infrastructure provides you a single launch point for all reports that you can configure, schedule, and view. The Report Launch Pad page provides access to over 100 reports, each of which you can customize as needed.

Map Scaling and Sizing for Location Services

Cisco PI is also one of the key components needed to enable Location Services. PI provides the following services:

- Provides the administrative interface for importing and tuning plant floor maps for location services.

- Integrates with the Cisco CMX to synchronize plant floor maps.

- Synchronizes CMX services with WLCs.

Multiple WLCs and CMX may be managed and monitored by Cisco PI.

Location Services

With integrated location tracking, Cisco Wireless LANs help enable the following location-based use-cases within a plant environment:

- Quickly and efficiently locating valuable assets and key personnel

- Improving productivity via effective asset and personnel allocation

- Reducing loss because of the unauthorized removal of assets from company premises

- Improving customer satisfaction by rapidly locating critical service-impacting assets

- Improving WLAN planning and tuning capabilities

- Coordinating Wi-Fi device location with security policy enforcement

This solution uses the Cisco Connected Mobile Experiences (CMX) product to provide location services. CMX uses existing wireless infrastructure to calculate the location of the Wi-Fi devices and interferers such as BLE Beacons, microwave ovens, and so on in the network. CMX uses RSSI triangulation from three nearby APs to located connected and unconnected Wi-Fi devices, interferers, and active RFID tags. With a properly deployed solution, the accuracy and precision of the Cisco Location Based Services solution is:

- Accuracy of less than or equal to 10 meters, with 90% precision

- Accuracy of less than or equal to 5 meters, with 50% precision

Figure 25   Wi-Fi Client Location with Cisco CMX

Figure 26   Wi-Fi Client Location within Prime

Figure 27   RFID Tags within Cisco Prime

Asset Tracking

Managing thousands of costly, mobile assets and equipment is challenging and labor-intensive. A significant portion of asset inventories are lost, stolen, or misplaced, impacting productivity every day.

Assets can be tracked throughout the refinery using RFID Tags, whether or not they are associated to the network. Depending on the tag system deployed, we can either track the location of an asset with a tag, or even provide two-way communication for emergency notifications.

A Cisco-only Real Time Location System (RTLS) will require the deployment of Cisco Prime Infrastructure and Cisco CMX alongside the WLC. These three components will work together to aggregate client data, triangulate a position, and highlight the location on a map.

Identifying an accurate location begins with an accurate map. Building or site floor plans must be uploaded to Prime Infrastructure and appropriate scaling parameters defined. It is critical that this step is properly completed to ensure accurate measurements. Multiple floors or areas can be defined.

The WLC must be added to Cisco Prime Infrastructure as a network device to be managed. Once fully discovered, Prime will be able to import the APs managed by the WLC. With the site maps defined, the APs can then be positioned on the map corresponding to their physical location. Client locations will be determined relative to the design of this map. To improve absolute location accuracy, GPS markers may be added to the map.

Finally, the CMX must be added to Prime Infrastructure and the maps must be synchronized.

Active Tags

Radio Frequency Identification (RFID) is already a common method for tracking assets within a confined environment, but requires additional hardware to be deployed for comprehensive location information. Active RFID tags contain a battery that directly powers RF communication, allowing the tag to transmit information about itself, either by constantly beaconing this information to a tag reader or by transmitting prompted to do so by an exciter. Active tags are typically used in real-time tracking of high-value assets in closed-loop systems (that is, systems in which the tags are not intended to physically leave the control premises of the tag owner or originator).

Wi-Fi Active RFID tags are another variation, designed to operate in the same bands as 802.11 wireless networks. These tags exhibit the characteristics of active RFID tags, but also comply with applicable IEEE 802.11 standards and protocols. Wi-Fi RFID tags can use the existing Cisco wireless infrastructure without additional hardware.

Multiple vendors manufacture Wi-Fi Active RFID tags for asset tracking. These tags are battery operated and send out beacons at consistent intervals so that location currency is always known and maintained.

Tags can typically operate in two modes. The first is a one-way communication mode, whereby the tag does not need to associate and simply sends beacons that are heard by an AP. The second mode is an associated mode, whereby the tag is associated to a WLAN and both sends and receives data from a RTLS server. This data can be for maintenance purposes such as firmware upgrades or for various emergency notifications.

Some RFID tag vendors use Cisco Compatible Extensions (CCX) on the WLAN to transmit additional information that can be used to track an asset or perform maintenance without association. An example is an Extronics or Ekahua tag with a panic button. For these sort of tags, the location data is extrapolated using the beacons and the PANIC BUTTON data is sent over CCX.

When using a dedicated system for asset tracking with Active RFID tags, a vendor-specific RTLS server may also need to be deployed in the control room. Depending on the vendor, the tags themselves may also need to be programmed before initial use using a tag activator. It is also important to note the frequency at which the tags will operate, with most active tags transmitting beacons at 2.4 GHz.

RSSI Probe Mode

The most basic method to determine the location of a wireless client is to collect and analyze the Received Signal Strength Information (RSSI) from 802.11 probe request frames. This method may also sometimes be referred to as Beacon Mode or Blink Mode. Probe requests are sent when the wireless client actively scans for APs with which to join. Probes are typically sent on multiple channels in order to allow the client to determine the best AP to join with. This makes the probes visible by all APs (operating on different channels) within range of the client.

The RSSI data from the probes is then forwarded from all APs to the wireless LAN controller. The WLC, in turn, forwards the aggregate RSSI data to CMX. CMX then analyses all of the received RSSI data per client and, in conjunction with the knowledge of physical AP placement data defined in Cisco Prime, CMX can triangulate the location of the client. The calculation is based on proximity; the closer the transmitter is to the receiver, the higher the RSSI value will be. It is thus important to have sufficient wireless coverage to allow for at least three APs to be capable of hearing probe requests from any client to effectively triangulate the location.

Associated Mode

In associated mode, tags are configured to associate and authenticate to the WLAN for each location and maintenance update. In this mode, tags send probe requests to APs on their SSID and measure AP responses to obtain RSSI. Tags then associate/authenticate to the network to send this data to the server. In this mode, tags are capable of two-way communication and require an IP address for communication. In this mode the tags will need a path to reach the RTLS server in the control room and a DHCP server.

In an associated mode, the RTLS server can acknowledge the tag messages and if an acknowledgment is not received, the tag can retry transmission to ensure that its location is always updated. The largest downside of an associated mode is decreased battery life.

Improving Accuracy

To improve accuracy where AP coverage may not be ideal due to environmental or cost constraints or where a much higher degree of accuracy is required, beacons or choke points exciters may be deployed. These small devices are designed to activate any nearby wireless tag using a short range communication method such as infra-red, Bluetooth Low Energy (BLE), or RFID. Once activated, the tag can send to the location appliance information about the beacon it just saw.

Choke points are tightly defined physical areas (such as entrances, exits or other types of constrictions) that provide passage between connected regions. Like an AP, these activators/beacons are placed on a map and due to their typical small range of operation, a very accurate location can be determined for that tag.

These methods should only be used to augment the broader asset tracking system.

Security

In an associated mode, depending on the vendor used for the tags, some encryption options may not be available for securing the WLAN. However, WEP and WPA2 (AES) are typically supported options.

One of the benefits of associated mode is that tags can tags can be upgraded or send additional information. In associated mode we can have 2-way communication to and from the tags. This traffic will require additional scrutiny as it traverses the network. A dedicated VLAN can be used for tag traffic within the Control Room on egress from the WLC. Traffic between the RTLS server and the Control Room network should pass through an ASA firewall or the IDMZ with the appropriate ports opened.

For example, the following ports are required for proper Ekahau tag communication:

- Location Update Port-8552 TCP/UDP

- Maintenance Update Port-8553 TCP/UDP

- Firmware Update-8554 or 8562 TCP/UDP (device dependent)

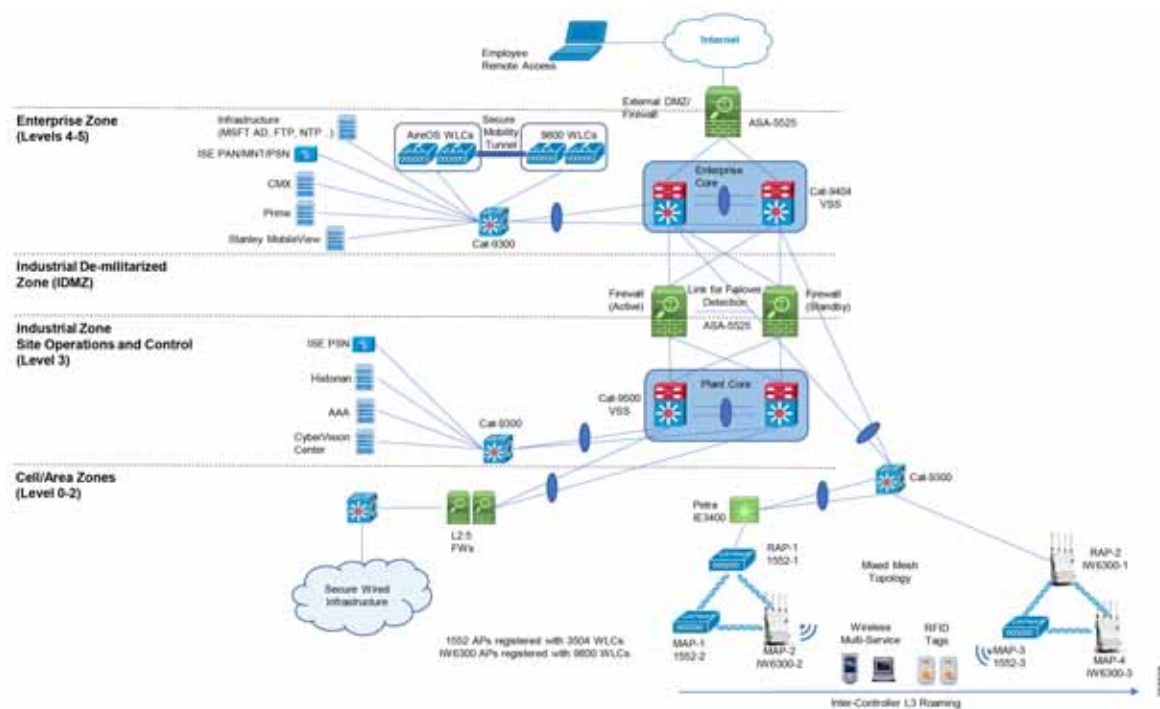- Temperature Sensors-8557 TCP/IP

Brownfield Deployment Architecture

Cisco Catalyst IW6300 Heavy Duty Access Point is purpose-built wireless access points for hazardous locations with Class I Division 2 (Zone 2) certification. It is the successor to the 1552H, 1552S, and 1552WU access points. This section specifically covers the migration and co-existence use cases of the Cisco Catalyst IW6300 Heavy Duty Series Access Point and the 1552 APs.

It covers the following scenarios:

- Customers with existing 1552H access points in their networks and adding additional IW-6300H access points

- Customers with existing 1552H access points in their networks and replacing some 1552H access points with IW-6300H access points

Figure 28   Brownfield Wireless Deployment

In case of Brownfield deployments, Cisco AireOS Wireless Controllers along with Cisco 1552 Access Points are already deployed within the environment. In this scenario, it is recommended to deploy the newer Cisco 9800 IOS-XE based Wireless Controller along with the newly released Cisco Industrial IW6300 Heavy-duty Access Points in the newer area to expand the wireless coverage. Integration between the existing wireless deployment and the new deployment can be achieved by creating a Mixed Mesh topology as depicted in the figure above.

When both the pairs of WLCs map the same Client VLAN/subnet for a particular WLAN SSID, L2 roaming occurs. In this scenario, when a wireless client roams from the first pair of WLCs to the second pair of WLCs, the client traffic goes to the newly roamed to WLC which offloads it onto the wired network. The traffic doesn't need to traverse the mobility tunnel to go the original WLC.

When both the pairs of WLCs map different Client VLANs/subnets for a particular WLAN SSID, L3 roaming occurs. In this scenario, when a wireless client roams from the first pair of WLCs to the second pair of WLCs, the client maintains the same IP address even after it roams, however this time around the client traffic goes to the newly roamed to WLC, is sent over the mobility tunnel to its original WLC which then offloads the traffic onto the wired network in the appropriate VLAN.

An important point to note here is that when establishing a mixed mesh using a pair of AireOS WLCs and a pair of Cat-9800 WLCs, only L3 roaming is supported. This means that the client traffic always traverses the Secure Mobility Tunnel to the original roamed from WLC which then offloads the traffic onto the wired network.

In this deployment model, even though we utilize two different pairs of WLCs we only need a single instance of both the Cisco Prime Infrastructure and CMX for network management and location/asset tracking. Cisco Prime Infrastructure and CMX gather information from both the pairs of WLCs and provide a consolidated view of the mixed mesh topology and location information for wireless clients and RFID tags.

Brownfield Deployment Supported Versions

Cisco 1552H Access Point (1552H) is supported on AireOS Wireless LAN Controllers Release 8.5 and AireOS Release 8.3 (for 1552H access points with 64-MB memory). Cisco Catalyst IW6300 Heavy Duty Series Access Point (IW-6300H) is supported on AireOS Release 8.10 or IOS-XE Release 17.1.1s. The co-existence of 1552H and IW-6300H access points requires two Wireless LAN Controllers (WLCs) to manage 1552H and IW-6300H respectively.

These are the considerations that need to be taken into account before beginning the migrations:

- Seamless mobility

- Mesh interoperability

- Access point replacement and site survey

Table 6   Industrial Wireless Mesh Components - Brownfield Expansion/Migration Deployment

Cisco Products	Version	Role
Cisco Catalyst 9800 Wireless Controller	IOS-XE 17.1.1s	Wireless LAN Controller for Greenfield and Brownfield Expansion/Migration scenarios.
Cisco AireOS 35XX, 55XX Wireless Controller	AireOS 8.5MR4 (8.5.141.107)	Wireless LAN Controller used in existing brownfield deployment.
Cisco AireOS 35XX, 55XX Wireless Controller	AireOS 8.10.105	Wireless LAN Controller for Brownfield Expansion/Migration scenarios.
Cisco 1552 AP	AireOS 8.5MR4 (8.5.141.107)	Outdoors Ruggedized AP deployed within existing brownfield deployments.
Cisco IW6300 AP	IOS-XE 17.1.1s or AireOS 8.10.105	Newly introduced ruggedized AP for outdoor environments. Can be used both for greenfield and brownfield expansion/migration/replacement.
Cisco Prime Infrastructure	3.7	Wired and Wireless Network Management
Cisco CMX	10.6.2	Location Services, Asset Tracking
Cisco Identity Services Engine (ISE)	2.6	Identity Store, IEEE 802.1X authentication, Network Policy Server
Cisco Catalyst 9300	IOS-XE 17.1.1s	PoE enabled access layer switch
Cisco IE 3400	IOS-XE 17.1.1	Ruggedized PoE-enabled access layer switch

Brownfield Expansion Caveats and Considerations

- There is no single version of WLC image that supports both the 1552 AP and the IW6300 AP. Hence we need to deploy a pair of controllers to support the existing 1552 APs existing within a brownfield deployment and the newer IW6300 APs being deployed to expand wireless coverage within a plant.

  - IW6300 AP is not supported on the AireOS 8.5MR4 release.

- – IW6300 AP is supported on AireOS 8.10.105 and beyond.

  – IW6300 AP is supported on Catalyst 9800 WLCs with IOS-XE 17.1.1s and beyond.

  – 1552 AP is supported only until AireOS 8.5 MR4.

  – 1552 AP is not supported on AireOS 8.10.105 and beyond.

  – 1552 AP is not supported on Catalyst 9800 WLCs.

- For the brownfield expansion scenario two different sets of controllers with different image versions are used and an Inter-Release Controller Mobility (IRCM) AireOS image on the existing AireOS based WLC. The supported deployment models are as follows:

  – AireOS 8.5MR4 IRCM to AireOS 8.10.105

  – AireOS 8.3 IRCM to AireOS 8.10

  – AireOS 8.5MR4 IRCM to Catalyst IOS-XE 17.1.1s

  – IRCM between AireOS 8.3 and IOS-XE 17.1.1 is not supported

Inter-Release Controller Mobility (IRCM)

Inter-Release Controller Mobility (IRCM) is a set of features and functionality that enable interworking between controllers running different software releases. IRCM enables seamless mobility and wireless services across controllers running Cisco AireOS and Cisco IOS (for example, Cisco 5520 WLC to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access or termination.

The Inter-Release Controller Mobility (IRCM) feature is supported by the following Cisco Wireless Controllers.

- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.

- Supported Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software. The following controllers are supported:

  – Cisco 3504 Wireless Controllers

  – Cisco 5508 Wireless Controllers

  – Cisco 5520 Wireless Controllers

  – Cisco 8510 Wireless Controllers

  – Cisco 8540 Wireless Controllers

Note: Contact the Cisco Technical Assistance Center (TAC) or send an email to wnbu-escalation@cisco.com to receive the Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software.

IRCM Overview

Cisco Catalyst 9800 wireless controller uses CAPWAP based tunnels for mobility. The mobility control channel is encrypted and the mobility data channel can be optionally encrypted. This is termed as Secure Mobility.

AireOS uses EoIP tunnels for mobility. Support for CAPWAP based encrypted mobility (Secure Mobility) was brought in. However the support for IRCM with Catalyst 9800 is present only in 8.8MR1 and above.
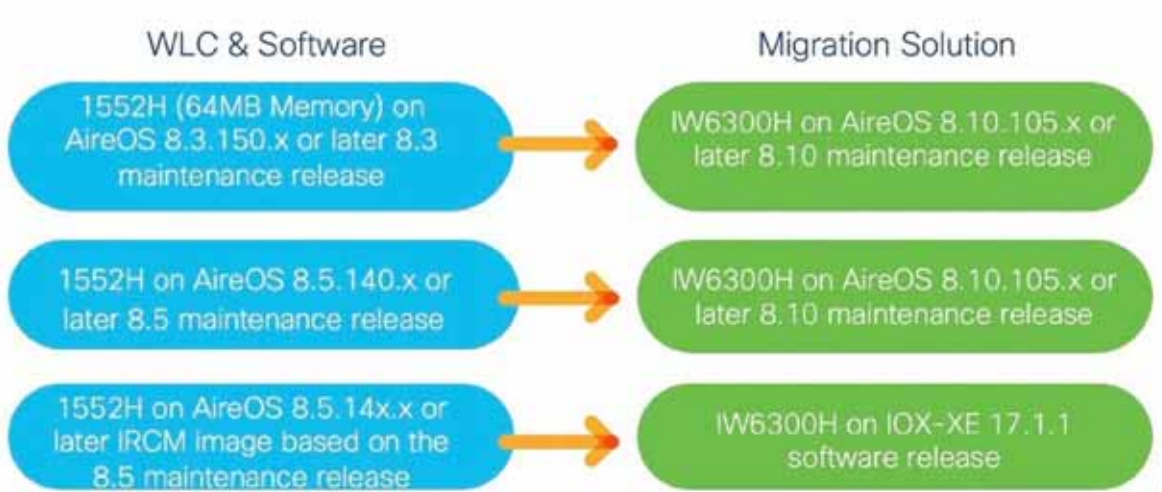
Notes:

- Ensure use of the AireOS controller that supports Encrypted Mobility feature.

- AVC is not supported for IRCM.

- In mixed deployments, the WLAN profile name and the policy profile name need to be the same.

■ In mixed deployments, ensure that AireOS controllers are upgraded to Release 8.5 MR4 or a later release to work with the Cisco Catalyst 9800 Series Wireless Controller.

■ Mobility group multicast is not supported because AireOS does not support mobility multicast in encrypted mobility.

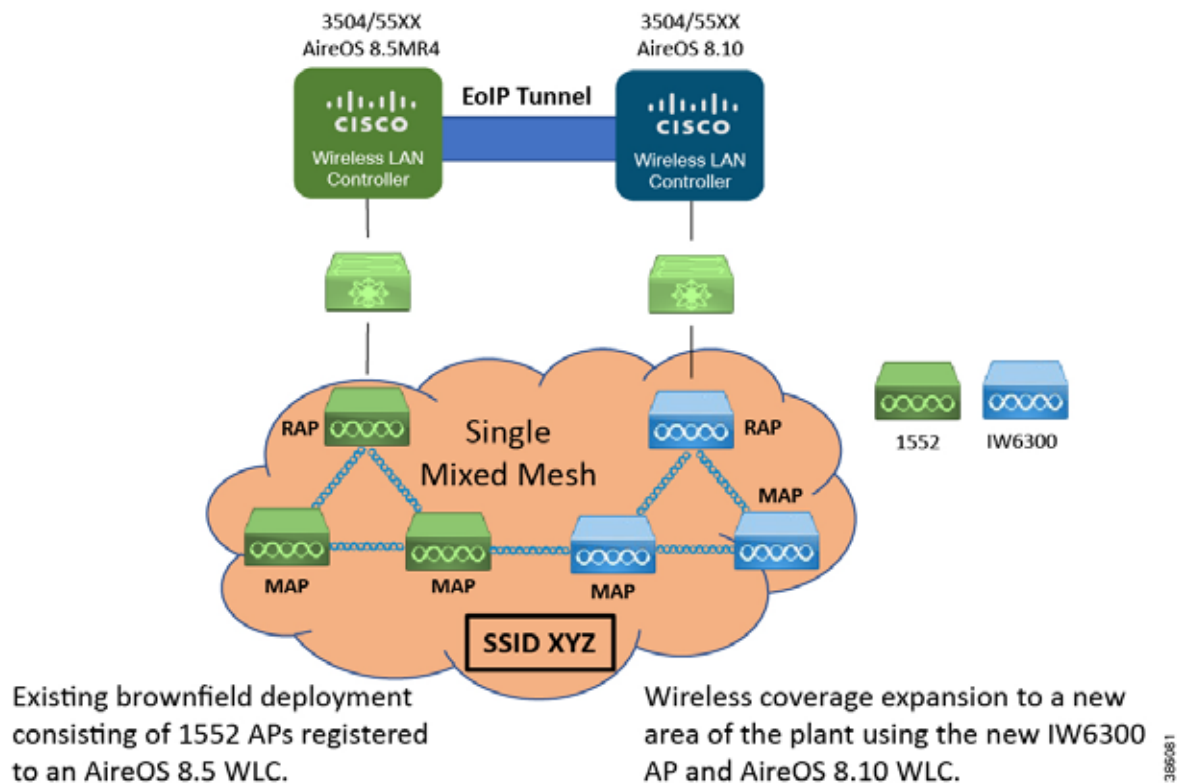The IRCM deployments and use cases in this document are based on the following prerequisites:

Figure 29   Migration Solution Matrix

Brownfield Expansion

This scenario covers the use-case in which an existing deployment of Cisco 1552 APs registered to AireOS based WLCs needs to be expanded to provide coverage to a newer area of the plant. In this case it is recommended to deploy the newer Cisco Industrial IW6300 APs registered to either an AireOS 8.10 based WLC or the next-gen Cat9800 IOS-XE 17.1 based WLC.

This mixed mesh deployment model supports both expansion of coverage within a new area of the plant as well as replacement of existing or bad 1552 APs with newer IW6300 APs. The long-term goal of this deployment model would be to eventually replace the older 1552 APs with the newer IW6300 APs over time. Until that time when all of your 1552 APs have been migrated to IW6300 APs this mixed mesh deployment using different pairs of controllers help preserve your existing investment in Cisco AireOS WLCs and 1552 APs while helping you to expand wireless coverage in a newer area of the plant using the latest and greatest Cisco 9800 WLCs and IW6300 APs as shown in the figures below.
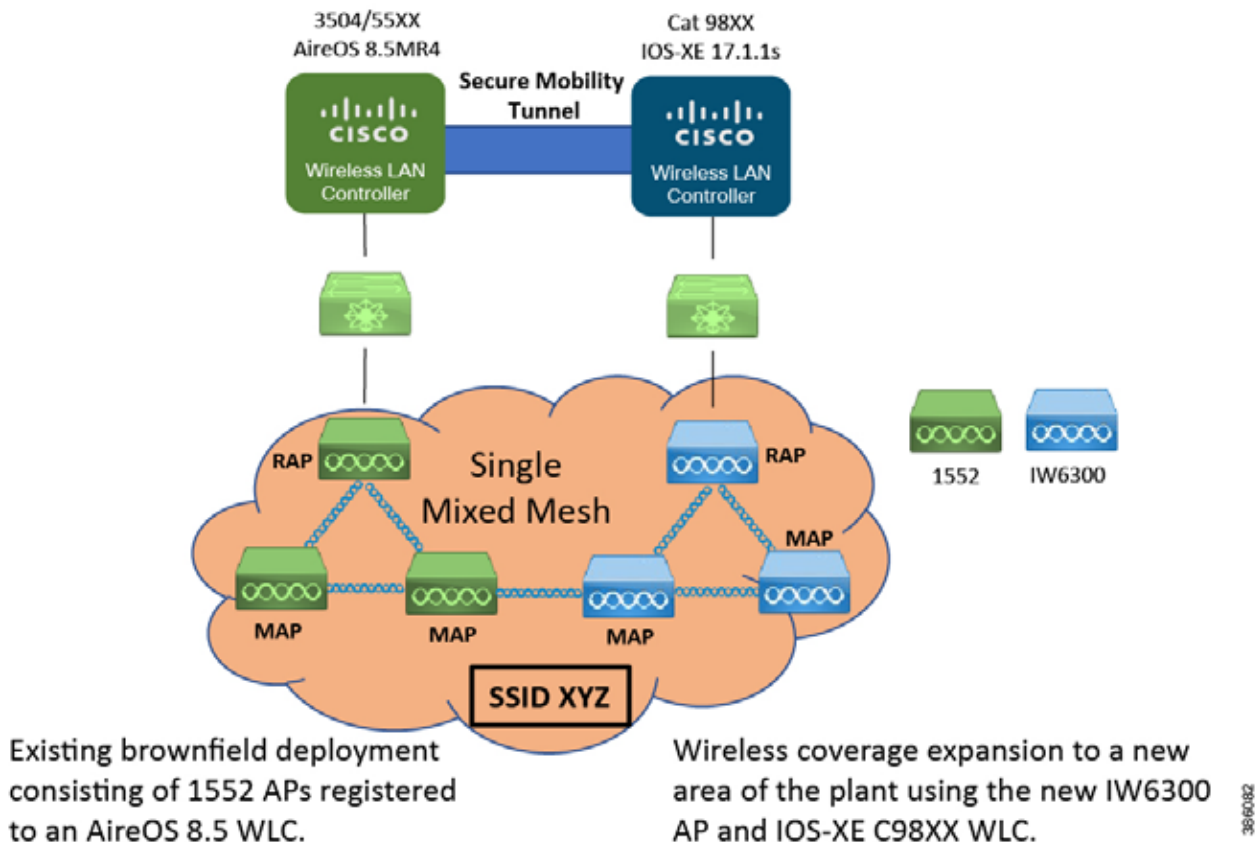
Figure 30   Expansion Scenario 1 - AireOS 8.5 and AireOS 8.10

For expansion scenario-1, the existing 1552H network first needs to be upgraded to AireOS 8.5 (Release 8.5.140.x or later) or AireOS 8.3 (Release 8.3.150.x or later) if APs have only 64MB memory.

- AP1552H joins AireOS 8.5/8.3WLC, IW6300H joins AireOS 8.10 WLC

- Both the WLANs, the original one on the AireOS WLC and the one newly configured on the AireOS 8.10 controller broadcast the same SSID to form a single mixed mesh network to provide seamless client mobility

- AireOS 8.5/8.3WLC pairs up with AireOS 8.10 WLC using EoIP between the two

- Layer 2 and Layer 3 seamless client roaming between AireOS 8.5/8.3 WLC and AireOS 8.10 WLC is permitted

- AP1552H and IW-6300H can be in bridge mode or local mode

- An important point to note is that both the 1552s and the IW6300 APs are part of the same single mesh network

In expansion scenario-1 depicted above, the IW6300 APs are deployed and registered to an AireOS 8.10 WLC. Next an EoIP tunnel is established between the existing AireOS 8.3/8.5 WLC and the newly deployed AireOS 8.10 WLC to enable seamless mobility between the existing deployment and the new deployment to provide expanded wireless coverage to a newer area of the plant. The new deployment advertises the same SSID as the existing deployment.The existing and the new deployment form a single mesh network which enables seamless roaming.

Figure 31   Expansion Scenario 2 - AireOS 8.5 and IOS-XE 17.1.1s

For expansion scenario-2, existing 1552H network needs to be upgraded to AireOS 8.5 special IRCM image first (requested via wnbu-escalation@cisco.com).

■   AP1552H joins Aire OS8.5 IRCM special WLC, IW6300H joins IOS-XE 17.1.1s WLC

■   Two networks broadcast the same SSID to form a single mixed mesh network.

■   8.5 IRCM special WLC pairs up with IOS-XE 17.1.1s WLC using secure mobility

■   Only layer 3 seamless client roaming between 8.5 IRCM special WLC and IOS-XE 17.1.1s WLC is permitted. Layer 3 roaming (inter-subnet roaming) requires that the WLAN interfaces of the two WLCs are on different IP subnets.

■   AP1552H and IW-6300H can be bridge mode or local mode.

In expansion scenario-2 depicted above, the IW6300 APs are deployed and registered to an IOS-XE 17.1.1s 98XX WLC. Next a Secure Mobility tunnel is established between the existing AireOS 8.3/8.5 WLC and the newly deployed 98XX WLC to enable seamless mobility between the existing deployment and the new deployment to provide expanded wireless coverage to a newer area of the plant. The new deployment advertises the same SSID as the existing deployment. Only L3 roaming is supported with this mixed mesh deployment mode.

In both the deployment models we can either have the same client VLAN configured on both the pair of controllers or we can have different client VLANs configured. In our testing for the CVD we had configured the same client VLAN and subnet within both the pair of WLCs.
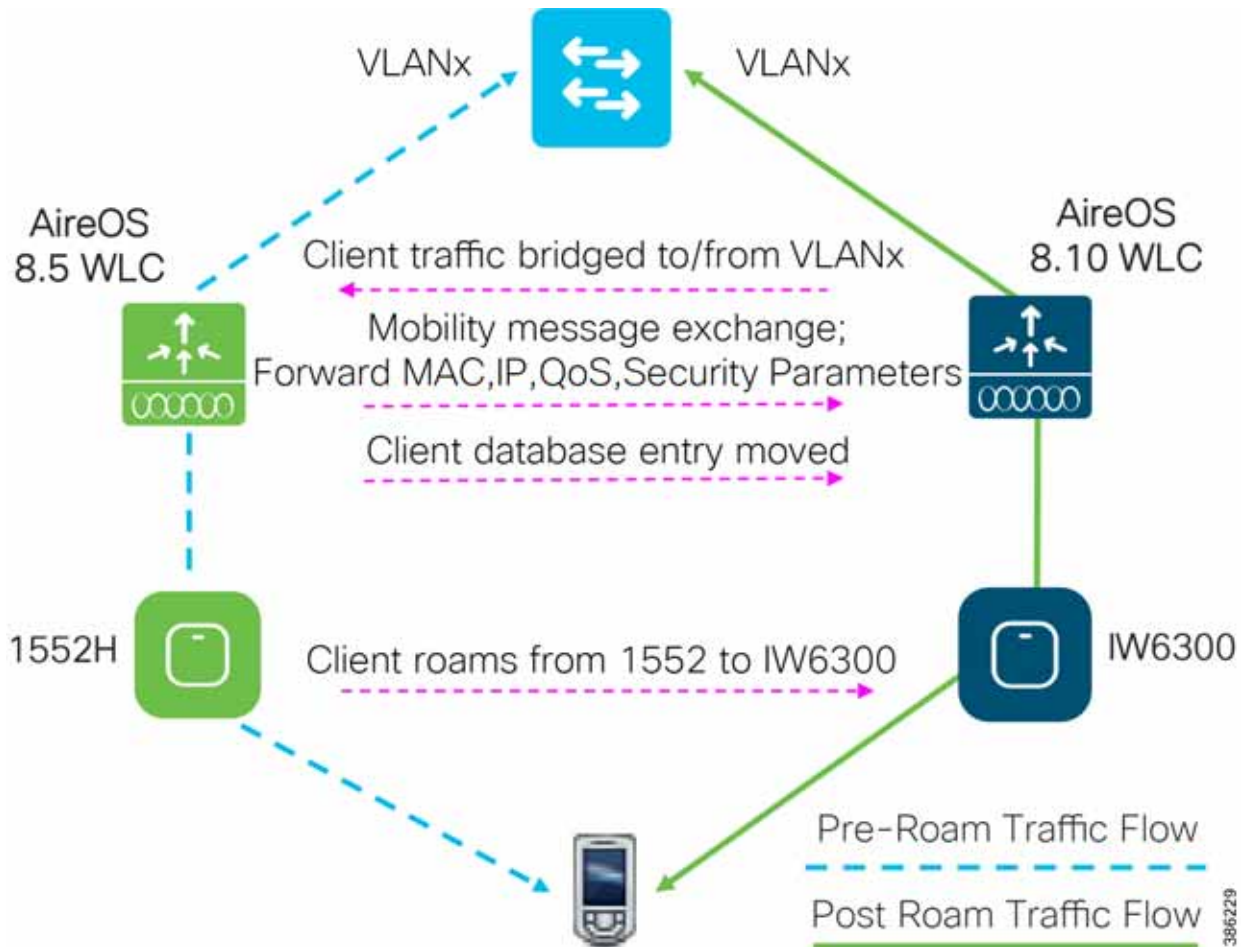
In case of Expansion Scenario-1 when a client roams from a 1552 AP to an IW6300 AP it results in a L2 roam. However in the case of Expansion Scenario-2 when a client roams from a 1552 AP to an IW6300 AP it results in a L3 roam.

Mesh Interoperability

AP1552H and IW-6300H mesh interoperability can be maintained between two Wireless Controllers, with the following support:

- AP1552H MAPs can join a release 8.5 controller through a mesh network formed by IW-6300H APs connected to a release 8.10 AireOS controller or 17.1.1s IOS-XE Wireless Controller.

- IW-6300H MAPs can join a release 8.10 AireOS controller or 17.1.1s IOS-XE Wireless Controller through a mesh network formed by AP1552H APs connected to a release 8.5 controller.
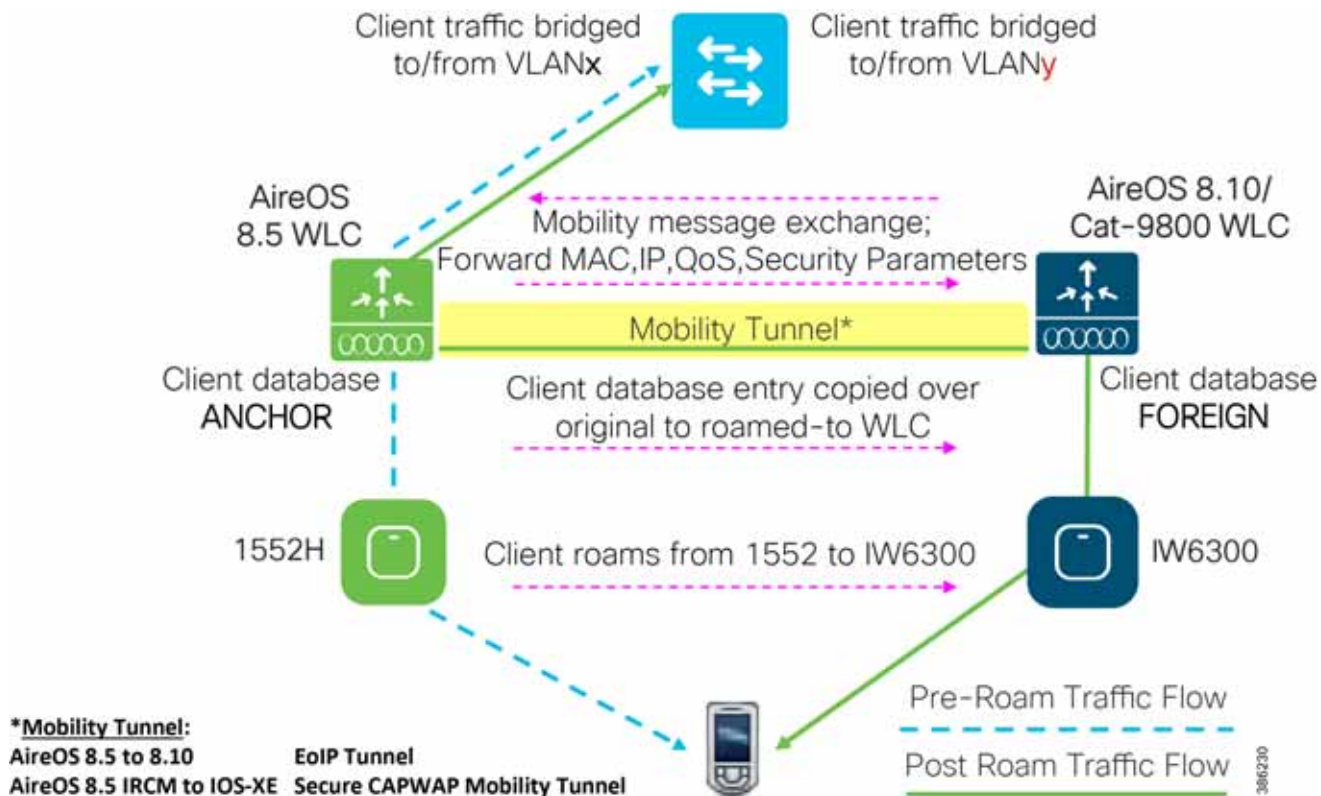
Figure 32   Inter-Controller L2 Roaming

When a client joins an access point associated with a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

Note: All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication in order to comply with the IEEE standard.

Inter-Subnet Roaming

Figure 33   Inter-Subnet L3 Roaming

When a client roams between controllers with the same SSID, but different interface subnets (L3 roam), the controllers still exchange mobility messages, but they handle the client database entry in a completely different manner. Instead of moving the client database entry to the new controller, the original controller retains its copy of the client entry in its database and marks it as an Export Anchor. The client database entry is copied to the new controller client database and marked as Export Foreign.

In terms of the client itself, the two controllers are now referred to as anchor and foreign, respectively. The client, however, has no knowledge of this and retains its original IP address from the anchor controller WLAN interface address space.

The client IP point of presence on the network remains the anchor WLC. Traffic flows to the client from the wired network through the Anchor controller and flows over either an EoIP tunnel (AireOS to AireOS WLCs) or over a secure mobility tunnel (AireOS to IOS-XE WLCs) to the foreign controller and then to the new AP to the client. In the reverse direction the foreign controller takes the traffic from the client and passes the traffic to the Anchor over the mobility tunnel where it then drops the traffic onto the original client subnet.

If the client roams back to the original controller, the anchor and foreign markings are removed and the client database entry is deleted from the Foreign controller. Should the client roam to a different foreign controller the original anchor controller is maintained, and the foreign client entry is transferred to the new Foreign controller.

Note: Only L3 roaming is supported between AireOS and IOS-XE based WLCs even if the client subnet between the two WLC platforms is the same. A controller running IRCM compatible AireOS release and a Catalyst 9800 wireless controller should not have the same client VLANs configured for seamless L3 roaming to happen.
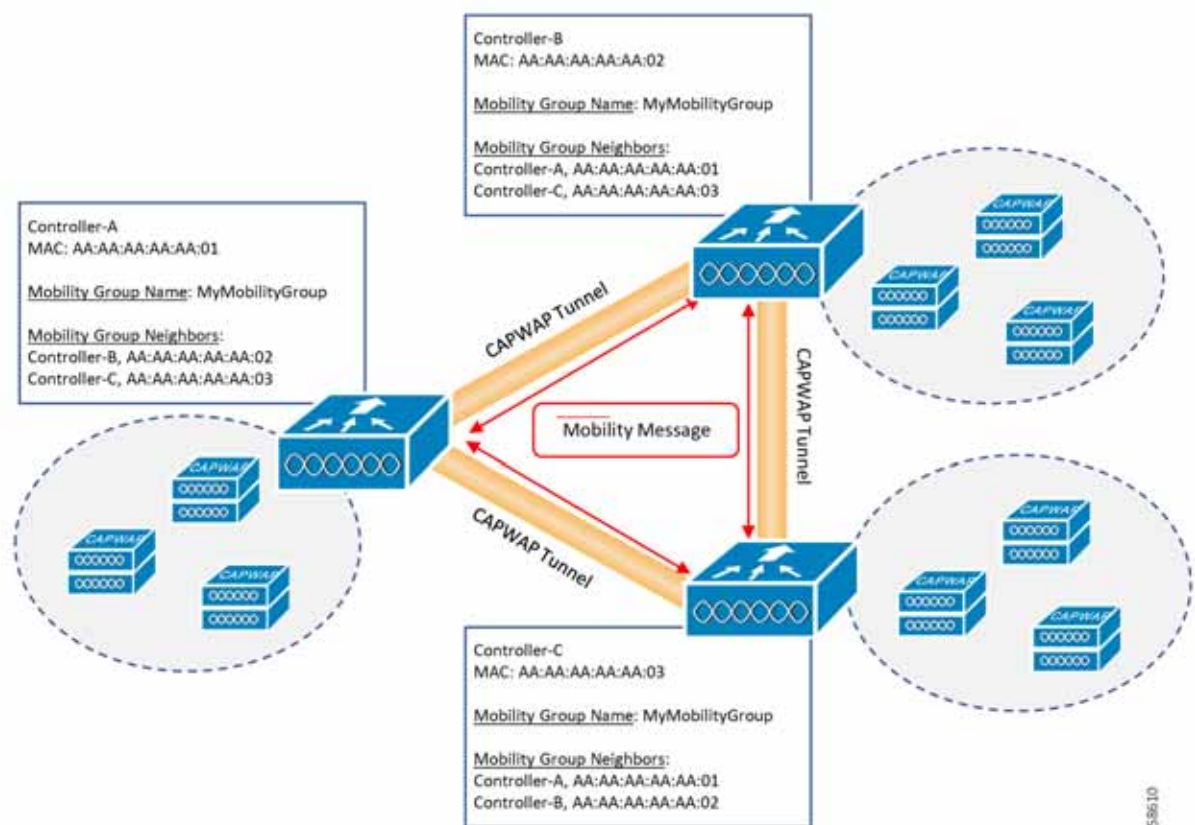
Note: The Cisco Catalyst 9800 Series Wireless Controller mobility tunnel is a CAPWAP tunnel with control path (UDP 16666) and data path (UDP 16667). The control path is DTLS encrypted by default. Data path DTLS can be enabled when you add the mobility peer.

Mobility Group

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. Enable multiple controllers to create a mobility group in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

As shown in the figure above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client.

Figure 34   Mobility Group

For our use-cases consisting of a mixed mesh deployment in brownfield scenarios, we need to create a mobility group between the existing AireOS 8.3/8.5 controller and the newer AireOS 8.10 or IOS-XE 9800 controller to enable seamless roaming. This enables exchange of client information between the two sets of controllers within the mixed mesh. The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers that are part of the same mobility group.

A controller sends a Mobile Announce message to members in the mobility list each time that a new client associates to it. The controller sends the message only to those members that are in the same group as the controller (the local group) and then includes all of the other members while sending retries.

You can configure the controller to use multicast to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled on all group members.

Notes:

■ Ensure that the data DTLS configuration on the Cisco Catalyst 9800 Series Wireless Controller and AireOS are the same, as configuration mismatch is not supported on the Cisco Catalyst 9800 Series Wireless Controller and it causes the mobility data path to go down.

■ In inter-controller roaming scenarios, WLAN and policy profile configuration must be identical on both the controllers.

■ Policy profile name and client VLAN under policy profile can be different across the controllers with the same WLAN profile mapped.

■ Data DTLS and SSC hash key must be same for mobility tunnels between members.

■ Controllers that are mobility peers must use the same DHCP server to have an updated client mobility move count on intra-VLAN.

■ Controllers that are mobility peers must use the same DHCP server to have an updated client mobility move count on intra-VLAN.

■ Mobility move count is updated under client detail only during inter-controller roaming. Intra-controller roaming can be verified under client stats and mobility history.

■ Only IPv4 tunnel is supported between Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS controller.

■ In an HA scenario, ensure that wireless mobility is explicitly configured using mac address, otherwise the mobility tunnel will go down after SSO.

Mixed Mesh Architecture and Data Flow

The diagram below depicts the architecture for a Mixed Mesh deployment where-in the 1552 APs are registered with an AireOS WLC and the IW6300 APs are registered with the Cat98XX IOS-XE WLC. A "Secure Mobility Tunnel" is configured between the AireOS WLC and the Cat 98XX WLC.

Below we have configured a unique Bridge Group Name (BGN) for each WLC. Both the BGNs advertise the same SSID. Using BGNs we can direct Mesh APs towards the appropriate RAP.

As can be seen in the figure below even though MAP-2 is an IW6300 it can have its parent AP be a 1552 AP however, its registered with the Cat 9800 WLC and hence its CAPWAP tunnel terminates at the Cat-9800. Similarly the CAPWAP tunnel for MAP-6 which is a 1552 AP terminates on the AireOS WLC.
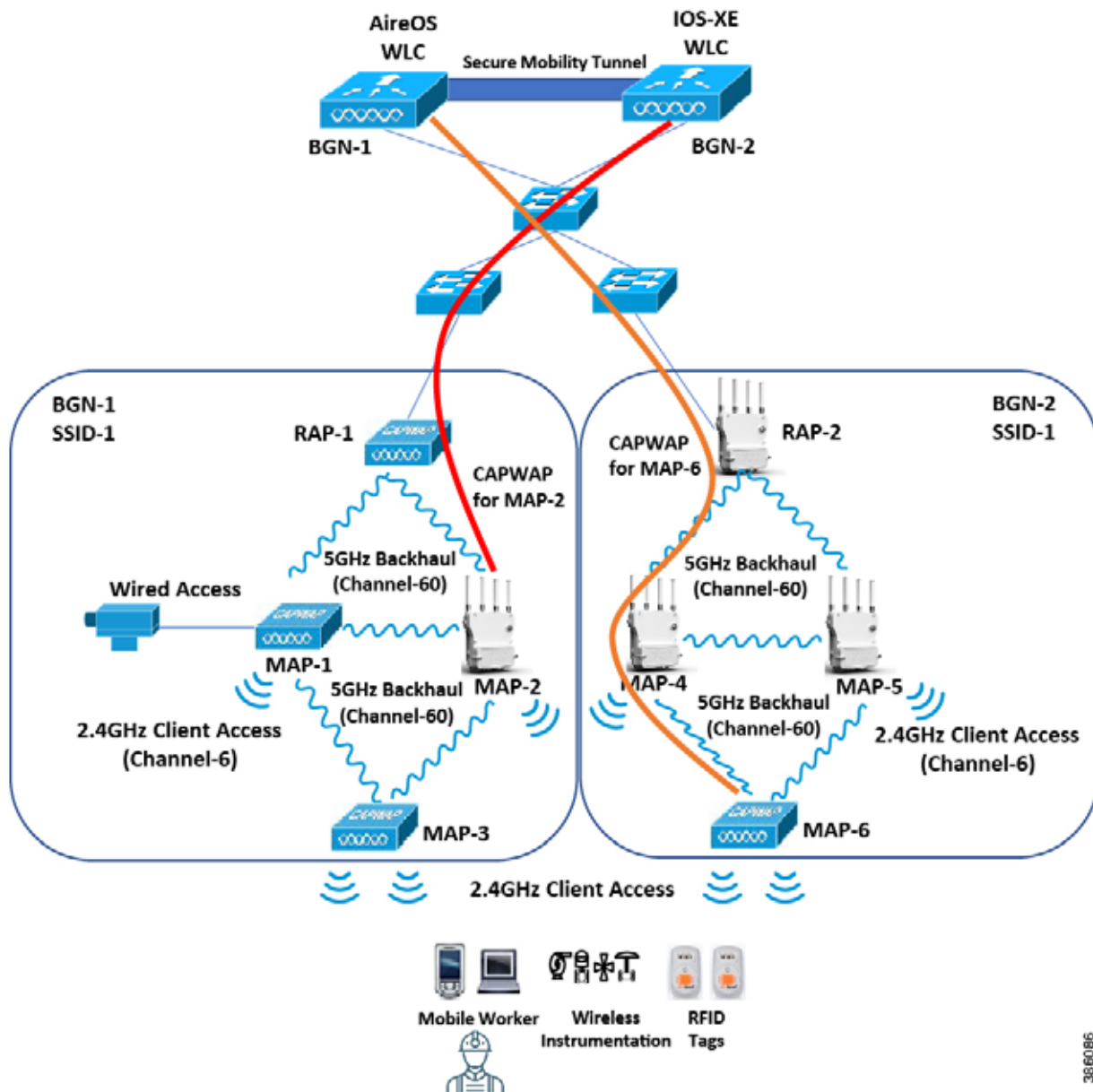
The same 5GHz backhaul channel is used for all the RAPs and MAPs in this deployment. The same 2.4GHz client Wi-Fi channel is used throughout the deployment. So, it is recommended to disable Dynamic Channel Assignment (DCA) and use Static Channel Assignment and manually assign a channel for the 2.4GHz Client Access and a channel for the 5GHz backhaul on all of the APs (RAPs and MAPs).

We recommend that the Client Access on the Backhaul 5GHz channel be disabled, and only the 2.4GHz channel is used for Client Access. For Mesh Convergence Mode select "VERYFAST", and enable "Background Scanning". The Mesh Background Scanning and Auto parent selection helps improve convergence times and parent selection reliability and

stability – a MAP should be able to find and connect with a better potential parent across any channel and maintain its uplink with a best parent all the time. We can also configure a preferred parent for the MAPs to help with faster mesh convergence.

A child MAP maintains its uplink with its parent using AWPP – Neighbor Discovery Request/Response (NDReq/NDResp) messages which are acting as keep-alives. If there are consecutive losses of NDResp messages, a parent is declared to be lost and the child MAP tries to find its new parent. A MAP maintains a list of neighbors of current **on-channel**, and on losing its current parent, it will try roaming to next best potential neighbor in the same serving channel. But if there are no other neighbors found in same channel, it has to do scan/seek across all/subset channels to find a parent.
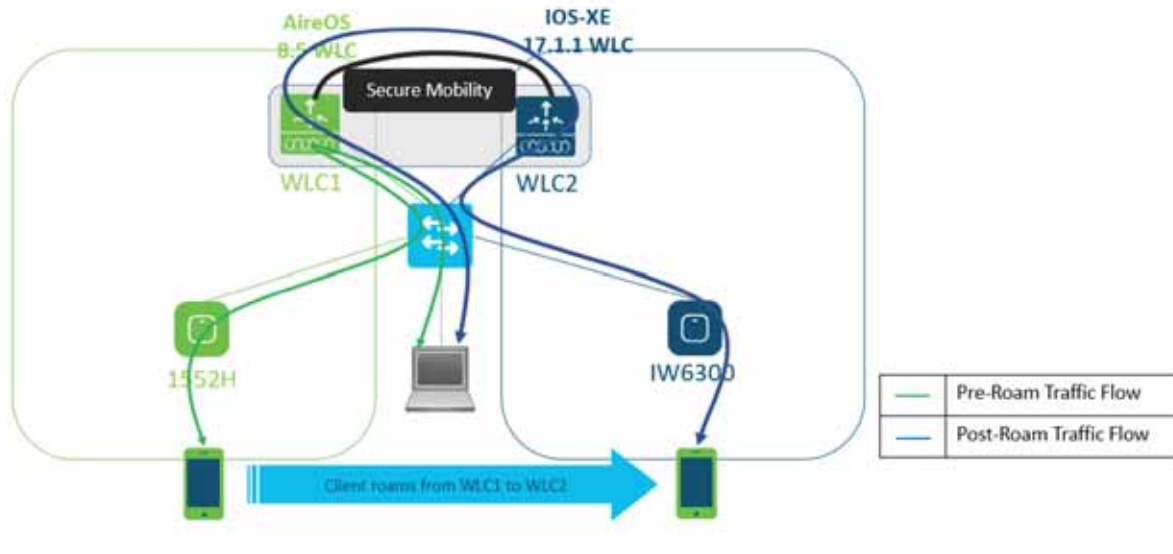
Figure 35   Mixed Mesh Architecture and Data Flow

Using this mixed mesh deployment architecture, the Cat 9800 IOS-XE based WLC and the IW6300 APs are used to expand wireless coverage to a new area of the plant while providing seamless mobility and roaming with the existing wireless deployment consisting of the AireOS WLC and 1552 APs.
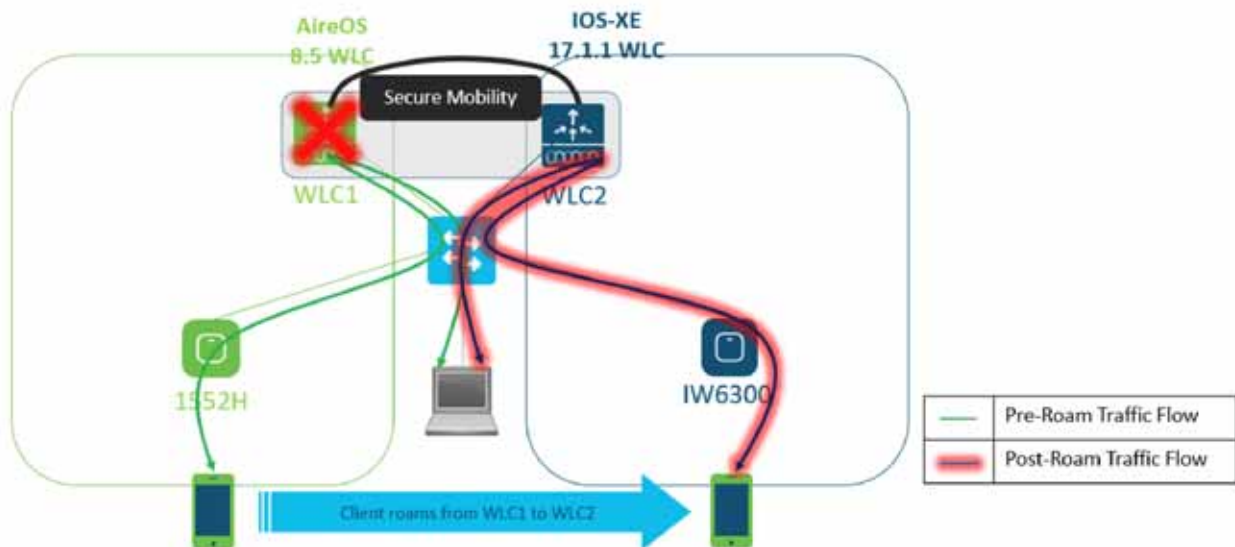
This deployment model also enables replacement of existing bad 1552s APs with IW6300 APs like that shown with MAP-2. In this case, the IW6300 MAP-2 joins the existing mesh, registers with the Cat98XX WLC and establishes a CAPWAP tunnel with it.

Figure 36   Client Traffic Flow within Mixed Mesh Environment

As far as client traffic is concerned, when the client is associated with a 1552 AP, the traffic goes over the CAPWAP tunnel to the AireOS WLC and is then offloaded to the wired network. Once the client roams to and is associated with an IW6300 AP, the client traffic traverses the CAPWAP tunnel to the Cat 9800 WLC, is then directed over the secure mobility tunnel to WLC1 and is then offloaded onto the wired network. The return traffic to the wireless client also follows the same path in that it has to traverse the secure mobility tunnel configured between WLC1 and WLC2 and then sent over to the IW6300 and eventually to the client.

Figure 37 Failure of Anchor Controller HA Pair

In the rare eventuality that the Anchor Controller pair (AireOS WLC HA pair) goes down, the roamed client will lose its original IP and get a new one from its roamed to Cat 9800 WLC. In this scenario, the client traffic is directly offloaded from the 9800 WLC onto the switch and is not forwarded across the secure mobility tunnel to the AireOS WLC since its down.

Replacing/Migrating an existing 1552 AP with an IW6300 AP

Before refreshing the existing AP1552H network, review the existing WLAN network and see whether you have future requirements for new applications. If you expect to achieve coverage at higher data rates, such as by taking advantage of 802.11ac 256-QAM rates or 80 MHz bandwidth, a new site survey is needed because the deployment must be denser to achieve higher rates over the same area, which means that APs likely need to be located in the places that are not previously surveyed.

■ The coverage provided by an IW6300 AP is similar to that of a 1552 AP. No new site-survey need be conducted when replacing a 1552 AP with an IW6300 AP.

■ The radiation patterns are similar and the level of pattern ripple are nearly the same between 1552 and IW-6300 when using chassis-mounted dual-band dipoles on APs mounted to a metal pole with the Cisco pole mount kits.

■ At 2.4 GHz the angles of the peaks and nulls do vary so there may be minor increases and decreases in link strength in some directions.

■ At 5 GHz the radiation patterns are virtually identical due to the shorter wavelength. Coverage will be the same.

■ Overall, there is no significant degradation expected when replacing a 1552 with an IW-6300 at the same location.
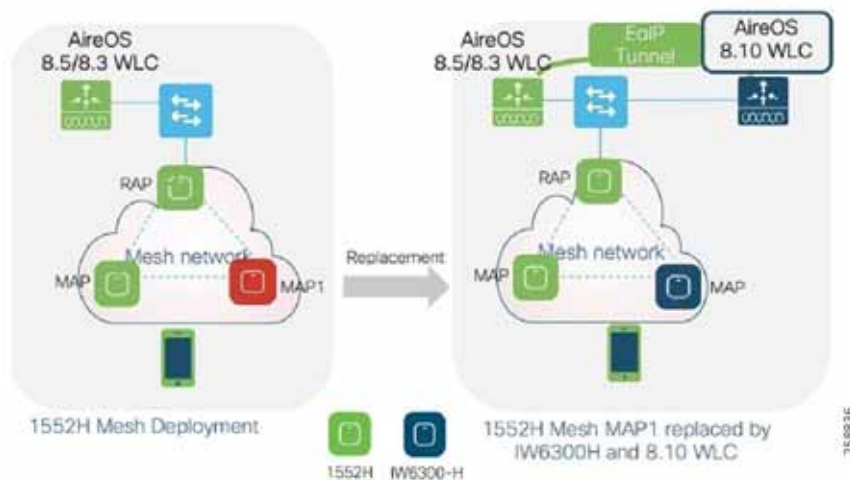
Table 7 1552 to IW6300 Replacement Installation Considerations

RF site survey	No new site survey required to achieve similar data-rate
Wi-Fi Antenna	Compatible

Power source	1552H <-> IW-6300H-AC
	1552SA <-> IW-6300H-AC
	1552SD <-> IW-6300H-DCW
	1552WU <-> IW-6300H-DCW
Power injector	Replace with AIR-PWRINJ-60RGD
Power cable	Compatible
Mounting	Replace with IW6300 mounting bracket, keep pole mount kit
SFP	Compatible
Power input port size	Compatible (1/2 NPT)
I/O ports	PG13.5 -> ½ NPT

Replacement Scenario 1 - Replacing 1552H AP With IW6300-H and New AireOS WLC
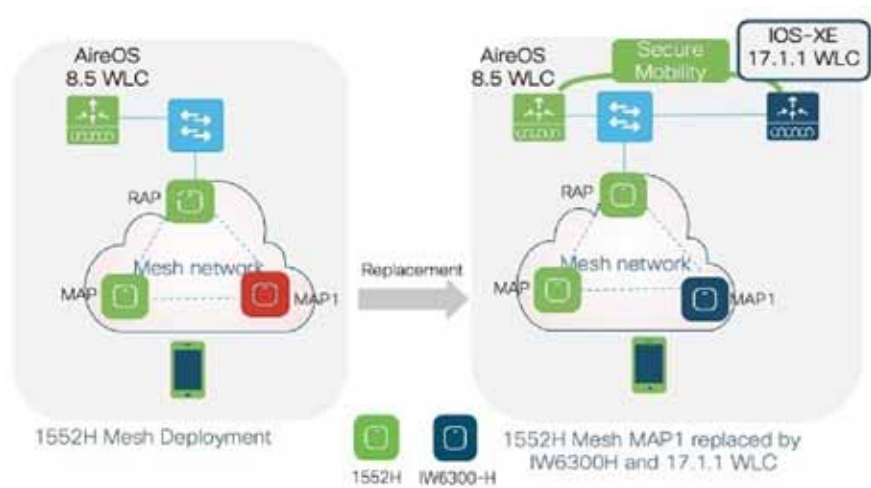
Figure 38 Mesh AP Replacement Scenario 1

In the above scenario, the existing 1552H network first needs to be upgraded to AireOS 8.5 (Release 8.5.140.x or later) or AireOS 8.3 (Release 8.3.150.x or later) if having only 64MB memory.

■ AP1552H Mesh AP or Root AP can be replaced by IW-6300H and new AireOS 8.10 WLC

■ MAC address of AP1552H and IW-6300H should be added to the MAC filter list on both controllers, or external AAA servers

Mesh related configuration on the two controllers should be exactly the same (for example, bridge group name, convergence mode, security mode, Ethernet bridging, etc.)

Note: The output of the `show mesh ap tree` command on each controller will not show the complete picture of the mesh network. Prime Infrastructure is recommended to manage the mixed mesh network.

Replacement Scenario 2 - Replacing 1552H AP with IW6300-H and New IOS-XE WLC

Figure 39   Mesh AP Replacement Scenario 2

Note: This scenario is not applicable for existing networks that still have 1552Hs with 64MB memory deployed.

In above scenario, existing 1552H network needs to be upgraded to AireOS 8.5 special IRCM image first (requested via wnbu-escalation@cisco.com).

■   AP1552H Mesh AP or Root AP can be replaced by IW-6300H and new IOS-XE 17.1.1s WLC

■   MAC address of AP1552H and IW-6300H should be added to the MAC filter list on both controllers, or external AAA servers

Mesh related configuration on the two controllers should be exactly the same (for example, bridge group name, convergence mode, security mode, Ethernet bridging, etc.)

Note: The output of the `show mesh ap tree` command on each controller will not show the entire picture of the mesh network. Prime Infrastructure is recommended to manage the mixed mesh network.

Emerson WiHART Deployment for Condition Monitoring

Emerson WiHART Gateways

Emerson™ Wireless 1410S Gateway

Emerson has partnered with Cisco to introduce a next-generation industrial wireless networking solution that fundamentally transforms data management to improve plant productivity, reliability and safety. The new Emerson Wireless 1410S Gateway with the Cisco Catalyst® IW6300 Heavy Duty Series Access Point combines the latest in wireless technology with advanced *Wireless*HART® sensor technology, delivering reliable and highly secure data, even in the harshest industrial environments.

The Emerson 1410S gateway provides a network capacity of up to 200+ *Wireless*HART devices (or) 200+ *Wireless*HART and 100 ISA100 devices.

Figure 40   Emerson™ Wireless 1410S Gateway

Note: Please refer to the Oil and Gas Refinery WLAN Mesh Implementation Guide for details on how to install and power-up the Emerson 1410S Wireless Gateway Module.

Figure 41   Emerson™ Wireless 1410H Gateway with Emerson Wireless 781 Field Link

The Emerson Wireless 1410H Gateway provides the option to create a flexible industrial wireless infrastructure using the *Wireless*HART™ technology. This Wireless Gateway can be used either redundantly or to add additional field devices. For redundancy, this Gateway provides two *Wireless*HART networks to switchover in case of power failure or lost connections. For increased capacity, this Gateway can accommodate up to 200 field devices.

The Emerson 781 Field Link antenna enables flexible remote antenna location of up to 200 meters (650 feet) for access into hazardous areas. The 1410H gateway connects *Wireless*HART self-organizing networks with host systems and data applications (200 device capacity).

Figure 42   Emerson™ Wireless 1410D Gateway with Emerson Wireless 781 Field Link

Designed to connect *Wireless*HART® networks with host systems and data applications, the Emerson™ Wireless 1410D Gateway with 781 Field Link allows users with limited safe locations to strengthen and add to wireless networks quickly and easily. The wireless gateway uses the 781 Field Link to enable flexible remote antenna locations of up to 650 feet (200 meters) allowing the gateway to be in the control room while placing the 781 Field Link into a hazardous area.

Emerson Rosemount (WiHART) Sensors

The Emerson Rosemount WiHART sensors use standard IEEE 802.15.4 radios. It uses the 2.4GHz band slided into 15 radio channels. Time-synchronized channel hopping is used to avoid interference from other radios, Wi-Fi, and EMC sources to increase reliability. Direct sequence spread spectrum (DSSS) technology delivers high reliability within a challenging radio environment.

The *Wireless*HART protocol provides a self-organizing network with adaptive mesh routing. The self-organizing,

self-healing network manages multiple communication paths for any given device. If an obstruction is introduced into the network, data will continue to flow because the device already has other established paths. The network will then lay in more communication paths as needed for that device.

Emerson Rosemount provides a wide array of WiHART sensors for applications ranging from pressure management, flow measurement, level measurement, temperature measurement, corrosion and erosion monitoring, gas analysis, liquid analysis, tank gauging, flame and gas detection. Below are listed a sample of the Rosemount WiHART sensors that were integrated within our test lab environment.

Figure 43   Rosemount™ 702 Wireless Discrete Transmitter

The Rosemount™ 702 Wireless Discrete Dual Input Transmitter is a cost-effective and installation-ready device that provides two inputs. With the security and reliability of *Wireless*HART® technology, this transmitter offers access to discrete points that are not connected to the control system due to wiring costs and lack of I/O. Commonly used as a repeater, this device also provides personnel access awareness and can be used for monitoring safety showers and eye wash stations.

Figure 44   Rosemount™ 708 Wireless Acoustic Transmitter

Featuring ultrasonic acoustic event detection that mounts externally, the Rosemount™ 708 Wireless Acoustic Transmitter offers a fast, cost effective installation. It provides visibility into steam traps and pressure relieve valves (PRVs) by accurately communicating acoustic level and temperature data as well as device data, event status and leak detection via the *Wireless*HART® network. The Steam Trap Monitor software (optional) provides real-time information about steam trap conditions, energy usage and emissions.

Figure 45   Rosemount™ 648 Wireless Temperature Transmitter with Rosemount™ 214C Sensor

The Rosemount 648 Wireless Temperature Transmitter offers best-in-class wireless accuracy and stability for process monitoring. This durable transmitter is designed with a dual-compartment housing for field reliability. When combined with Rosemount X-well™ Technology and the Rosemount 0085 Pipe Clamp sensor, this transmitter can provide accurate measurement of process temperature via an in-transmitter thermal conductivity algorithm, eliminating the need for a thermowell or process penetration.

The Rosemount 214C sensors are designed to provide flexible and reliable temperature measurements in process monitoring and control environments. Temperature ranges of -321 to 1112 °F (-196 to 600 °C) for RTDs and -321 to 2192 °F (-196 to 1200 °C) for thermocouples.

Figure 46   Rosemount™ Wireless Pressure Gauge

The Rosemount Wireless Pressure Gauge features a robust design with industry-proven sensor technology to resist common traditional gauge failures. The Wireless Pressure Gauge delivers data remotely via a *Wireless*HART® network. This sensor provides overpressure ratings from 1.5x to 150x and enhances safety by keeping the process contained with two layers of process isolation.

Rosemount™ 3051S Series Pressure Transmitter and Rosemount 3051SF Series Flow Meter

Rosemount 3051S Coplanar Pressure Transmitters are the industry leader for Differential, Gage, and Absolute pressure measurement. The coplanar platform allows seamless integration with manifolds, primary elements, and seal solutions.

Emerson PlantWeb Insight
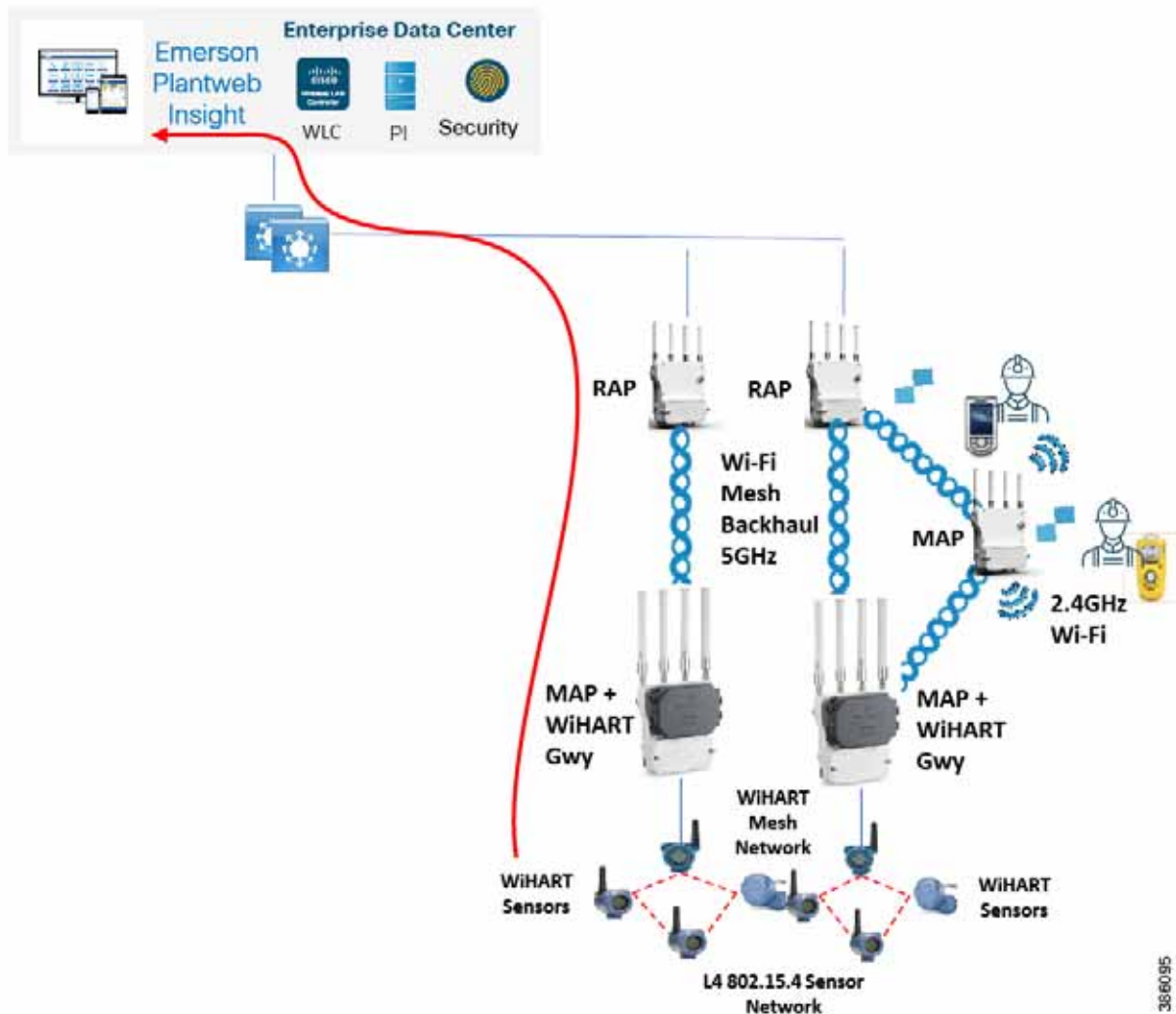
Figure 47   Emerson PlantWeb Insight

Emerson PlantWeb Insight is a data analytics platform that provides better visibility into the health of the facility key assets. It is a visualization and analytics software platform providing strategic interpretation and monitoring of plant assets. It provides relevant-time actionable information and insights about abnormal situations, asset status, asset health, energy costs, emissions loss, etc. It contains applications that are based on key assets such as steam traps, pumps, heat exchangers, pressure relief valves etc. It is easily deployed within a virtual machine. The web-based platform allows secure access to the data from anywhere at any time.

Wi-HART Data flow over Wi-FI

In the figure below, the Wi-HART sensor traffic arrives at the Emerson Wi-HART gateway which is directly wire-connected to either a RAP or a MAP Ethernet port. This traffic is then carried over the wireless mesh backhaul and dropped off at the RAM Ethernet switch port. It then traverses the network to reach its intended destination which is the Emerson Plantweb Insight software in this case.

Figure 48   WiHART Data-flow over Wi-Fi

Installing and Connecting Wireless Instrumentation

The Emerson IoT module (1410S) or the Emerson IoT gateways (1410D, 1410H) plug into the Cisco IW6300 AP Ethernet port and utilize the Ethernet bridging functionality within the AP.

Once the gateway is installed and has an IP, we can access the web portal embedded within the Smart Wireless Gateway to configure the Network ID and the common Join Key for the sensors.

Configure the Network ID and the Join Key on the sensor side. After that, and sufficient time for network polling has passed, the sensor registered with the gateway associated with that particular Network ID and joins the mesh network. To verify device operation and connectivity use the Smart Wireless Gateway's web based user interface and navigate to the Devices page.

Security Considerations

*Wireless*HART employs robust security measures to protect the network and secure data at all times:

- Uses a robust, multi-tiered and always-on security model

- Industry standard 128-bit AES encryption is used to secure the data

- Unique encryption key is used for each message

- Provides data integrity and device authentication

- Provides ability to rotate encryption keys used to join the network - automatic or on demand

WiHART Data Link Layer Security

- Channel hopping for security protection and co-existence

- Multiple levels of security keys for access

- Indication of failed access attempts, perhaps by a rogue device

- Reports message integrity and authentication failures

- Safe from Wi-Fi type internet attacks

Data Security

Security features associated with privacy aim to prevent eavesdropping by unauthorized devices inside or outside the network. A *Wireless*HART sensor network provides end-to-end CCM mode 128-bit AES encryption at the network/transport layer for every message in the network. In addition to individual session keys, a common network key is shared among all devices on a network to facilitate broadcast activity as needed. Encryption keys can be rotated as dictated by plant security policy to provide an even higher level of protection. A separate 128-bit join encryption key is used to keep data private that is sent and received during the joining process.

- The join key serves as authentication to the Security Manager that the device belongs to this network.

- The join key is treated separately from the other keys to enhance Security.

- Join keys can either be unique to each device, or be common to a given *Wireless*HART network based on the plant security policies.

- Join keys can be changed after the device joins the network to further increase security.

Data Security features associated with integrity ensures that data sent over the wireless sensor network has not been tampered with or falsified.
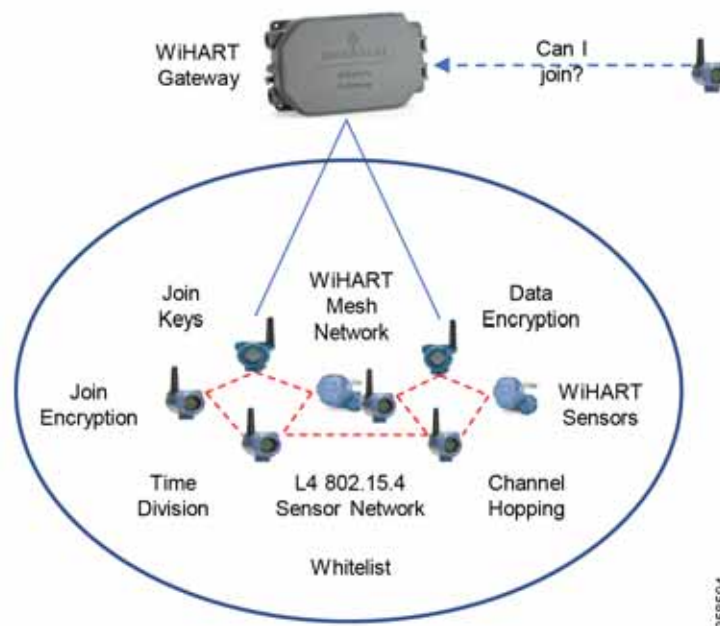
- *Wireless*HART uses two Message Integrity Check (MIC) Fields that are added to each packet.

- At the session layer, the receiving device uses the session MIC along with the protected data to confirm that the contents of the packet have not been altered.

- At the link layer a separate MIC protects network routing information to prevent attacks that attempt to change the packet network/transport layer information.

Data Integrity also involves verifying that the packet has come from the correct source. The network/transport layer message integrity check field, the information used to generate the check field, and the sender/receiver unique session key that codes and decodes the data are tools that can be used to verify the source.

Network Security

A wireless sensor network also needs tools to protect it against attacks. These attacks can attempt to compromise the network by inserting Trojan horse devices, impersonating networks to get sensitive data from legitimate devices, and disrupting the network to deny service. Attacks can be launched from outside or inside the company by external people or employees. Successful network security depends upon techniques to support authentication, authorization and attack detection.

■ Together the *Wireless*HART Gateway and the wireless sensors joining the network are configured to limit and control which devices are allowed to access the network.

■ The network can only be secure if all the devices in the wireless network maintain security.

■ A *Wireless*HART Gateway has a secure authentication process which it uses to negotiate with all joining devices to ensure they are legitimate. As with all other network communications, all join negotiation traffic is encrypted end-to-end.

Denial of service (DoS) attacks are aimed at impairing the proper operation of the system by interfering with communications within the wireless sensor network. These attacks may try to jam the radio or they may try to overload a process like packet acknowledgments.

■ *Wireless*HART devices report anomalous conditions that might signal a denial of service attack, such as traffic counters, retransmissions, etc.

■ *Wireless*HART devices can be network routers or just data sources (user configurable) but only authenticated messages are routed onward.

■ *Wireless*HART devices are not authorized to be network key servers or wireless network managers.

■ Join, network and session keys must be provided to the *Wireless*HART Network Manager and join keys must be provided to Network Devices. These keys are used for device authentication and encryption of data in the network.

■ The *Wireless*HART Security Manager is responsible for the generation, storage, and management of these keys.

■ There is one Security Manager associated with each *Wireless*HART Network. The Security Manager may be a centralized function in some plant automation networks, servicing more than just one *Wireless*HART Network and in some cases other networks and applications.

Strong Key Management

An extremely important part of *Wireless*HART security involves proper encryption key generation and management. *Wireless*HART uses multiple keys at multiple layers to ensure security, confidentiality, data integrity and authentication. Join keys, session keys and network keys are used in different ways to protect data.

Key Management is Crucial for Security

Just as in the IT world, passwords must be kept in a secure fashion. Similarly, for *Wireless*HART, keys must be stored and distributed securely to ensure their secrecy.
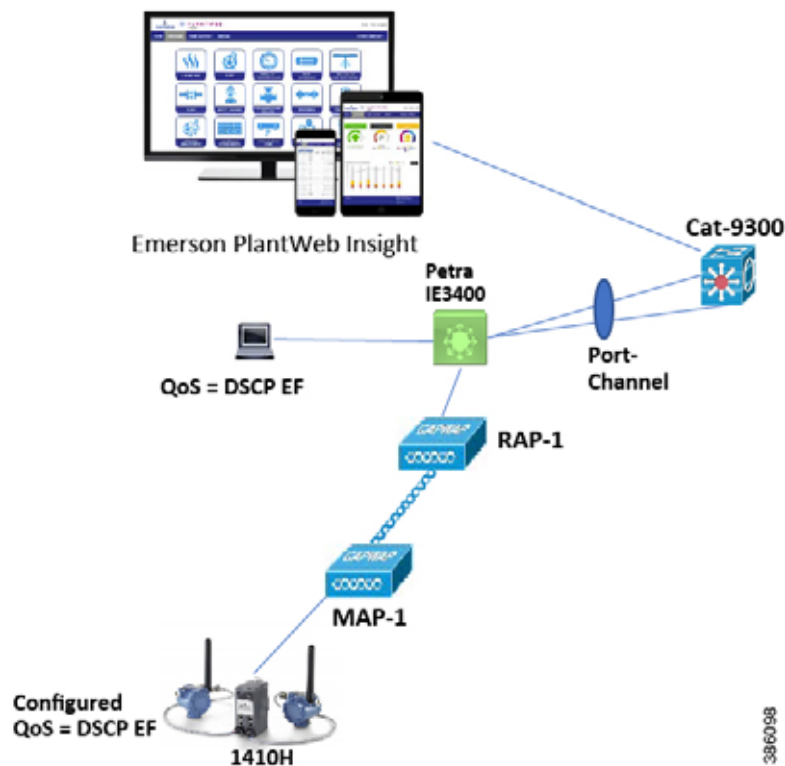
Encryption keys should be randomly generated and must be protected. The use of strong keys rather than default keys, makes it nearly impossible for an attacker to be able to guess a valid key. For this reason, *Wireless*HART provides the capability to utilize random strong keys. Some systems allow users to choose their own join keys; in these cases, these join keys should be selected and protected carefully. Some other systems may automatically support this entire join key process. All other keys are randomly generated by the *Wireless*HART network system.

If a common join key is being used, it should be changed periodically to increase the overall integrity of the system. Note: if the network is configured to use unique join keys, (also known as an access control list), rotation or changing is not required, since each key is generated for that device. Ensuring all devices are on the network when the join key is changed will make sure devices aren't orphaned. Some implementations of *Wireless*HART support automatic changing of keys.

The Security Manager, a part of the *Wireless*HART system, is usually embedded within the *Wireless*HART Gateway and automatically handles all keys except for the join key. As a user, this leaves only one type of key to control. In some cases, the security manager can also automatically manage this type of key as well. Implementations which hide all keys from view reduce the chance of inadvertent exposure.

QoS

Any QoS markings performed by the Rosemount gateways are preserved over the mesh network until the traffic is offloaded at the RAP Ethernet port.

Figure 49   Emerson Gateway QoS Marking

Industrial Wireless Site Survey and Design Considerations

Wireless Site Surveys

A radio site survey is highly recommended before the installation of any equipment. The purpose of a site survey is to conduct a detailed engineering study to create a competent network design that, once installed, will meet the needs of each use case that has been identified for the area. At the same time, the site survey gathers site-specific information that will aid in the installation of core infrastructure such as cabling, electrical, and AP hardware installation needs.

A proper site survey involves temporarily setting up an appropriate AP and antenna combination in deterministic locations to test and measure several facets of wireless connectivity such as Coverage, Signal Quality, Data Rate, Signal Overlap, RFI/EMI, and Environmental issues. This data is then analyzed to determine the correct hardware and install locations before undertaking the larger project costs of drilling holes, routing cables and conduit, and then mounting equipment.

Without a proper site survey or engineering design study, that equipment might be installed in non-optimal locations that greatly reduce the potential equipment performance resulting in coverage gaps and application problems. This would then require more equipment installed at high costs to overcome the potential coverage gaps and therefore increase overall project costs, perhaps far beyond the cost of simply doing the site survey (numerous instances have been experienced supporting the statements in this paragraph).

Pre-Survey Data Collection

An engineer must investigate the customer requirements to ensure that the survey accommodates proposed performance criteria as stated by the customer and equipment and application vendors. Thorough analysis may reveal non-typical needs that affect the site surveys.

For example, large outdoor areas with low user density would likely require a survey based on fewer AP installation points with more power and higher gain antennas. On the other hand, indoor environments with a high user density would likely require a survey based on a higher density of APs with lower power and less antenna gain to minimize coverage patterns, therefore providing higher aggregate capacity.

Example customer requirements could consist of the following:

- Areas that require coverage to support WLAN and other applications

- Density of users to support

- Client devices to support for WLAN:

    - Identify equipment parameters of any other WLAN client device

    - Specific applications that are suspected of requiring high network performance should be documented to understand the following:

    –WAN requirements

    –Throughput requirements

    –Network access (constant or bursting)

    –Cisco 7925 802.11a/b/g example:

        All data rates supported, suggest minimal 12Mbps for 802.11a/g

        40mW max transmit power for 802.11a/g, 50mW for 802.11b

        Diversity antenna for 5GHz 802.11a only

        RSSI greater than 35dBm (minimal -67dBm for 802.11b/g)

        25dB Signal to Noise Ratio (SNR) for survey

        Packet Error Rate (PER) 1% or less

        19dBm separation between same channel APs to minimize elevated noise levels and co-channel interference

- Designated high throughput rates for maximum network performance per AP

- High density areas such as training rooms, cafeterias, and equipment docking stations to be covered

- 802.11a/b/g/n

- Support for legacy 802.11b client devices propagation

- Control to minimize unwanted coverage

- Support for additional applications in the future not already identified

Environment RF Assessment

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

Spectrum Analysis

The principle goals of a spectral analysis are to search for and locate sources of mitigating radio frequency interference and then act accordingly to reduce the effects to other equipment and end user applications. Although comparatively rare in everyday life, RFI opportunities increase proportionally to the density of wireless devices. Therefore, areas such as medical, military, industrial, and commercial environments are more prone to effects of RFI due to wireless equipment being more commonplace as a result of applications needs. Other factors that effect RFI are band utilization from emitter oscillation and dwell times. Identifying these elements may also identify the source.

The following methodology may be used to determine sources of RFI:

1. Choose a location where equipment is sensitive to RFI or suspected and visually inspect for obvious sources such as antennas and transmitters.

2. Inspect the equipment to gather any detailed information such as operating frequencies and statements of Effective Isotropic Radiated Power (EIRP).

3. Energize the spectrum analyzer with a zero gain multi-band antenna that can cross multiple frequencies. The antenna should be free of obstruction to enable proper reception of surrounding signals.

4. Readings should be taken across the spectrum with particular attention and detailed analysis in frequencies of interest, which include known ranges used by equipment, nearby side bands, and potential harmonics. The information received will illuminate out-of-tolerance operations and potential sources of RFI.

5. If sources of RFI are observed, accurately measure the frequency, amplitude, dwell time. and oscillation time to cross-reference with known allowed emitters and determine the level of interference perceived.

6. Locate the sources of mitigating interference by moving the spectrum analyzer around and observing amplitude changes. Or use a directional antenna tuned for that particular frequency for rudimentary direction finding to zero into the area.

Survey and Test Tool

WLAN and Voice over WLAN (VoWLAN) deployments have a growing number of survey and test tools. Many of these tools have common capabilities for generalized site surveys. The following are the variations that may be pertinent to site surveys:

- Free tools are available for generalized WLAN information and have been used incorrectly as a definitive site survey tool.

- Client-specific tools such as the embedded client tools on the Cisco Wireless IP Phone and client utilities for laptops and tablets can provide very good basic information from the actual client perspective.

- Premium diagnostic hardware and software tools provide more in-depth information about the testing and environment. These tools evaluate passive, active, and even packet level information. AirMagnet and Ekahauo are two Wi-Fi survey test tool companies that are commonly used.
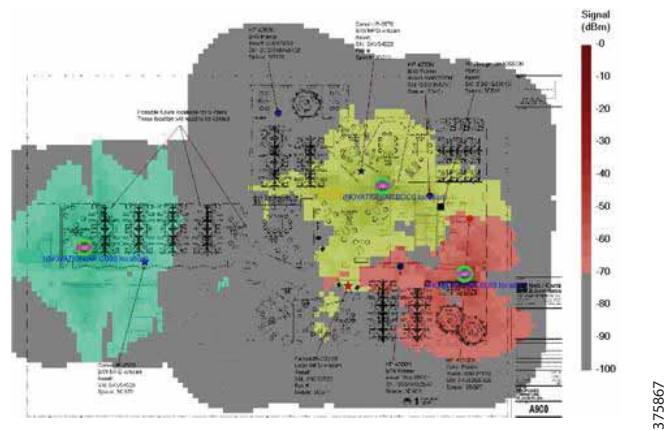
Premium Site Survey Test Suites

The AirMagnet Survey product allows field engineers to collect live information on signals, packets, and spectrum data during site surveys. This information may be collected while in active and passive modes; active mode surveys can reveal more detailed information while passive modes may allow for faster survey methodologies.

Survey Pro can coordinate test data with imported drawings and map data that can be correlated to reference points as well as spectrum analyzer data to help visualize wireless network coverage.

Figure 50 shows indoor survey data with colors enhanced to show channelization.

Figure 50   Indoor Survey Data

Site Survey Techniques

General site survey techniques vary among engineers based on experience and training, which may result in wide ranging designs for the same environment. Each of these different designs may be sufficient; however, this lack of uniform methodology and design principles can leave a customer or end user questioning these facets of the technology. Topics in this section include Baseline Propagation Assessments, Active Site Survey, Passive Site Survey, 2D Site Surveys, and 3D Site Surveys. These principles can be applied to indoor and outdoor environments, including oil and gas facilities onshore and offshore.

Work Safety

Safety is the first priority when working in any environment, especially within oil and gas locations. Several levels of safety training and certifications that may include national, regional, and site-specific training should be expected. For budgetary purposes, from 8 to 40 hours of instruction that will define the key requirements for safe working conditions at the location can be expected.

Additional site-specific safety training might be required when wireless site survey and installation conditions require:

- Work at heights (platform, lifts, and ladders)

- Equipment operator (high lifts)

- Confined spaces

- Helicopter transport to offshore (dunk tank crash survival training)

- Lockout/tagout/try out

A best practice for safety and security is to ensure a local site escort be present at all times with the survey/installation team and that this escort be on constant alert for potential hazards during the survey process.

Personal Protective Equipment (PPE) is sometimes available in limited quantity on the job site and it is recommended that a field engineer have their own minimum set of items that comply with local standards. Example minimum PPE items include:

- Flame resistant coveralls and clothing

- Steel-toed boots with a defined heel and high upper for ankle protection

- Hard hat

- Safety glasses (additional safety goggles sometimes required over the glasses)

- Hearing protection (foam inserts and outer earmuffs)

- Flame resistant leather work gloves

- H2S or 4-in-1 personal gas detector (likely loaned from customer site)

Site Survey equipment must be rated and operated around the environment for which it is rated. Cisco hazardous-rated APs are rated for Class 1 Div 2 / ATEX Zone 2 environments. It is important to note that these devices must be powered externally so be sure to use a compliant safe method of temporarily powering the APs. Site Survey laptops/tablets used for collecting data must also be rated for the environments into which they will be taken.

Figure 51 shows Cisco Technical solutions Architect (TSAs) working at a refinery.

Figure 51   TSAs at a Refinery

These Site Survey Engineers are wearing the required Personal Protective Equipment (PPE) and using survey equipment (tablet, AP or portable power) that is rated Class 1 Div 2 / ATEX Zone 2

The purpose of this assessment is to better understand propagation within an environment to establish general survey guidelines for that facility. Guidelines to consider are acceptable antenna types, maximum or minimal AP power settings, and general separation between APs to maintain as low of a noise floor as possible.

This baseline assessment may be considered more important in multi-floor environments where WLAN infrastructure is deployed in three-dimensional rather than two-dimensional planes. Understanding floor propagation and attenuation characteristics may affect overall positioning of APs on each floor as the findings may prohibit cookie cutter deployment techniques.

Cookie-cutter deployments refer to multiple situations or environments that are the same or very similar. In the case of a multi-floor facility this would refer to the general layout of the floor plan being the same or similar on alternating floors such as in a hotel, office building, or hospital patient wards. In these environments, a cookie cutter deployment technique would be using the same AP placements on alternating floors to avoid stacking columns of APs throughout the building.

Two potential issues with the stacked AP deployment occur, depending on the amount of through floor propagation and attenuation values. The first issue is if the attenuation values are minimal between the floors and AP locations on adjacent floors happen to be configured for the same frequency. This deployment would suffer from co-channel interference between the APs and a significant noise floor. The 19dBm of separation between co-channel APs noted in the Cisco Design Guide should be considered from all directions.

The second potential stacking issue involves roaming algorithms of various client devices. Those devices that may use RSSI levels as the primary or only factor to determine roam have been observed exhibiting roam-lock behavior. Roam-lock is a description used when client devices show a tendency to roam between APs continuously, thereby using more cycles to initialize and re-initialize connections rather than pass data. The result of this scenario is very low data throughput with the connectivity issues.

Test Criteria

In a multiple level facility, any three sequential similar levels can be selected to conduct the tests. If the network is to support 802.11a/n/ac and 802.11b/g/n, then these tests should be conducted with both technologies. If both technologies would be used, then it is best practices to first conduct these tests with 802.11a/n/ac, determine the best power settings, and then do 802.11b/g/n and alter power settings for those frequencies to match coverage cells to that of the 802.11a/n/ac coverage cells. This matched coverage cell architecture will ease overall design and deployment issues.

1. Set up one AP in one area of the middle floor. Set Power level on Access Point to at least one power level below the maximum power of supported client devices or to the minimized power level required to provide minimal coverage for the application in that particular environment. This method would allow scaling coverage up or down once installed.

2. If deploying the actual client device for which the facility is being surveyed, use the typical configurations on that device during the survey test activities. It is advisable to use engineering technical tools that specialize in site survey data acquisition. If using a test tool client adapter for testing rather than the actual client, then set client adapter power to emulate the actual client device for which this survey is designed.

3. Begin the site survey for the AP location to determine coverage area of that AP on that level with the specific power setting and antenna configuration while recording the data.

4. If 5GHz 802.11a/n/ac and 2.4GHz 802.11b/g are to be used for this location, then at this point configure AP power for 802.11b/g while standing at the edge of the 802.11a coverage cell to match the cell sizes. After this, the baseline power levels for both 802.11a and 802.11b/g is set. This step is omitted when using outdoor mesh equipment where the 5GHz radio is only used for backhaul communications and not supporting client connectivity.

5. Once this baseline is established, then re-do the site survey process in that same floor for that same AP location for 802.11b/g coverage ensuring that this information is documented.

6. Conduct an active site survey on the two adjacent levels for each wireless band (802.11a and 802.11b/g) and document the results of each test. If the signal strength is not sufficient to obtain detailed diagnostic data, then switch to passive mode and collect any data available.

Impact

If substantial propagation is found on adjacent levels, then staggering the AP locations on each sequential level rather than stacking them would be prudent to provide additional physical isolation attenuation between AP locations. This testing may yield a survey and installation pattern that could speed up the remainder of the survey process.

Implementation Considerations

Many factors should be considered when designing and deploying a wireless network. Each of the topics listed has a unique ability to affect wireless communications and thus must be considered during the site survey and installation process.

Common RF Installation Considerations

- Fresnel zone

- Knife-edge diffraction

- Obstruction shadowing

- Environmental attenuation

- Reflection and scattering

- Multipath

- Delay spread values

- Antenna polarization, isolation

- Reactive near-field, Radiating near-field

- In-band RFI and out-of-band RFI / Harmonics

- EMI

- RF Noise floor

- Equipment specifications

- Antenna field of view

- Antenna E and H planes

- Survey characteristics:

  - Coverage

  - RSSI

  - SNR

  - Data rate

  - Retries/loss

  - Overlap/redundancy

- Required Infrastructure:

  - High installation costs

Regardless of proper AP locations between levels, site survey engineering personnel should also consider how the overall layout applies to applications such as location appliances that rely on RSSI trilateration to determine approximate locations of a client device. In an oil and gas processing area, the elevated spaces may only require singular AP locations to provide the needed coverage or connectivity. A suitable location on infrastructure like a vessel or stack may not exist to install APs to support RSSI trilateration; therefore, location information might be limited to the nearest AP and a wider margin of error. Additional accuracy might be yielded with complimentary third-party localized exciters that can change the behavior of a tag when the client devices pass by a near-field micro-area such as a doorway or ladder access.

Passive Survey

Passive site survey results use test tools in a receive-only mode for interpreting WLAN and general RF diagnostic data within an environment. This capability, which is provided by both low- and high-end site survey tools, is integrated into mapping functions of the higher-end tools. Passive survey tools generally provide a bird's eye view of all WLAN transmitting devices within an area based primarily on signal strength, however, they may not provide the detailed signal quality information that is obtained with an active site survey.

Conducting a passive site survey with multiple APs will yield overall information of all APs transmission levels in a surveyed area. A field engineer must consider the ramifications of this type of survey. For example, this method may place APs in a generally well-guessed correct area, but one that ultimately may not be optimal.

Active Survey

Active site survey results show greater detail of the local WLAN and RF environment. Interpreting this test information can help a field engineer to identify signal strength and quality while also revealing issues of RFI or EMI within the test environment. For example, in an environment where the survey utility experiences high signal strength but very poor quality as represented in high packet retries and/or high packet loss, then this may be an indication of local RFI or EMI. This type of information within a plant can be critical to a field engineer when considering AP placement and antenna choices. Typical method for active survey is to place an AP and maintain a connection to it with the capabilities to see all data characteristics for that location, transmitter power, antenna, etc. In this way the proper placement of APs can be determined.

Predictive Survey

Predictive site surveys are conducted via computer modeling to estimate the approximate location and number of APs required to provide coverage in a given area. Predictive modeling accuracy is highly reliant on the amount and accuracy of data put into the modeling tool to interpret attenuation and reflection boundaries. Predictive site surveys are considered a tool best for estimating because it does not have the ability to fully simulate local environmental effects of RFI, EMI, environmental, and construction issues that are not represented in drawings or clutter data. Onsite analysis is still required to validate predictive results and then finalize with local testing to determine the actual AP performance and install location data.

Two-Dimensional Site Survey

A two-dimensional site survey only addresses WLAN coverage on a single floor. This has been the common practice for many since the introduction of WLAN devices and is still widely used today.

One methodology for conducting a site survey is referred to as the corner-out method. This process can be considered time consuming; however, the time invested in gathering information will yield the highest level of accuracy for the AP placement within an environment.

1. The first step in the corner-out method is to locate the AP in the furthest corner of a facility that may need guaranteed coverage with the antennas of choice for that environment. Determine the area of coverage emitted from that location. This defines a boundary in which the AP anywhere can be safely relocated within while still providing coverage to that remote corner where the testing began.

2. The next step is to determine the power levels and coverage cell size based on area Wi-Fi client power, receiver sensitivity, user density, and application density requirements. If this is an 802.11a and 802.11b/g survey, then these power levels should be changed on all interfaces to have a matched coverage cell size. The area of relocation for the first survey point has now become more defined.

3. With the AP moved into its first official test location, the site survey will yield the anticipated controlled results. Depending on the desired results, it may be best to leave an AP in remote rooms for more cellular isolation that directly relates to the density of APs required to support coverage. Utilizing remote rooms with APs on the outer edge of a building and a mix of other AP locations inward of a building may provide more accurate trilateration data for Cisco Wireless Location Services. Sometimes APs are located in hallways where they are more serviceable and where the hallway itself provides an unobstructed conduit allowing further propagation range from a single AP; because of co-channel interference this is no longer considered a best practice.

4. Each additional AP location may be methodically determined in the same manner from the outermost location requiring coverage within a cell.

5. Continuing with this site survey method will yield highly accurate results for the rest of the floor. Each color indicates channels 1, 6, and 11.
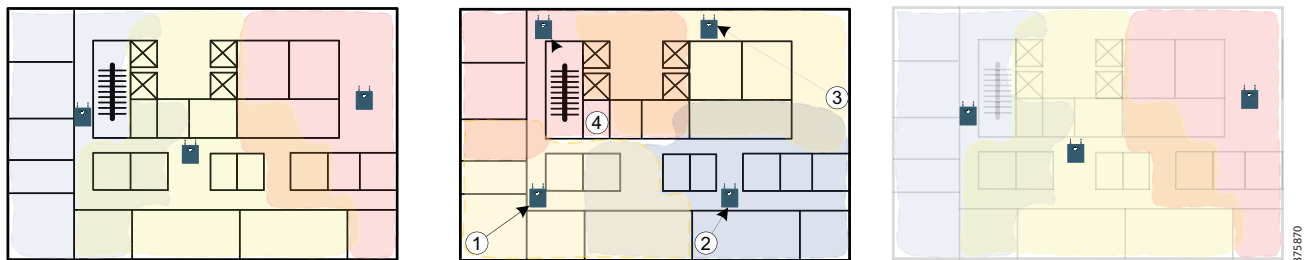
Figure 52   2D Site Survey

Three-Dimensional Site Survey

For buildings that have multiple floors requiring coverage throughout, the field engineer must consider the ramifications of AP coverage bleed through from adjacent floors. Remember that the Cisco 7921 Design Guide specifies 19dBm of isolation between APs on the same channel—that isolation is required from all directions not just the same floor.

Figure 53   3D Site Survey

This should only be done with a deployment method of staggering rather than stacking AP locations between floors to provide greater RF separation and signal isolation. The term stacking refers to placing the APs in the same location on every floor, thereby reducing the overall physical isolation between them and making them more susceptible to co-channel interference from adjacent floors.
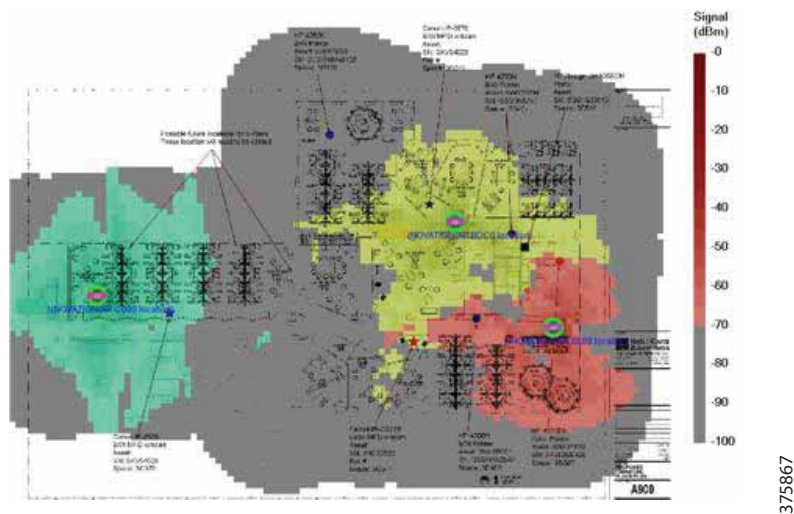
Surveying each AP location for 3D results may require as much as 200% more time. For buildings that have same or similar configured floors, conducting the baseline survey and establishing an acceptable pattern between floors for every other floor AP placement can significantly reduce the additional time required for this type of survey. Information to determine the amount of space needed for physical isolation can be obtained using the described Baseline Testing Methodology within this document.

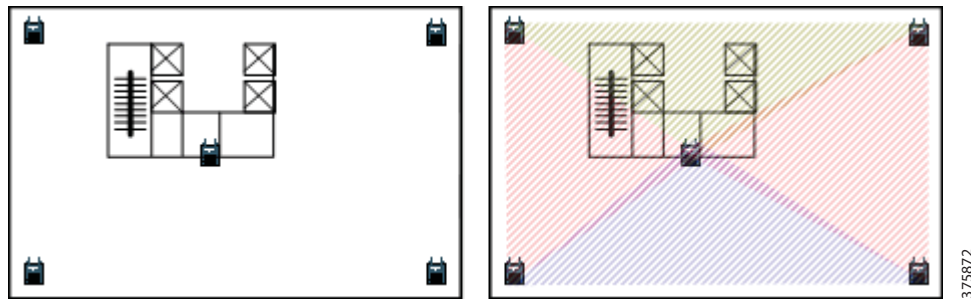## Advanced Site Survey for VoWLAN and Location-Based Services

Recent popularity for applications such as Context Aware location services has changed the mechanics of the site survey once again. Cisco's current recommendation for a WLAN that supports Location-Based Services (LBS) is that any area requiring this feature be seen from at least three APs with no less than -67dBm signal strength on the same floor or level. An increase in AP density over traditional methods will be required to do this with 802.11b/g/n and 802.11a/n/ac standards.

One effective method to increase AP density while maintaining a lower noise floor is to provide outside-in coverage. This method uses the physical boundaries of a building to better isolate coverage for more of a pico-cellular design to minimize co-channel overlap at the same time.

Figure 54   Indoor Site Survey Channelization

- In Figure 54, Map A illustrates the higher AP density that may be required to support location services for 802.11a/b/g/n/ac devices with greater accuracy. The byproduct of this method is a higher wireless density for more aggregate wireless capacity.

- Map B illustrates perceived trilateration areas in support of LBS. When planning a survey, the field engineer must consider what their approach will be to provide this trilateration and perhaps visualize the design goals.

- Map C illustrates an adjacent floor installation where the access points have been staggered rather than stacked. This method may not be necessary if minimal through floor penetration is experienced during the baseline survey. Again, generally it is recommended not to stack/replicate locations in order to enhance cellular isolation.

Figure 55   Site Surveys for Large Open Spaces

For large open spaces, the AP density will likely be less but accuracy may also be less as a result. One must account for the AP density and determine if this provides the level of accuracy desired given the applications relying on location based services
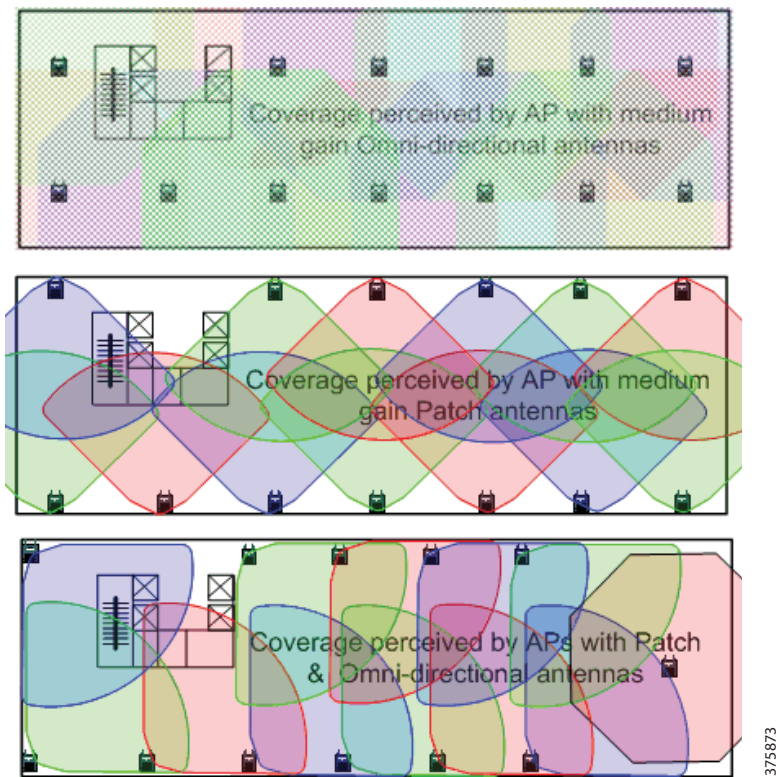
Omni versus Directional Energy Surveys

Predominant antenna technology used indoors has been and is omni-directional. These antenna types include the dipole or rubber duck, low profile ceiling mount, and medium gain stick type antenna.

Generally, these are all very good antennas developed to maximize performance in all directions from a single installation point in the middle of a small or large area while minimizing installation requirements.

Some large-scale, open-air environments where numerous APs required for coverage may also be well within each other's coverage pattern may challenge this type of antenna technology. Remember that higher gain antennas have reciprocity therefore can offer the same directional gain for transmit and receive. This allows for the transmit power between the AP and the client to be matched and will offer a balanced RF environment over matched antennas and higher transmit power from the AP over the client. For these environments, a field engineer must consider the benefits of directional energy to provide controlled propagation while also isolating noise sources that are out of the antenna pattern.

Figure 56   Omni versus Directional Energy Survey

The examples above illustrate the concept of controlled propagation to provide a lower noise floor with which the APs and client devices would have to contend. The top graphic shows a noisy environment with all Omni-directional antennas then the same area using directional antennas. These alternative designs have been proven in certain situations to lower the overall noise floor dramatically, thereby enabling higher quality WLAN communications. It is important to note that the same baseline concerns for two- and three-dimensional surveys still apply when using directional antennas.

Impact of Use Cases and Site Surveys in Oil and Gas

For oil and gas process areas, the common AP—keep in mind that the antennas have to be hazardous-rated to use in these environments—will be an outdoor hazardous-rated AP and the most common antenna of choice will likely be a medium gain dual band omni-directional antenna. Applying the information from previous sections, we can surmise that many of these outdoor environments will benefit from maximizing coverage with omni-directional antennas from minimal installation points as a means of minimizing installation costs.

The use cases will drive wireless requirements and AP densities within a location. Table 8 shows example comparisons of equipment requirements based on different use cases.

Table 8   Size of the Wireless Network

Type of Wireless Network	Approximate Number of APs per 10 Acres	Approximate Number of APs per 10 Hectares
Process Control Network—Wireless monitoring with 802.15 base stations on Cisco Mesh	2-4	5-10
Handheld computer data entry	8	19
Voice over WLAN with Cisco 7926G-EX	12	28

Table 8   Size of the Wireless Network

Type of Wireless Network	Approximate Number of APs per 10 Acres	Approximate Number of APs per 10 Hectares
Voice over WLAN for Remote Expert	12	28
Video over WLAN for Physical Security	2	5
Location Analytics/Man Down (based on 2D coverage; 3D requires additional APs for elevated structures)	36	84
Wireless data connection of land-based oil drilling wells with high-power client devices	1	3

Note: The numbers in Table 8 are case study numbers and serve only as approximations. The actual number of APs required will be determined during a proper site survey and network design.

Network Optimization

The end user should be made aware that the survey is valid for the site as it existed during the onsite survey activities. Any changes made to the environment post survey can potentially invalidate the results. A post installation survey should be completed in order to tune and optimize the WLAN, especially for a VoWLAN and/or LBS site survey. Consideration should be given to verifying coverage, roaming, channel, and TX power usage.

Installation

Installation of the Connected Refinery Solution components is an extremely important part of the deployment process.

All relevant stakeholders from the installation site must be consulted in advance and involved throughout the deployment process. Their knowledge about vital issues, when factored into the deployment, will help decrease unnecessary delays.

Examples of such stakeholders are the local site manager, Health Safety and Environment (HSE) staff, and operations manager(s). The actual number will depend on the number of plants in a site that the work will be taking place in addition to the project staff.

The following list contains some important aspects and considerations that need to be taken prior to the commencing of the installation activities and need to be validated with the local site responsible personnel as mentioned above:
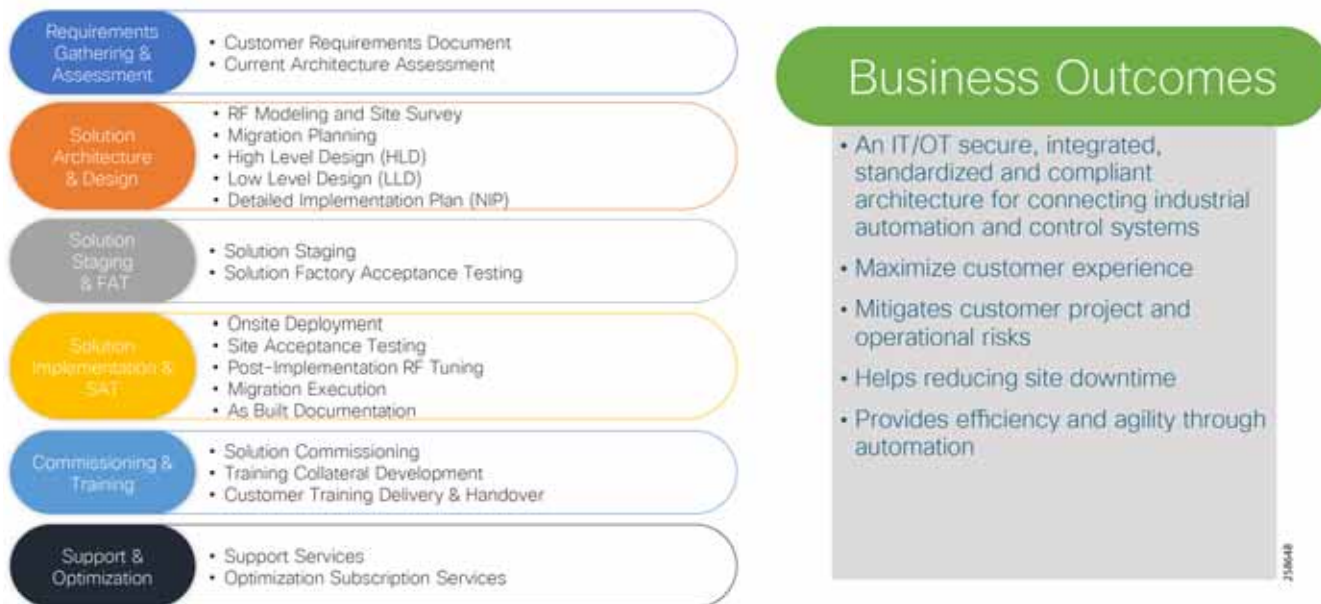
- Adherence to health and safety rules.

- Electrical installation work that needs to be conducted to enable the equipment to be deployed in the field.

- Availability of authorized equipment to use at the site (such as scissor lift and scaffolding that needs to be deployed prior to commencing the installation activities).

- Availability of adequate fiber/copper links to connect the APs to allow for the implementation of the selected use cases.

- Ensure that all the appropriate certifications of the products are available and applicable to the specific regulations and bodies to which the location of the site is adhering.

Cisco Customer Experience

Thanks to a unique architectural-based approach, Cisco CX Industrial Networking and Security services help mining operators to accelerate the digitization of their existing operations. Through strategy development, architectural assessments, network design, migration and deployment assistance, and support services; Cisco and key ecosystem partners plan, build, and manage solutions. These solutions focus on business outcomes resulting in improved work site safety, risk mitigation, higher productivity, improved operational efficiency, deeper intelligence and insights, with security at the core of the end-to-end solution.

Cisco CX offers a broad range of services that are scaled and customized to meet any operator's objectives. Relying on a proven methodology, CX partners with customers as they progress through their innovation and digitization journey, helping them achieve tangible results.

Figure 57   Cisco CX Industrial Networking Services

Cisco CX services and key partners in the industrial space maintain high standards for expertise and experience. Cisco CX Industrial Networking and Security Services consists of business and technical experts, with expertise within the mining industry. Our proven processes and tools deliver consistent results based on best practices and strong communication. Our experts deliver services that allow organizations to accelerate the integration and transformation of their current infrastructure to the next generation network, capable of evolving operations to continue to meet the evolving demands of the business.