Wireless Networks Enabling Autonomous Vehicles for Underground Mines

Release 1.5

September 2020

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

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

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

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

©2020 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

Contents

Wireless Networks Enabling Autonomous Vehicles for Underground Mines

Chapter 1: Cisco IoT Underground Mining Solution for Sandvik Autonomous Vehicles

Executive Summary

Operations in today's mining industry need to be flexible and reactive to commodity price fluctuations and shifting customer demand, while maintaining operational efficiency, product quality, sustainability and most importantly safety of the mine and its personnel. Mining companies are seeking to drive operational and safety improvements into their production systems and assets through convergence and digitization by leveraging new paradigms introduced by the Industrial Internet of Things (IIoT). However, such initiatives require the secure connection of process environments via standard networking technologies to allow mining companies and their key partners access to a rich stream of new data, real-time visibility, optimized production systems and when needed, secure remote access to the systems and assets in the operational environments.

The Cisco® Industrial Automation (IA) Mining solution and relevant product technologies are an essential foundation to securely connect and digitize mining production environments to achieve these significantly improved business operational outcomes. The Cisco solution overcomes top customer barriers to digitization including security concerns, inflexible legacy networks, and complexity. The solution provides a proven and validated blueprint for connecting Industrial Automation and Control Systems (IACS) and production assets, improving industrial security, and improving plant data access and reliable operations. Following this best practice blueprint with Cisco market-leading technologies will help decrease deployment time, risk, complexity, and improve overall security and operating uptime.

This version of the Cisco Reference Design and Implementation guide focuses on the design, implementation and validation of a subset of the Cisco Industrial Automation Mining 1.0 Reference Architecture to provide wireless connectivity within an underground mining environment to enable the Sandvik AutoMine application for remote operations of autonomous vehicles.

Challenges in the Mining Industry

The Mining industry faces challenges from many fronts. Constant threat of the commodity price falling below the current production cost at a given location, environmental issues, need for water, power, waste storage, water treatment, regulatory compliance, and site remediation just to name a few.

Operations in today's mining industry need to be flexible and reactive to commodity price fluctuations and shifting customer demand. Digitizing the mine helps provide greater visibility and insights, thus improving decision-making capabilities; helps lower safety risks and operational costs, resulting in increased operational efficiency and productivity.

Safety is paramount in a dangerous, nonstop, 24x7x365 mining production environment. Product grade, quality, worker productivity and overall equipment efficiency (OEE) metrics are key concerns mining companies.

Additionally, Mining is often performed in isolated parts of the world and requires the development of a local ecosystem comprised of infrastructure and services to support the mining operation. With remote locations, a mining company may be the landlord for housing, an Internet provider, water utility, waste management utility, transporter of people and

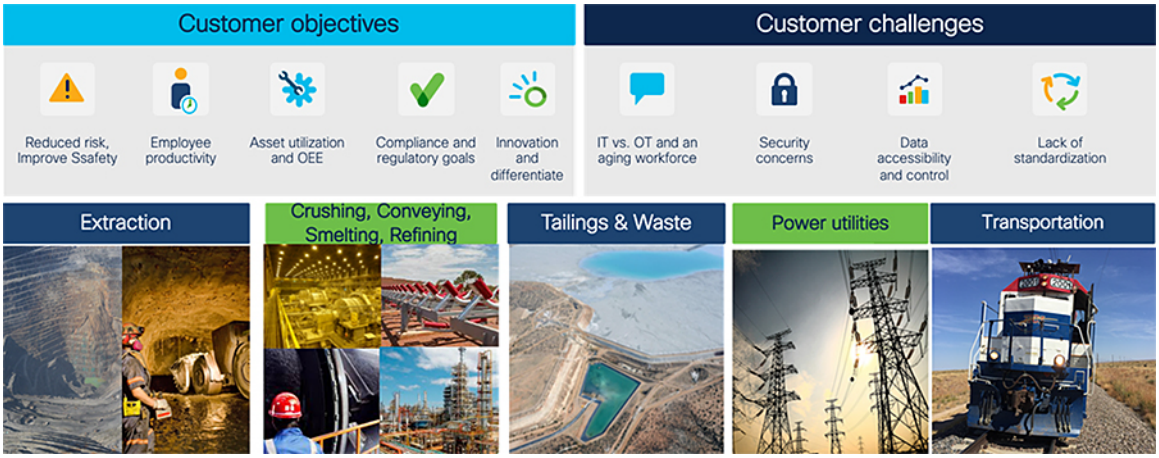
product, phone company, power provider, with each of these being a necessary component to support the primary mining processes. Operators obtain licenses to mine from governments that impose strict environmental operational requirements, maintain the land lease, and obtain lease extensions for future operations.

The mining process disrupts water tables (reduction, pollution, and redirection), generates dust, impacts flora and fauna, and consumes vast amounts of energy. When transporting the ore from the mine to a processing plant or to a customer location, mines often use railway systems that cross public boundaries and roads. Mine bulk impacts nearby towns (dust, pollutants to marine environments, noise, light). If things go wrong, entire ecosystems can be disrupted – such as tailing dam failures, toxified water tables, land subsistence, and permanently redirected water flows. Ore refineries generate large volumes of unusable material that have to be handled in an environmentally responsible manner. Mines need both social and environmental licenses to operate. They have responsibilities to the communities and geographic areas in which they operate and need to remediate land back to a government in an agreed state at the completion of the mining operations.

The mining sector plays a significant role in global metals, minerals, and energy production supply chains. Mining companies are major employers and contributors to government revenues via royalties and taxes. Smooth, reliable and consistent operations is vital to mining companies, countries and world economies alike.

Figure 1 below highlights key objectives and complexities of digitizing mining production environments, from extraction to transportation and all the steps in between.

Figure 1 Mining Customer Objectives and Challenges



Mining Use-Cases and Requirements

Safety Systems

Prioritize safe, healthy, and sustainable operations, with worker and environmental safety as the top priority. In every part in the mining value chain safety is the top priority. The ultimate goal is to achieve zero worker injuries and minimize human error. Autonomous, semi-autonomous, and remote operations are helping achieve this goal today by removing people from high-risk environments. Machine autonomy demands a highly available, deterministic, and secure network infrastructure upon which network-intensive mining systems and applications rely. Slope and seismic activity monitoring allow for production optimization while diminishing safety risk.

Autonomous Mining Operations

Traditionally, most heavy equipment operations in a mine are performed with an operator located within the mining equipment. Not only is this costly, but it also puts personnel into potentially hazardous situations such as equipment rolls or collisions.

For underground mines, transportation from personnel housing to mine operator staging areas can take over an hour (one way). Workers might be required to wear special personal protective equipment (PPE), which requires a significant amount of time to maintain and change into. In some underground areas that are extremely dangerous and unstable, such as wet muck underground tunnels, or even in extremely hot or cold mine locations, mine personnel can be directly exposed to dangerous environments for only limited amounts of time.

Mining operations are driving toward fully autonomous operational models throughout the production chain. Removing humans that manually operate equipment in high risk production areas will improve productivity, improve product quality, increase worker safety, and help reduce the overall cost of operations. Common use cases today involving autonomous vehicles and equipment are either fully automated, without any direct human interaction, or semi-automated, with equipment that is remotely operated and monitored. Remote operations centers can be located close to the mine site or located completely offsite and away from the mine.

The first step in the evolution from manual to semi-automated or fully automated mining operations is *digital dispatch*. Digital dispatch processes connect mobile fleets to the mine network, thus allowing for proper route calculations and ensuring that operators unload the correct materials in the right spots, efficiently transporting high-grade ore to the crusher and appropriately delivering overburden to the correct dump. Digital dispatch requires connecting the mine fleet over a wireless network.

Semi-autonomous machine operations include loaders in a one-to-one or one-to-many remote operator to machine ratio. One use case is a haul truck operator who can control a loader from inside the cab of the truck to load ore into their truck, thus eliminating the need for an additional operator who would be sitting idle the entire time that the truck is in transit. A ratio of one-to-one or one-to-many allows remote personnel to operate mining equipment from a safe location. Allowing operators to work from a control room located *aboveground* while operating machinery located in a high-risk environment *underground* improves operational efficiency by eliminating some of the travel time, removing the need for PPE, and most importantly, removing personnel from harm's way. In addition, remote operators can now simultaneously manage more than one machine, thus reducing the number of operators needed.

Likewise, autonomous trucks can haul resources from shovels or front-end loaders in a mine to a crusher area. When fully automated, trucks may continuously operate at optimum performance, thus reducing engine wear and improving tire performance and fuel efficiency. This reduces maintenance costs, reduces downtime, and increases productivity.

Reliable wireless network performance is critical to ensuring continuous equipment operations. Network personnel strive to minimize packet loss and wireless roam times to achieve optimal application performance. Any wired network issues, or prolonged wireless roam times can trigger the safety system that in-turn will result in the vehicle or equipment stopping, ultimately affecting productivity, reduced production and has financial implications. Cisco's portfolio of industrial and ruggedized wired and outdoor wireless products plays an integral part in providing a high-performing, highly available, and secured networking infrastructure for supporting autonomous systems within a mine.

Connecting the mine vehicle fleet to the production network allows vehicle intelligent monitoring systems (VIMS) to feed a large data analytics engine. Analysis of VIMS data by mine operators enables better equipment monitoring and proactive maintenance. Cisco's solution helps mining companies improve predictive maintenance and provides visibility into issues such as problems with engine oil pressure or faulty cooling systems before they escalate. Discovering and addressing these issues before a failure occurs can save up to 72 hours of downtime or a $500,000 engine replacement cost.

Autonomous Dozing

Dozing can be done in several ways. The traditional way is to have an operator inside the cab driving the dozer. Several times a dozer is used to compact an area or to move in a repetitive manner to move some material. When this is the case autonomy can play a big role in executing the repetitive motions. An operator can remotely move an automated dozer from one job to the other and this way a single operator can efficiently control several dozers.

Autonomous Haulage

Likewise, autonomous trucks can haul resources from shovels or front-end loaders in a mine to a crusher area. When fully automated, trucks may continuously operate at optimum performance, thus reducing engine wear, improving tire performance and fuel efficiency. This reduces maintenance costs and downtime and increases productivity.

Tailing Ponds

Currently, many mine operators monitor tailing ponds manually. Operations management send personnel to tailing ponds; however, prior approval is typically required for access. Acquiring approval for access can take time, as does the drive to and from the tailing pond (which can take an hour in some facilities). Additionally, supervisors require that personnel check valves and place discharge hoses. Ultimately, a large amount of time is expended prior to the movement of any water or waste product.

A tailing pond at an open pit mine is shown in Figure 2.

Figure 2 Tailing Pond at an Open Pit Mine

Enabling connectivity and visibility into water and waste flow from the process plant to the tailing ponds will improve production efficiency, resource utilization, monitoring for safety, and environmental compliance. Being able to monitor valve positions remotely allows operators to proactively identify where waste would be delivered without having to dispatch personnel to visually inspect valve conditions along the lengthy pipes that run between the processing plant and the tailing ponds. This capability will speed up the waste management process and improve safety with the knowledge that waste is being sent to the correct location. Otherwise, waste could cause instability if sent to an incorrect tailing pond and may potentially lead to environmental impact.

Tailing dams require seismic and dam wall monitoring. Mobile mine workers want full coverage via remote access to production and corporate systems when working in and around tailing dams.

Dust control is another major concern around mines in general and at tailing areas specifically, because tailing ponds are made of very small particles of earth. Environmental impact is a major concern, as not only could dust have a negative impact on the environment but it also could result in large fines from the local environmental supervisory agencies. By automating dust control sprays and using video to demonstrate dust control, a mining operation can limit the financial impact from penalties imposed should dust-related issues occur. Other places where automated dust control is needed include ore heaps and bulk shipping ports.

Key networking capabilities required to support the mobility domain include:

- Resilient, reliable and mobile wireless networks to connect key assets and personnel
- Wireless backhaul and WAN technologies to interconnect the extraction zones to local sitewide operational services and Remote Operations Centers.

The Sandvik-Cisco Systems partnership targets the acceleration of mining digitalization and the extension/ enhancement of the Sandvik offering; it also seeks to integrate Cisco technology with existing mining operations. With its global coverage, both from a technology and a commercial perspective (sales and support), Cisco is in a unique position to collaborate with Sandvik in this space to bridge the gap between operations technology (OT) and information technology (IT).

Chapter 2: Sandvik AutoMine Use-case and High-Level Network Architecture

Digitalization in Underground Mining

With growing pressures on the global mining industry, achieving breakthrough performance in all areas of the mining life-cycle is fundamental to staying profitable. Mining companies will have to re-think how they have been operating in the past and adapt a digital future to improve productivity, safety and efficiency.

Digital technologies have the potential to unlock new ways of managing variability and enhancing productivity. As the skilled labor pool shrinks companies are seeking opportunities to better utilize their more experienced workers, and to gain new flexibility to meet future supply chain demands.

Connected devices and smart machines help capture real-time process information enabling better decision-making. Gaining deeper insights into equipment health and operations can dramatically improve asset productivity. Remote operation centers are the evolution to the digitization effort helping enable visibility, management, and remote command and control to allow for economies of scale.

The mine digitalization revolution and the development of technology has and will continue to enable huge improvements for underground mining operations. This requires a modern and standardized infrastructure that will support the digitalization process as well as openness and interoperability between different systems.

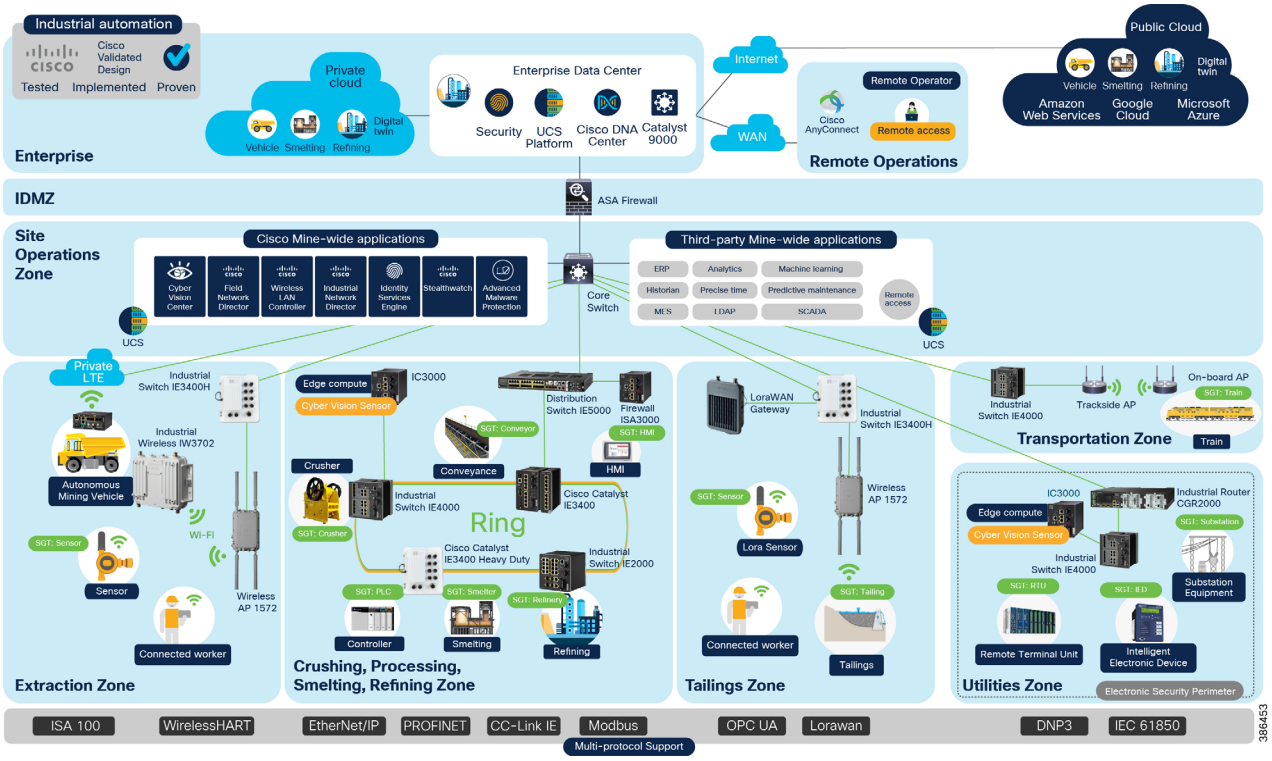
Benefits of Digitalization in Underground Mining:

- Increased Productivity
- Improved Mine Safety
- Informed Decision Making
- Improved Failure Anticipation
- Reduced Environmental Impact

Cisco Industrial Automation – Mining Reference Architecture

The Cisco Industrial Automation Mining CRD defines a reference architecture (Figure 3 below) to support multiple operational and non-operational services over a secure, robust communications infrastructure. The architecture applies to wired and wireless network designs, security and data management technologies across the mine. The reference architecture provides a blueprint for the essential security and connectivity foundation required to deploy and implement the various building blocks for a mine. This solution is therefore key to digitizing mining use cases to achieve significantly improved safety and business relevant outcomes.

Figure 3 Cisco Industrial Automation for Mining Reference Architecture



The Mining Industrial Automation solution applies the best IT capabilities and expertise tuned and aligned with OT requirements and applications deployed in mining industrial environments:

- High Availability for all key industrial communication and services.
- Real-time, deterministic application support with low network latency and jitter for the most challenging applications, such as motion control.
- Deployable in a range of industrial environmental conditions with Industrial-grade as well as commercial-off-the-shelf (COTS) IT equipment.
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s of IACS devices) deployments
- Intent-based manageability and ease-of-use to facilitate deployment and maintenance especially by OT personnel with limited IT capabilities and knowledge.
- Compatible with industrial vendors, including Rockwell Automation, Schneider Electric, Siemens, Mitsubishi Electric, Emerson, Honeywell, Omron, and SEL.
- Reliance on open standards to ensure vendor choice and protection from proprietary constraints.
- Distribution of Accurate Time across the site to support motion applications and Schedule of Events data collection.
- Converged network to support communication from sensor to cloud enabling many Industry 4.0 use cases, such as machine learning and predictive maintenance.
- IT-preferred architecture integrating OT contexts, following security guidelines from the security organization that are applicable and validated for Industrial applications (achieves best practices for both OT and IT environments while integrating security best practices).

- Deploy IoT applications with support for Edge Compute deployment models.
- OT-focused, continuous cybersecurity monitoring of IACS devices and communications.

Autonomous Mining

Mining companies continue to deal with labor shortages, higher production costs, government and environmental regulations and fluctuating commodities markets. They need to find more effective ways to improve operational utilization, contain costs, and improve worker safety.

The solution is for remote-controlled, semi-autonomous, and autonomous equipment to address challenges in the underground mining environment. Remote control rooms can be built on the surface to house consoles for fixed and mobile equipment in the underground mine, such as drillers, hammers, trucks, and loaders. Automatic drilling and positioning functionalities are recommended for efficient production. Drivers are trained to remotely operate equipment from the control room.

Automation is part of a broader industrial movement, often referred to as the fourth industrial revolution or Industry 4.0, which also includes robotics, artificial intelligence (AI), and the Internet of Things. This movement is marked by technology integration and interconnection, which can improve Overall Equipment Efficiency (OEE) and productivity

Due to their immense potential for improving safety and productivity, mining companies are investing in autonomous solutions. The mining industry is increasingly embracing automation as a safety and productivity enabler and as a critical factor in creating a sustainable future of mining. For these reasons, automation is a key part of many mining companies' digital transformation roadmaps alongside advances in artificial intelligence, system integration, remote operations and the Internet of Things.

Successfully implementing autonomous systems adds clear value: it can improve safety, increase production efficiency, and lower maintenance costs. Implementing autonomous systems also presents new challenges such as security and safety risks and workforce and workflow changes.

Semi-Autonomous Operations

Semi-autonomous (Remote command) machine operations include loaders in a one-to-one or one-to-many remote operator to machine ratio. One use case is a haul truck operator who can control a loader from inside the cab of the truck to load ore into his truck, thus eliminating the need for an additional operator who would be sitting idle the entire time that the truck is in transit. A ratio of one-to-one or one-to-many allows remote personnel to operate the equipment from a safe location.

Allowing operators to work from a control room located aboveground while operating machinery located in a high-risk environment underground improves operational efficiency by eliminating some of the travel time, reducing downtime during shift change, improving visibility of equipment location, removing the need for PPE, and most importantly, removing personnel from harm's way. In addition, remote operators can now simultaneously manage more than one machine, thus reducing the number of operators needed.

Autonomous Operations

Likewise, autonomous trucks can haul resources from shovels or front-end loaders in a mine to a crusher area. When fully automated, trucks may continuously operate at optimum performance, thus reducing engine wear and improving tire performance and fuel efficiency. This reduces maintenance costs and downtime and increases productivity.

Reliable network performance is critical to ensure continuous operation of equipment. IT personal strive to minimize packet loss and roaming times to achieve optimal application performance. Any computer network issues, or prolonged roaming times can initiate safety systems that result in the vehicle or equipment stopping, ultimately affecting productivity and production. Cisco's portfolio of industrial and outdoor wired and wireless products plays an integral part in providing a high-performing, highly available, and secured networking infrastructure for supporting autonomous systems in the mine.

Connecting the mine vehicle fleet to the network allows vehicle intelligent monitoring systems (VIMS) to feed a large data engine. Analysis of VIMS data by mine operators enables better equipment monitoring and proactive maintenance. Cisco's solution has helped mining companies improve predictive maintenance, and it has also provided visibility into issues such as problems with engine oil pressure or faulty cooling systems before they escalated. Discovering and addressing these issues before a failure occurs can typically save hours of downtime and costly engine replacements.

The key networking capabilities required to support the mobility domain include:

- Resilient, reliable and mobile wireless networks to connect key assets and personnel,
- Wireless backhaul and WAN technologies to interconnect the extraction zones to local sitewide operational services and Remote Operations Centers.

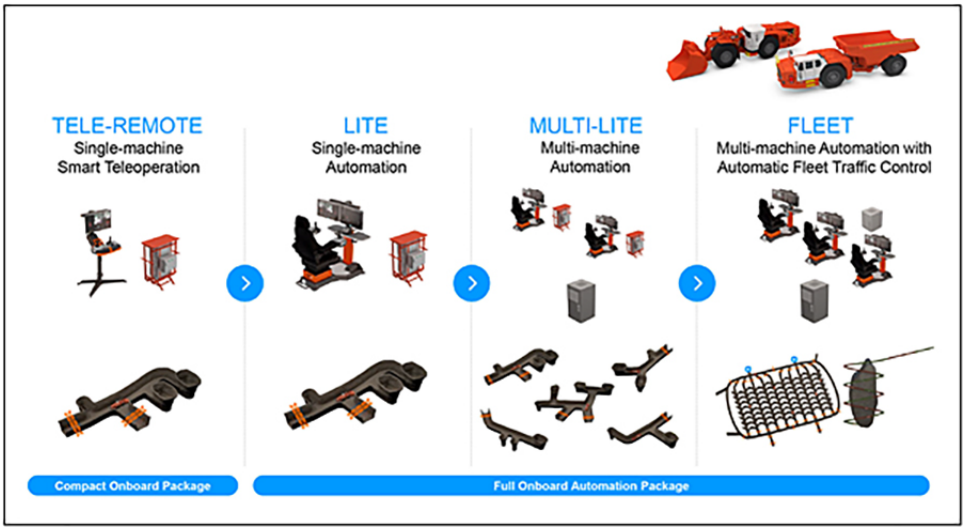
Advantages of Autonomous / Semi-Autonomous Mining Operations

- **Higher Operational Efficiency:** Programmed loader and truck cycles enable fast, precise operation that is controlled within equipment limitations. Bottlenecks are reduced for material handling, cycle times, and productivity.
- **24 x 7 Operations:** Ore extraction can proceed in round-the-clock shifts with minimal transition time, thereby dramatically improving productivity and daily output.
- **Improved Worker Safety:** Improvements in worker safety and health are realized by connecting autonomous vehicles, and other equipment, which can be operated remotely from a safe location with no risk to workers.
- **Improved Mine Safety:** Fewer workers are required in underground areas. Depending on the level of automation, these workers could be limited to maintenance and other general functions.
- **Improved equipment utilization:** Vehicle automation provides more detailed telemetry on vehicle health and status, thereby facilitating predictive and better preventive maintenance scheduling and lower risk of incidents and abuse. Vehicle automation increases productivity and decreases vehicle maintenance costs.
- **Ability to attract tech-savvy young talent pool**: Embracing technology has the added benefit of helping mining operations attract a new generation of tech-savvy talent by moving labor-intensive jobs out of the mine and into remote control centers. Fewer risks and safer conditions expand the pool of candidates to operate underground vehicles.

Sandvik AutoMine

The AutoMine® product family allows customers to scale up automation at their own pace. AutoMine® covers all aspects of automation, from remote and autonomous operation of a single piece of equipment, to multi-machine control and full-fleet automation using automatic mission and traffic control capabilities.

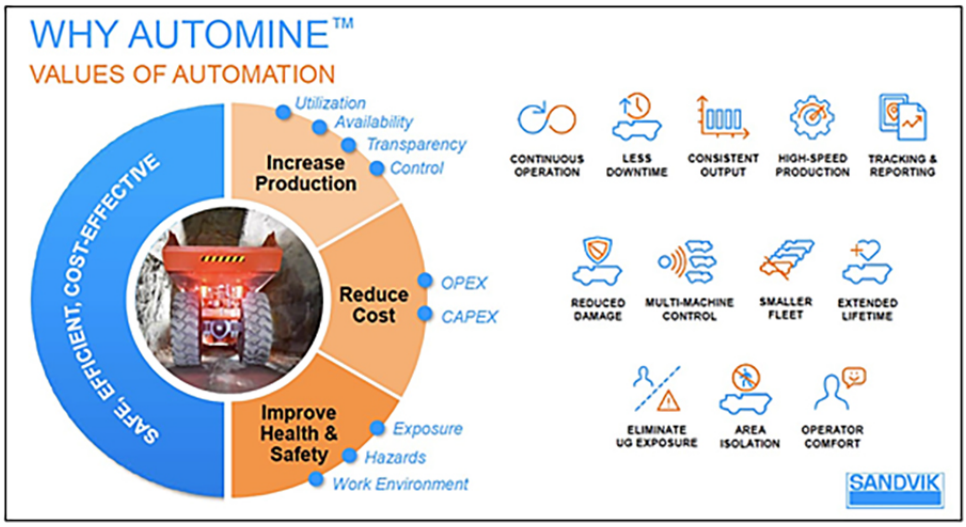
Figure 4 Sandvik AutoMine Product Family



The product family consists of three different level solutions:

- **AutoMine® Tele-Remote** is the entry-level solution that provides a new and easy way to explore the full potential of automated Sandvik equipment while achieving the benefits of increased productivity, safety, and cost efficiency in mining operations. It provides functionality for the teleoperation and monitoring of a single loader or truck. It is easy to set up, operate, and maintain without advanced technical skills.
- **AutoMine® Lite** is an automation system for a single Sandvik loader or truck, including both optimized route-based automation and intelligent teleoperation with operator-assisting automatic steering. The solution provides an easy way to start exploring the full potential of Sandvik equipment automation and achieve benefits of increased productivity, safety, and cost efficiency in mining operations.
- **AutoMine® Multi-Lite** is an automation system, which enables each system operator to remotely control and simultaneously supervise multiple automated Sandvik underground loaders and trucks. With AutoMine® Multi-Lite, each piece of equipment completes automated missions in its own dedicated production area. In addition, AutoMine® Multi-Lite 2 includes intelligent teleoperation with operator-assisting automatic steering.

Figure 5 Sandvik AutoMine Value Proposition



Sandvik AutoMine Network Requirements

The table below highlights some of the high-level requirements for the Sandvik AutoMine solution supporting autonomous vehicles within the underground mining space.

Table 1 High-Level Network Requirements for Sandvik AutoMine

Category	Overall (Wired + Wireless) Requirements
General	Compatibility with IPv4 (Internet Communication Protocol) IEEE802.11g/n (2.4 GHz Wi-Fi) with turbo roaming. LTE minimum 10MHz wide channel.
Bandwidth	Dedicated bandwidth for the system (i.e. no other traffic is allowed in the system network segment, when it is operational) Min. 10 Mbps upstream for each Load Haul Dump (LHD). Actual bandwidth using TCP traffic. Min. 500 Kbps upstream for each access barrier.
Latency (Packet Transfer Delay)	Max. 250ms at all times in total between any two system components including both wired and wireless networks with handovers. This latency must be measured in the uplink direction while it is loaded with video stream traffic. Latency testing must be performed while network uplinks are transmitting typical video loads.
Jitter (Packet Transfer Delay Variation)	Only a small variance of 20ms is allowed in the packet transfer delay in order to be able to receive a constant video stream without interference.

Table 2 ACS 3.0 Network Requirements

Category	Requirements
Network Protocol	■ SafeEthernet protocol based upon the IEEE 802.3 standard. ■ Communication between the PLC and the DIO uses UDP/6010. ■ Polling packets are 170-250 bytes in size, transmitted every polling cycle. ■ Polling cycle duration is adjustable between 10-20ms.
IP Addressing	Use static IP-addressing for ACS system components, DIO-modules, and PLCs in the control room and X-OPC server installed in the MultiLite server.
Network Layout	In accordance with the generally accepted regulations for developing Ethernet networks, no network loops may occur. Data packets may only reach a controller over a single path.
Worst-Case Reaction Time for ACS System	An application response time of 1200ms before a safety event is triggered.

Network Latency	Roundtrip transmission delay from the Fleet PLC to the onboard DIO and back should be < 250ms.
Network Configuration	VLAN segmentation is not needed for a standard ACS deployment. The system does not require Layer-2 connectivity. Usually the system is setup on a single subnet for Wi-Fi use, but there is no requirement around Layer-2. Layer-3 can be used, however, the address plan must be approved by Sandvik. The communications system should have capabilities for fine-tuning the wireless network configuration and provide tools for adjusting wireless parameters such as radio channels, transmit power, etc.

AutoMine Network

AutoMine® requires a Layer 3 IPv4 connection from the control room to the loader computers and cameras. This is facilitated by the Cisco mine network that consists of the components shown in the table below.

Table 3 Cisco Network Components

Component	Role	Version
Cisco 3504 / Cisco 5520	Cisco AireOS Wireless LAN Controller (WLC)	AireOS 8.10.122
Cisco 1572	Mine Infrastructure AP (End-of-Sale 11/20 – Supported for existing Brownfield Deployments)	AireOS 8.10.122
Cisco IW3702	Mine Infrastructure AP	AireOS 8.10.122
Cisco IW3702	Autonomous Vehicle Work Group Bridge	Autonomous AP Software 15.3.3-JK2
Cisco AIR-ANT2568VG-N	Cisco 1572 Dual-band Omni-directional Antenna. 4 antennas recommended per AP for maximum omni performance	N/A
Cisco IE 4000	Mine Infrastructure Switch with Fiber ports	IOS 15.2(4)EA9, RELEASE SOFTWARE (fc2)
Cisco Catalyst 9300	Control Room Distribution Layer Switch	IOS-XE 17.1.1
Cisco Catalyst 9500	Control Room Distribution/Core Layer Switch	IOS-XE 17.1.1
CX RF Site Survey Services	Cisco Professional Services for Mine RF Site Survey and post-deployment RF-Tuning	-N/A-

Table 4 3rd-Party Network Components

Component	Role	Model
Mobile Mark Antenna for IW3702 WGB	Vibration Resistant Antennas for the Cisco IW3702 WGB mounted on the Autonomous Vehicle	RM3-2400 Heavy Duty Surface Mount Antenna Frequency: 2.4-2.5 GHz Gain: 5 dBi https://www.mobilemark.com/product/rm3-2400/

Note: The referenced and validated Mobile Mark Antenna is just one of the options of a Vibration Resistant antenna that might be mounted on the vehicle. There are other options available. Please refer to the actual antenna make and model installed on your vehicles and adjust the antenna configuration and gain accordingly.

Figure 6 Mobile Mark 2.4 GHz Vibration Resistant Antennas

Cisco IE 4000 switches are connected via fiber-optic cables at various points in the mine tunnels to provide network connectivity for wireless access points and safety access barriers. The IE 4000 switches are connected utilizing Gigabit Ethernet SFP ports. The number of IE 4000 switches in the chain should take into account the total bandwidth required to service the number of loaders in operation on that section (based on roughly 10Mb/s bandwidth requirement per vehicle).

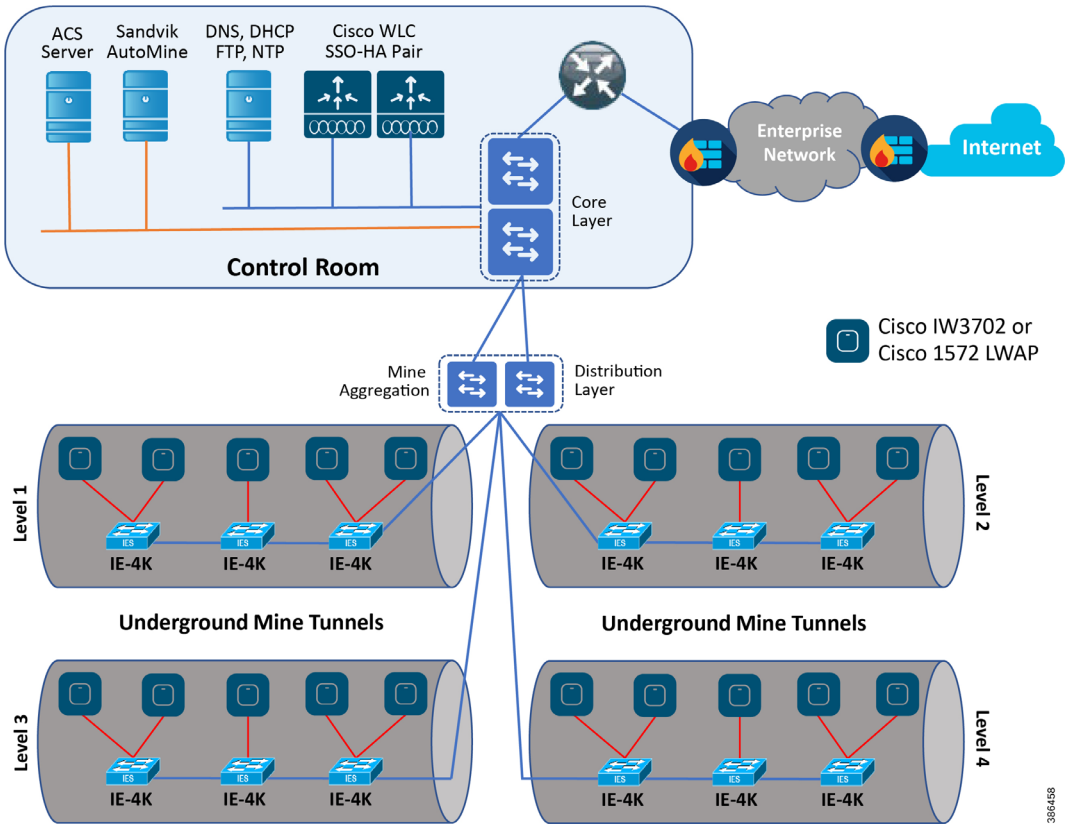
The pre-dominant wired access topologies within an underground mine are a Cisco Resilient Ether Protocol (REP) ring or a Hub-n-Spoke (Star) topology.

Note: The design, deployment and validation of an IE 4000 REP ring or Star topology is out of scope for this version of the Mining CVD.

A protective cabinet with suitable power and cable entry/exit protection houses each IE 4000 switch. Cisco 1572 or Cisco IW3702 Access Points are wall or ceiling mounted along the mine tunnels and connect to the IE 4000 switch via a single X-code M12 Copper Ethernet cable (max. distance 100 Meters). This connection to the IE 4000 switch provides both power (IEEE802.3af POE+) and a Gigabit Ethernet connection.

Two StackWise® Cisco Catalyst 9300 switches provide the distribution/aggregation layer for the IE 4000 switches in the mine network. These are installed in the control room or at a data center. The AutoMine® server rack top-of-the-rack switch in the control room would be connected to this aggregation layer.

Figure 7 Underground Mine – Sandvik AutoMine – Network Topology



Mine Network Security

- The 2.4Ghz Wi-Fi network shall use WPA2-PSK at a minimum to secure the air interface.
- TACACS+ can be used to provide central authentication/authorization for network device access.
- Access to all web-based interfaces should be configured for HTTPS only.
- Switch ports should be secured where appropriate with Port Security restricting MAC address per port or using MAC Bypass with a RADIUS server to authenticate devices connecting to the network.
- Filter untrusted DHCP addresses (enable DHCP snooping on all operational ports).
- Unused switch ports should be in a shutdown state and placed into an unused VLAN.
- Enable BPDU Guard on all access ports.

WLAN security (WPA2-PSK verified today) increases Wi-Fi network handover times as compared to an open network, but it has handover times which are acceptable for the Sandvik AutoMine application needs and should be used to secure the Wi-Fi network rather than deploying an open network.

Without WLAN security, handovers require only two Ethernet frames to be sent, but with WLAN security, eight packets are required. Handover times are usually between 30-40ms without security enabled and between 40-60ms with security enabled. This is acceptable for normal equipment operation; therefore, disabling WLAN security is not recommended.

Additional WLAN controls exist to increase wireless network security if needed. The network can be configured so that only pre-defined WLAN client MAC-addresses can connect to an access point, for example. This means that a particular WLAN client cannot associate to any of the access points if that WLAN client's MAC-address is not on the pre-defined MAC list.

Wireless Design and Deployment for Underground Mining

The rapid development of industrial and communications technology in recent years have been of great benefit to mining activities. Companies are rapidly deploying new tools and applications to gain the associated productivity and financial benefits. However, they face a key challenge in that they require the appropriate network infrastructure to support reliable high-speed data communications technology in the mining environment, particularly underground mines.

Many new technologies developed and sold by vendors requires high-speed digital networks to manage the increasing volumes of data generated within the mining environment. With a converged network infrastructure, industrial control and mining solution vendors are moving towards a single standardized, consolidated communications infrastructure based on digital Ethernet (transmission control protocol/internet protocol or TCP/IP) network framework - or at least are developing communications interfaces to allow their devices to interconnect with this type of network - in mine sites to improve production and cost optimization. This allows mining companies to run multiple services over a single network backbone, thereby improving management while lowering deployment and support costs. The rapid shift from traditional, legacy analog systems to high-speed digital networks has created a lag in the knowledge and experience that is required to properly plan, design, deploy, and maintain such systems.

This version of the Mining CVD specifically focuses on the wireless design and deployment aspects around support for the Sandvik AutoMine and OptiMine solutions providing automation from tele-remote or autonomous operation of single pieces of equipment to multi-machine control and full fleet automation with automatic mission and traffic control capability within the Underground Mining space.

Communication infrastructure is becoming an increasingly vital component of efficient and productive underground mining operations, but the constantly changing nature of a mine, the highly mobile fleet, and the inherent environmental challenges may present a hurdle.

Mining operations are extremely hazardous and take place in unpredictable environments. In fact, mining operations are always in a state of change, with frequent expansions and changes to the site and internal passageways.

The requirement for a reliable wireless network is especially true but also particularly difficult for ‘last mile’ connectivity, the area where installed infrastructure ends, and the active/dynamic mining area starts. Much of the critical data necessary for safety, productivity, and asset health improvements originates in this area.

Cisco Connected Mine Architecture

The Cisco Connected Mine Architecture depicted in the figure below follows the Purdue model of Control Hierarchy and maps to the various levels defined there-in. It also aligns well with and build upon the overall Cisco Industrial Automation architecture.

The Enterprise Zone is managed by IT personnel and houses the enterprise applications, collaboration servers, ERP, MES etc. This is the layer that also provides connectivity to the Internet and the public cloud. Ingress and egress to the Internet is controlled by a layer of Enterprise Firewalls. These firewalls can also provide remote-access connectivity for remote-workers.

The Industrial Demilitarized Zone (IDMZ) layer sits between the Enterprise Zone and the Mine Control Zone. The role of the IDMZ is to provide strict segmentation between the IT and OT operational domains. The IDMZ also houses things like patch management servers, terminal servers, remote-access servers, mirrored servers, data-shares, anti-virus and anti-malware servers, certain application servers.

A redundant layer of firewalls control access into and out of the Mine Control Zone. Intrusion Prevention Services (IPS) and Intrusion Detection Services (IDS) can also be deployed here.

The core layer is the network backbone that hierarchically aggregates the distribution layer of the mine network and provides connectivity to data center components. The core layer also providing intelligent switching, routing, network access policy functions, QoS services, and high availability through redundant core layer switches. The core network is designed to be highly reliable and stable to inter-connect all the elements in the operational plant. It typically consists of Layer 3 devices, with high speed connectivity, redundant links, and redundant hardware interconnecting the operational domains over wide-geographic areas. Within the context of the mine architecture, the core aggregates traffic from all of the operational domain zones and provides access to the industrial DMZ, centralized Networking and Security services sitewide applications and enterprise WAN for connectivity for offsite functions such as the Remote Operations Center (ROC). The core applies segmentation techniques to keep the domains separated, typically extending the VPN segmentation from the ROC and WAN into the OT operational domains. Any cross pollination of traffic between the domains must be considered as the core layer provides policy-based connectivity between the functional operational domains.

At the distribution layer in the architecture, the wired mining architecture is closely 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 (collapsed core), where it may also provide site or plantwide connectivity.

The distribution switches are generally housed within environmentally controlled environments such as control rooms which are more aligned with traditional enterprise switching unless certain industrial protocols are required such as in power networks, then Industrial Ethernet switches may be used at this layer. These switches provide the networking interface at the Level 2 and 3 within the Purdue Model and in smaller plants may be collapsed into the Level 3 function of a collapsed core distribution deployment.

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

The distribution layer interfaces between the access layer and the core layer to provide many key functions, including:

- Aggregating access layer switches.
- Providing intelligent switching, routing, and network access policy functions to access the rest of the network.
- Providing high availability through redundant distribution layer switches and equal cost paths to the core, as well as providing differentiated QoS services to various classes of service applications at the distribution layer.

The distribution layer needs to be deployed within an environmentally controlled location, such as an above ground control room. Distribution layer equipment is typically placed in the proximity of the underground mine entrance.

In case of Underground Mining, the Mine Control Zone typically maps to the Remote Operation Centers built above ground to help centralize monitoring and controls of mines without having to put people in harms' way at the mines, hence improving safety. The more functions that can be performed in the ROC results in increased operational efficiency and effectiveness while improving safety. For example, the adoption of remote control and autonomous equipment operations provides the ability to have highly reliable mining operations while minimizing potential for human errors. This can dramatically decrease the number of safety incidents involving the mobile fleet and allows for a smaller number of operators to manage a larger fleet at much lower cost.

The Underground Mining Zone consists of fiber-connected Cisco IE 4000 switches forming a REP ring or Star topology. A given REP ring can traverse a very large geographical area within a large mine. Cisco infrastructure APs hang off the IE 4000 switches providing underground wireless connectivity for applications like autonomous vehicles, video-surveillance, worker mobility, Asset Tracking, etc.

This version of the Mining 1.5 CRD only focuses on the underground wireless deployment. Design and deployment of the REP ring or Star access/distribution layer, core layer, the IDMZ and Enterprise zones is outside the scope of this version of the CRD, but can be referenced within the Mining 1.0 CRD and the Industrial Automation Networking and Security CVD.

Figure 8 Cisco Connected Mine Reference Architecture - REP Ring Deployment

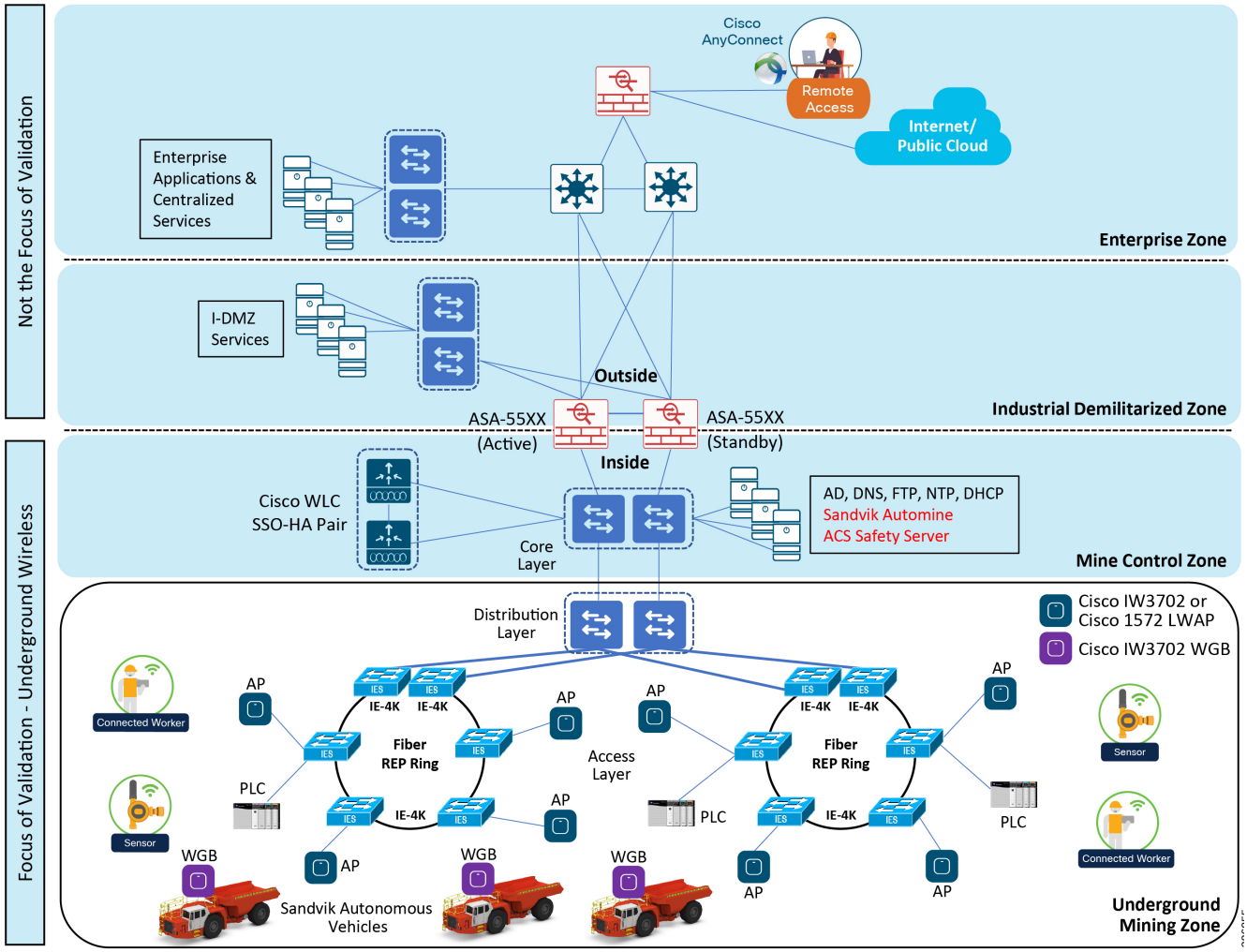
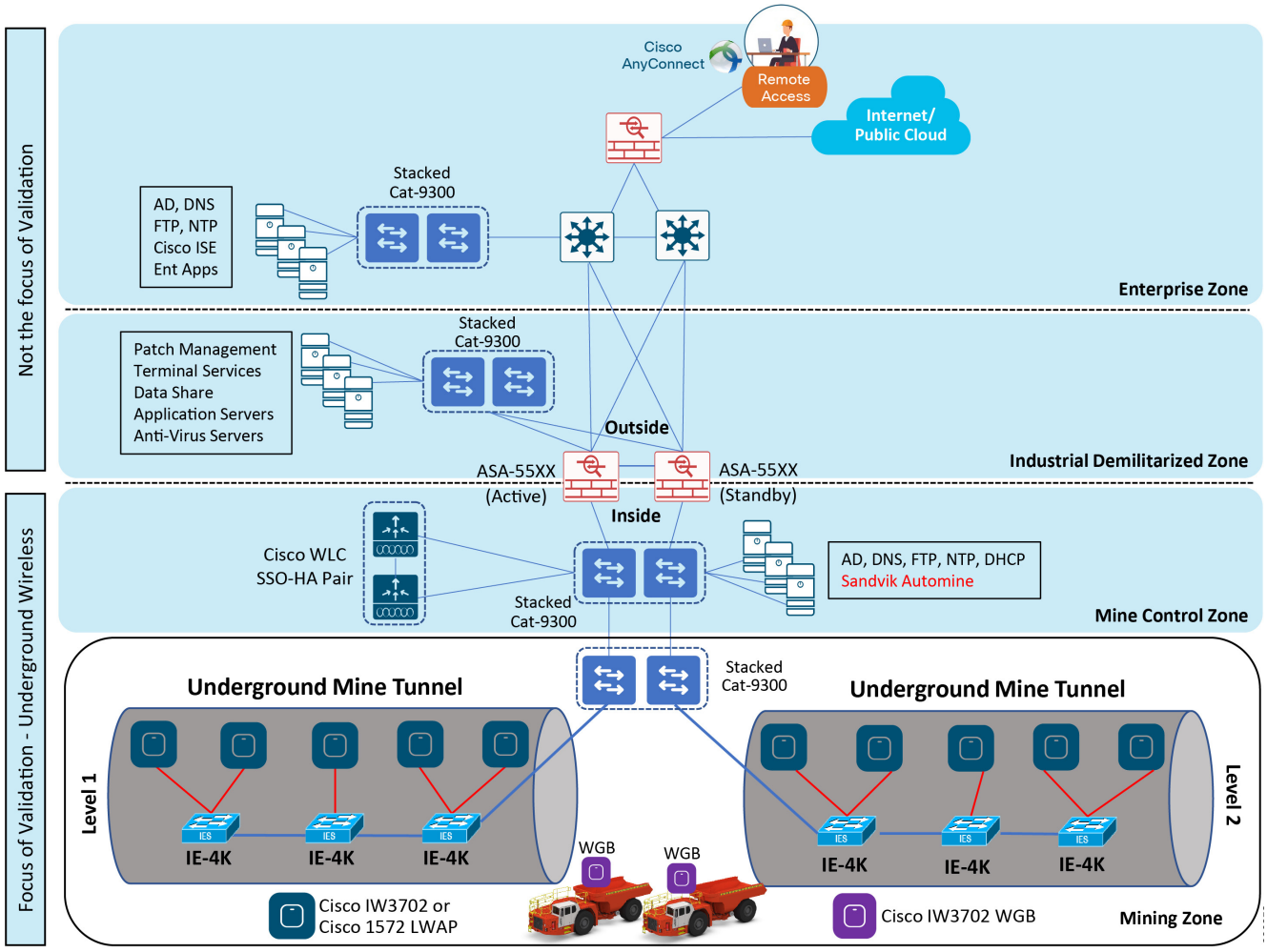


Figure 9 Cisco Connected Mine Architecture - Hub-n-Spoke/Star Deployment



Cisco Network Components

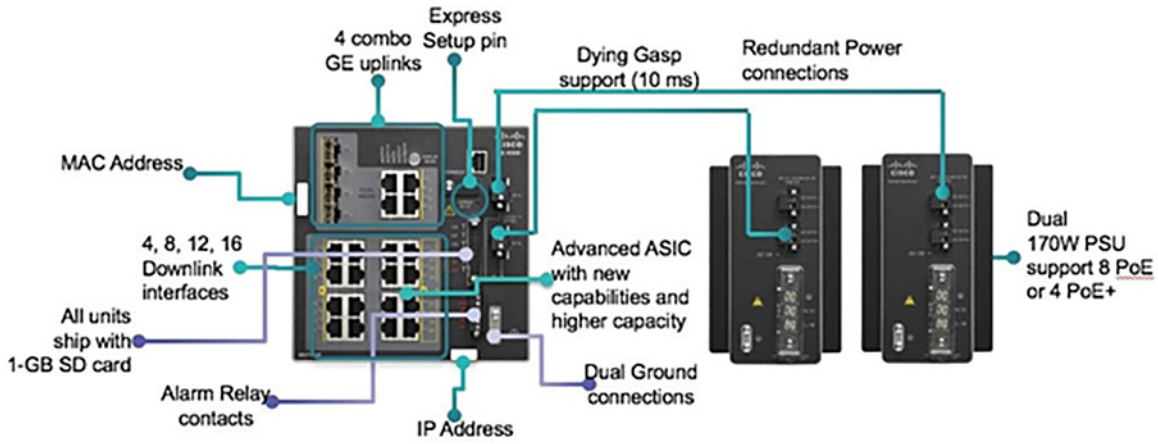
Cisco IE 4000 Industrial Ethernet Switch

Figure 10 Cisco IE 4000 Industrial Ethernet Switch

- Ruggedized: Compliant for utility and manufacturing deployments
- High MTBF: No moving parts, dual DC inputs, and swap drive
- Scales with large Layer 2 and 3 forwarding tables
- Advanced IP routing features for aggregation deployments
- High performance: All packet forwarding in hardware
- Advanced QoS and security features performed in hardware for deterministic behavior (MQC)
- Network Address Translation (NAT)
- DIN rail mount
- 4 Gigabit Ethernet combo (SFP and copper) uplinks in every model
- PoE and POE+ ports (model dependent)
- SD card backup and external storage
- 2 dry-contact alarm inputs and 1 output alarm for temperature, power, and storage

IE 4000 Datasheet:
https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-4000-series-switches/datasheet-c78-733058.html

Figure 11 Cisco IE 4000 Power Configuration Options



AC-to-DC PSU 54V DC Power Supply

- Part number: PWR-IE170W-PC-AC=
- Nominal AC input: 100 to 240V, 2.3A, and 50 to 60 Hz
- Supported AC input: 90 to 264V AC
- Nominal DC input: 125 to 250V DC
- Supported DC input: 106 to 300V DC W x H x D: 3.4 x 5.8 x 5.2 in.
- Fixed output: 54V DC and 3.15A Weight: 1.76 kg

Figure 12 AC-to-DC PSU 54V DC Power Supply

Cisco IW3702 Industrial Access Point

Industrial Wireless Access Point with speeds up to 1.3 Gbps with 802.11ac wave 1 support.

- Extremely rugged IP67-rated housing to protect against liquid and dust ingress compliant to EN 60529 standard
- Capable of operating in temperatures from -50 C to +75 C (-40 C for cold start)
- Vibration rated for Transportation and Mining applications

- M12 Ethernet and DC power connectors for vibration and shock resistance
- Versatile RF coverage with external N-type antenna connectors
- Range of 10 V DC to 60 V DC power input in addition to PoE/PoE+ to support a wide variety of power sources

Datasheet:
https://www.cisco.com/c/en/us/products/collateral/wireless/industrial-wireless-3700-series/datasheet-c78-734968.html

Figure 13 Cisco IW3702 Enclosure and Connectors

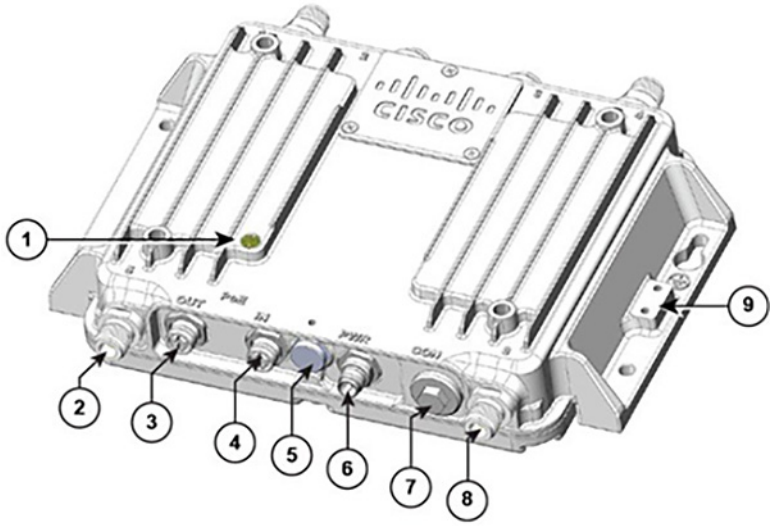
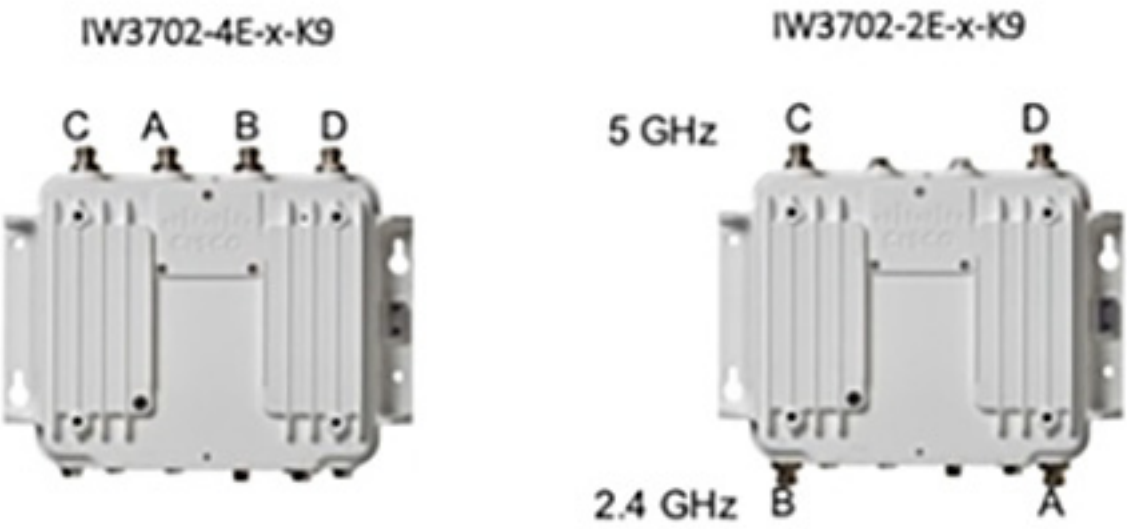


Figure 14 Cisco IW3702 Enclosure and Connectors



Cisco 1572 Industrial Access Point

Important Note: The 1572 Outdoor AP will be End-of-Sale in 11/2020. For new underground mining deployments we recommend using IW3702 Infrastructure APs. However, if you currently have an existing underground wireless deployment consisting of 1572 Infrastructure APs, the solution has been validated to work with it.

Figure 15 Cisco 1572 Outdoor AP

Cisco Wireless LAN Controllers (WLC)

Cisco Wireless LAN Controllers provides centralized control, management, and troubleshooting for wireless deployments. The WLAN controller provides the lightweight AP its configuration and also functions as a switch for all the wireless traffic. The WLAN controller also consolidated management for the entire wireless network in one place. WLAN controllers are physical devices that are rack mounted in the core data room and communicate with each AP at the same time. This allows for quick and easy configuration of multiple APs without having to manually configure each and every one.

It also eliminates the need to re-architect the wired network to host a WLAN. As you might assume, scalability is greatly improved by the addition of a WLAN controller as it easily allows the installation of more APs onto the network and reduces deployment and management complexities.

We recommend deploying a pair of Cisco 3504 WLCs for small to medium-sized deployments (up to 150 APs and 3,000 clients), and a pair of Cisco 5520 WLCs for larger deployments (up to 1500 APs and 20,000 clients).

Figure 16 Cisco 3504 Wireless LAN Controller

Datasheet:
https://www.cisco.com/c/en/us/products/collateral/wireless/3504-wireless-controller/datasheet-c78-738484.html

Figure 17 Cisco 5520 Wireless LAN Controller

Datasheet:
https://www.cisco.com/c/en/us/products/collateral/wireless/5520-wireless-controller/datasheet-c78-734257.html

Cisco Catalyst 9300 Access Layer Switch

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

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

Note: The embedded WLC within the 9300 has not been validated and is not supported as part of the solution.

Figure 18 Cisco Catalyst 9300 Access Layer Switch

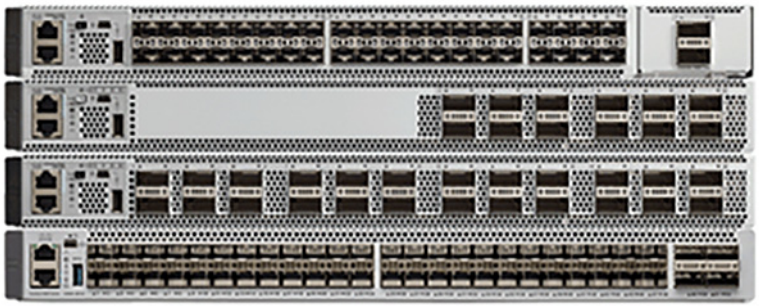
Datasheet and switch model selector:
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

Catalyst 9500 Distribution/Core Layer Switch

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

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

Figure 19 Cisco Catalyst 9500 Distribution/Core Layer Switch



Datasheet and switch model selector:
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html

Cisco IW3702 WGB Wi-Fi Client On-board Vehicle

A Work Group Bridge (WGB) is an access point (AP) that is configured to act as a wireless client towards the wireless infrastructure, with the goal of providing Layer-2 connectivity for the devices connected to its Ethernet interface. For our underground mining autonomous vehicle use-case, the WGB is installed on the vehicle to provide network connectivity to devices such as Cameras, IO devices, PLCs which are present on-board the vehicle. These devices need connectivity back to the Automine platform located in a centralized control room.

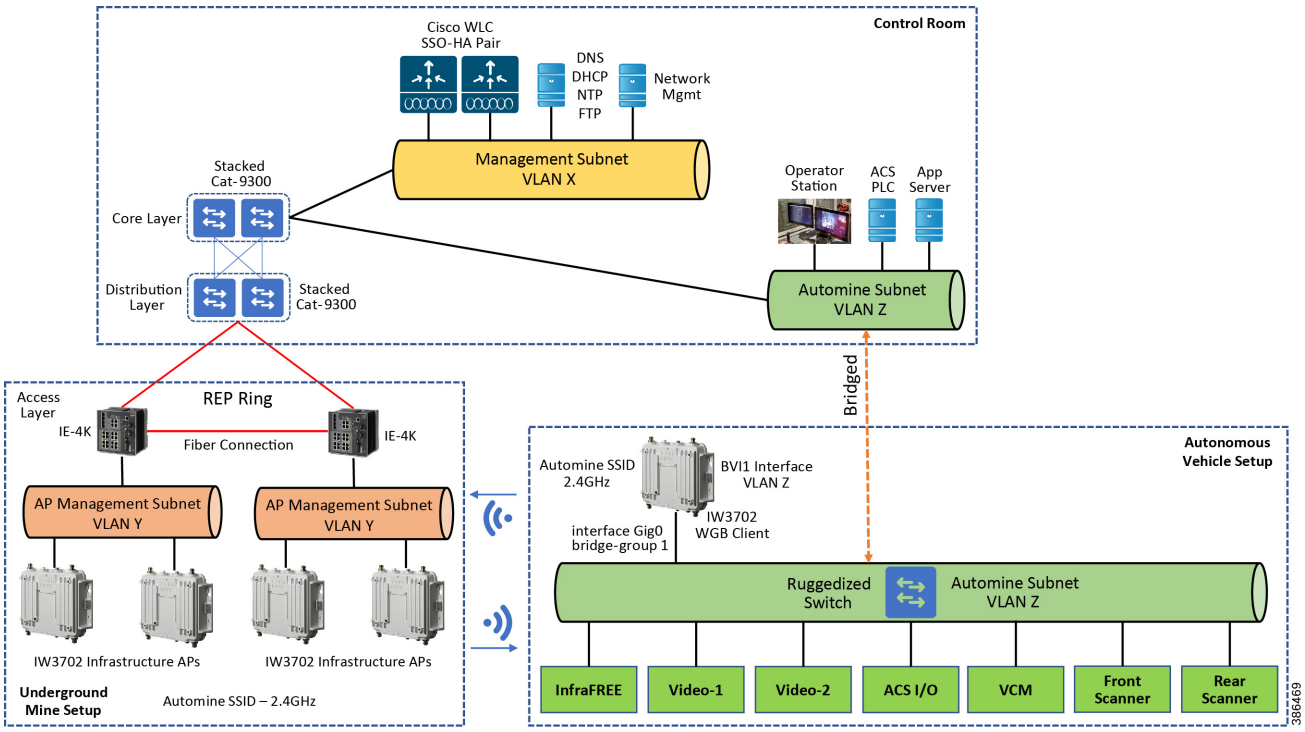
Note: Where more than one client Ethernet device exists behind the WGB and Industrial Ethernet switch will be required. The various clients can then be connected to the Industrial Ethernet switch, and the Industrial Ethernet switch is then connected to the Ethernet port of the WGB. For the Sandvik AutoMine use-case, there are multiple devices that need connectivity on the Autonomous vehicle, hence there is a need for an Industrial Ethernet switch on the vehicle.

Chapter 3: Wireless Design for Underground Mines deploying Sandvik Autonomous Vehicles

This chapter highlights the design considerations and best-practice deployment guidelines for implementing a wireless infrastructure within underground mines in support of the Sandvik AutoMine platform for autonomous vehicles.

Sandvik AutoMine Logical Network Design

Figure 20 Sandvik AutoMine Logical Network Design



The Sandvik AutoMine logical network is comprised of three areas:

- Control Room which houses the following components:
  - Automine Operator Stations
  - ACS Safety System and PLC
  - Cisco WLC SSO-HA Pair
  - Infrastructure Services: DNS, DHCP, NTP, FTP
  - Core Layer Switches
  - Mine Aggregation Distribution Layer Switches
- Underground Mine Area:
  - Cisco IE 4000 ruggedized switches
  - Cisco IW3702 infrastructure APs

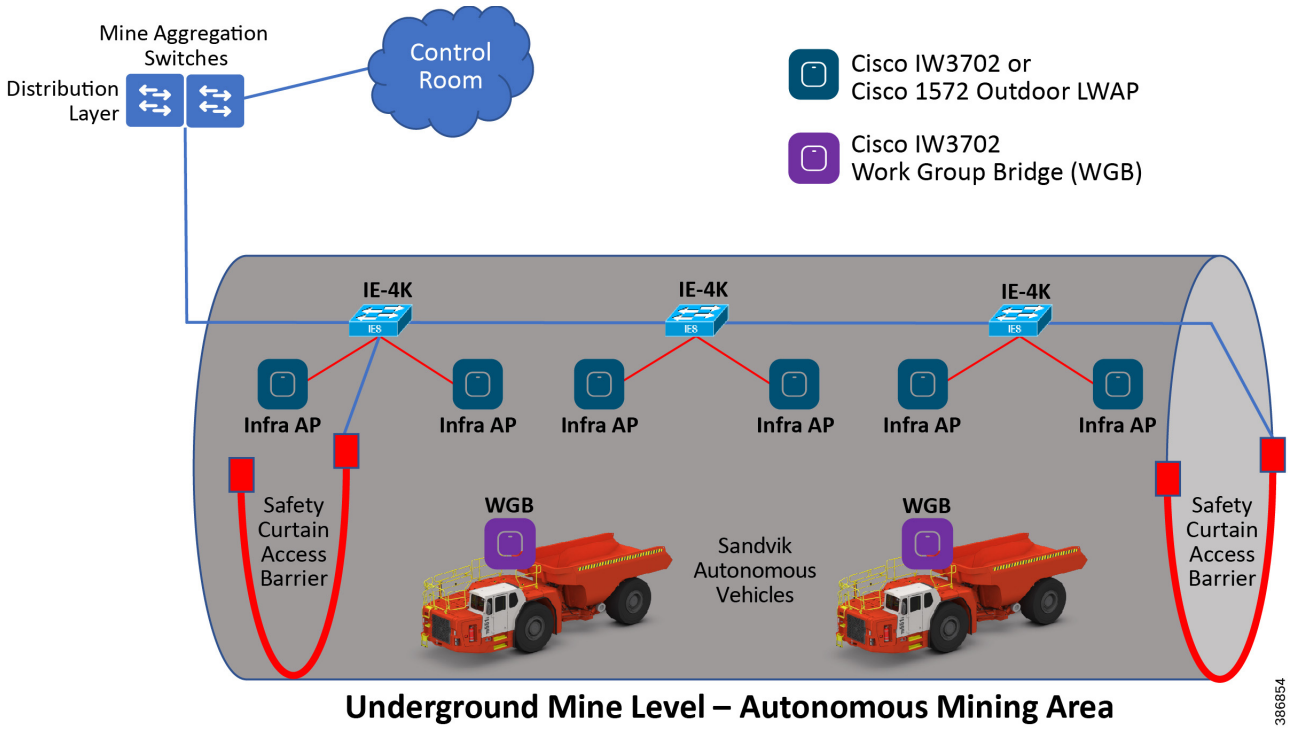
  - Sandvik ACS Safety Curtains

- Autonomous Vehicle Setup:
  - Cisco WGB Client
  - Ruggedized Switch
  - Sandvik AutoMine Components

The Sandvik AutoMine logical network uses three VLANs/subnets:

- Network Management Subnet (VLAN X) – Used for deploying Cisco WLCs, Network Management Servers, Servers hosting infrastructure services such as DNS, DHCP, NTP and FTP.
- AP Management Subnet (VLAN Y) – Used for communication between WLCs and APs.
- Automine Subnet (VLAN Z) – Used for deploying Sandvik AutoMine components such as Operator Stations, ACS Safety Servers, etc. within the Control Room and the components on-board the vehicle such as cameras, I/O devices, sensors etc. This subnet is also used to provide wired network connectivity to the ACS Safety Curtains.

Figure 21 Example Level within an Underground Mine



Distance between Operator Station/Control Room and Production Area – Available Options:

- Standard Ethernet copper: up to 90 meters with an individual cable.
- Multi-mode fiber optic: up to 2 kilometers with an individual cable.
- Single-mode fiber optic: up to 10 kilometers with an individual cable.
- Any distance with an external network that provides sufficient data transfer speed and capacity.

Wired Access Layer

The Cisco IE 4000 ruggedized switches form the wired access layer within an underground mining environment. The IE 4000s are typically connected to each other using fiber optic cables due to the large distances that need to be traversed within a mine. A typical deployment used to interconnect the IE4000 access layer switches with each other and the distribution layer within an underground mining environment is either a REP ring or a Star (Hub-n-Spoke) topology.

The IE 4000 switches are housed within a pre-fabricated industrial grade housing and are deployed at regular intervals within the underground mine. The IE 4000 switches have PoE ports which are used to provide power to the IW3702 Infrastructure APs within the mine. The APs utilize the Layer-2 Cisco Discovery Protocol (CDP) feature to negotiate the power draw from the IE 4000 switchport.

The IE 4000 switches also provide wired network connectivity to each of the ACS Safety barriers/curtains at each of the entry/exit points within the autonomous operations area within the underground mine.

Note: The design and deployment of a REP ring or Star topology is outside the scope of this document. Please refer to the Industrial Automation CVD for design and implementation guidance around REP ring or Star deployment.

Wireless Access Layer

The Cisco IW3702 industrial grade APs are deployed throughout the underground mine to provide pervasive wireless coverage. The IW3702 Infrastructure APs hang off the PoE port of the Cisco IE 4000 switches and provide wireless access within the underground mine. The IW3702 infrastructure APs operate as Lightweight APs (LWAP) which are registered and managed centrally using a redundant pair of Cisco 3504/5520 Wireless LAN Controllers (WLCs) located within the control room.

Two deployment modes are found within the wireless access layer in underground mines:

- Standard non-mesh topology where-in each of the LWAPs are wired connected to the IE 4000 switches.
- Mesh deployment where-in a subset (RAPs) of the LWAPs are wired connected to the IE 4000 switches and the remaining (MAPs) LWAPs are connected to the wired network using a wireless backhaul to the RAPs.

Note: This version of the CVD focuses on the non-mesh wireless deployment.

Each of the IW3702 LWAPs form a secure CAPWAP tunnel back to the active WLC in the control room. All traffic to/from the wireless clients is encapsulated and carried within the CAPWAP tunnel. The WLC then de-encapsulates this traffic and offloads it to the appropriate VLAN on the wired network.

For our specific use-case, the IW3702 LWAPs advertise the “Automine SSID” within the underground mine. This is the SSID which the Cisco WGB client installed on each of the autonomous vehicles connects to. This SSID is configured to use pre-shared key (WPA2-PSK) authentication along with AES encryption.

Distribution Layer

The distribution layer facilitates connectivity between the access layer and other services. The distribution layer switches are generally housed in controlled environments such as control rooms so may be more aligned with traditional enterprise switching unless certain industrial protocols are required, then Industrial Ethernet switches may be used at this layer. For this design, distribution layer functionality is provided by a redundant pair of Cat-9500 switches. This layer is also known as the mine aggregation layer as it consolidates traffic from various access layer domains. The distribution layer switches also participate within the formation of the REP ring topology along with the IE 4000 switches at the access layer. Within a Star (Hub-n-Spoke) topology the Distribution Layer switches act as the Hub and central aggregation point for traffic coming from the interconnected IE4000 switches deployed within various spokes.Northbound, the distribution layer switches are connected to the pair of core layer switches.

Core Layer

The core layer functionality is provided by a redundant pair of Cat-9500 switches. Southbound the core layer switches are connected to the pair of distribution layer switches. The redundant pair of Cat-9500 switches can either be co-located or geographically separated if geographical redundancy is required within the mine network deployment. The Catalyst 9500 SVL option provides for a superior High Availability design as described below. In smaller plants the distribution and core layer can converge onto the same platform (collapsed core), where it may also provide site or plant wide connectivity.

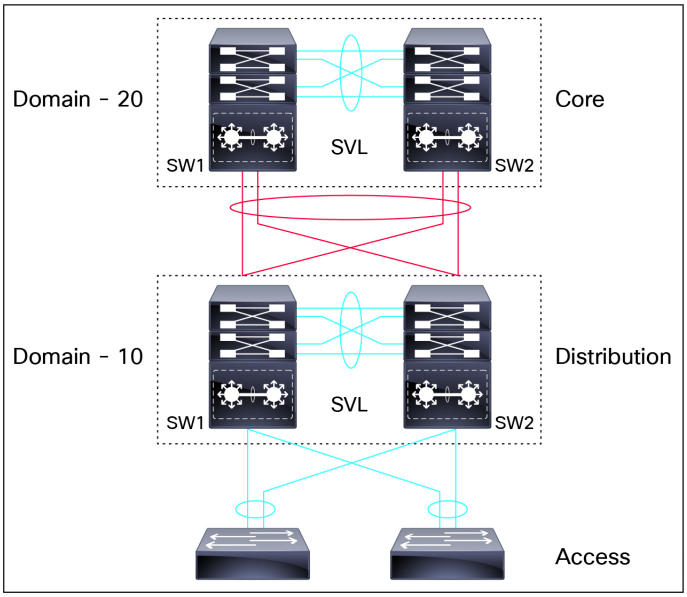
Catalyst-9500 StackWise Virtual High-Availability

Cisco StackWise Virtual is a two-node solution providing a Unified Control Plane Architecture by assigning one switch as active and the other as a hot-standby. Both the switches play an active role when it comes to data forwarding. Two Cat-9500 switches are connected together using a StackWise Virtual Link (SVL). The SVL helps bring the two switches together forming a single logical switch. Both the switches can be managed as a single entity. Since the control plane, management plane, and data plane are integrated, the system behaves as a single switch.

The virtualization of multiple physical switches into a single logical switch is from a control and management plane perspective only. Because of the control plane being common, it may look like a single logical entity to peer switches. The data plane of the switches is distributed. Each switch is capable of forwarding over its local interfaces without involving other members. However, when a packet coming into a switch has to be forwarded over a different member's port, the forwarding context of the packet is carried over to the destination switch after ingress processing is performed in the ingress switch. Egress processing is done only in the egress switch. This provides a uniform data plane behavior to the entire switch irrespective of whether the destination port is in a local switch or in a remote switch. However, the common control plane ensures that both the switches have an equivalent data plane entry for each forwarding entity.

An election mechanism elects one of the switches to be Cisco StackWise Virtual active and the other switch to be Cisco StackWise Virtual standby in terms of Control Plane functions. The active switch is responsible for all the management, bridging and routing protocols, and software data path. The standby switch is in a hot-standby state ready to take over the active role, if there is a failure on the active switch. This architecture supports stateful switchover redundancy. To guarantee that the hot-standby is always ready the switch configurations, forwarding and state information are synchronized from the active switch to the hot-standby switch. Any changes made to the StackWise Virtual active switch are immediately synchronized to the hot-standby switch. In the event of a switchover, the disruption to network traffic is minimal.

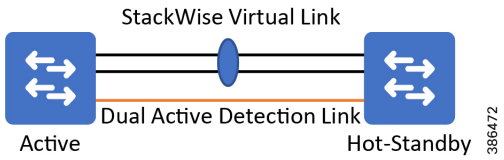
Figure 22 StackWise Virtual Architecture for Core and Distribution Layers



The StackWise Virtual architecture comprises three components:

- **StackWise Virtual Link (SVL)** - When a switch is powered up and the hardware is initialized, it looks for a configured StackWise Virtual link before the initialization of the control plane. This is because the SVL acts as a connector between the two switches helping unify the Control Plane. It helps combine both the switches to be in a single StackWise Virtual domain. The SVL carries all the control and data traffic between the active and hot-standby switch and typically consists of dual 10-G or 40-G physical links.
- **Dual-Active-Detection Link** - If the standby switch detects a complete loss of the StackWise Virtual link, it assumes the active switch has failed and will take over as the active switch. However, if the original Cisco StackWise Virtual active switch is still operational, both the switches will now be Cisco StackWise Virtual active switches. This situation is called a dual-active scenario. This scenario can have adverse effects on network stability because both the switches use the same IP addresses, SSH keys, and STP bridge IDs. Cisco StackWise Virtual detects a dual-active scenario and takes recovery action. Dual-active-detection link is the dedicated link used to mitigate this.
- **Multi-Chassis EtherChannel** - Multi-chassis EtherChannel (MEC) is an EtherChannel bundled with physical ports having common characteristics such as speed and duplex, that are distributed across each Cisco StackWise Virtual system. A Cisco StackWise Virtual MEC can connect to any network element that supports EtherChannel such as a host, server, router, or switch.

Figure 23 StackWise Virtual 2-node solution



- For the StackWise Virtual (SVL) Link, it is good to use two 10/40 GbE ports on separate ASICs for resilient connectivity.
- SVL Links should be point-to-point connections.
- It is recommended to use a dedicated link for Dual Active Detection.
- Make sure to dual attach all devices into the SVL Domain. This helps provide an alternate traffic path to/from the device.
- It is good to use LACP for the Port-Channels of MEC Member ports.

Hot Standby Redundancy Protocol (HSRP)

Hot Standby Redundancy Protocol (HSRP) is another alternative for redundancy at the distribution layer. HSRP provides high availability through redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router sends packets; the standby router takes over the routing duties when an active router fails or when pre-set conditions are met. HSRP deployed switches can help support the requirement for geographical diversity of redundant switches at the distribution layer.

RF Design

The “Automine SSID” WLAN uses the 2.4GHz spectrum and should be designed to use Wi-Fi channels 1, 6, 11 which are the only non-overlapping channels available in that range. The network should be designed so that adjacent access points are on different channels to avoid any kind of interference.

Wireless Coverage

- Coverage of an Access Point network must be according to Sandvik´s requirements.
- Coverage areas must overlap and signal quality must be good in every location where AutoMine system is used.
- Minimum required signal strength -55 dBm at all areas. In areas where handovers occur, both access points should be above the minimum required signal strength.
- No other systems should be using the 2.4GHz ISM spectrum in the area where AutoMine is to be deployed.
- The main goal when designing the wireless coverage for the AutoMine application is to provide adequate signal strength for wireless clients throughout the mine network and to be able to support the required data rate (10Mb/s per loader).

In addition, wireless cell size should be controlled to achieve desired number of clients per AP, and to minimize co-channel interference between cells:

- Determine the maximum number of wireless clients (loaders, etc.), including future expansion required.
- Identify redundancy requirements for coverage, for example, if two (or more) APs should be seen from any point to provide for failures.
- Perform a professional site survey to determine the number and locations of the APs that can cover the area with required level of redundancy. The site survey should also determine the appropriate antenna types and verify link performance and supported data rates.
- For details on how to perform an effective wireless site survey, please refer to “Chapter-4 Wireless Site Survey”.
- Design the wireless coverage to maintain the parameters listed in the table below.

Table 5 RF Network Parameters

Parameter	Recommended Value
RECEIVED SIGNAL STRENGTH INDICATOR (RSSI)	Min -55 dBm
SIGNAL-TO-NOISE RATIO (SNR)	Min 25 dB
SUPPORTED MINIMUM DATA RATE	10Mbps per Machine

- Configure transmit power manually for each device to provide adequate coverage.
- Change the transmit power from the maximum to reduce signal propagation outside the intended area and to minimize co-channel interference (CCI) on site.
- Use static channel allocation in the WLAN. Determine if wireless channels have to be reused based on spectrum availability. Channel allocation scheme should provide maximum distance separation between cells using the same channel.
- Do not reuse the channels for wireless cells operating with high utilization and high client count, unless complete signal separation can be achieved.
- If a channel is reused and CCI is expected, the available bandwidth is essentially shared between the wireless cells. The total packet rate should be calculated including every application using the channel.

WLC Configuration Considerations

Automine network SSIDs should be dedicated for Automine use only.

Automatic channel and transmit power assignment should be disabled. It's recommended to create a network plan and assign channels and power-levels manually to create a static and deterministic configuration.

Passive Client Mode

Passive client functionality must be activated on the SSID allocated for AutoMine use.

Passive clients are wireless devices, that are configured with a static IP-address. These clients do not transfer any IP information, such as IP-address, subnet mask or gateway information when they associate to a network. Cisco WLC normally uses broadcast optimization where ARP-requests are not broadcast to clients, but the WLC acts as an ARP proxy. This is a problem with the AutoMine system where components onboard vehicles have multiple unique IP-addresses. With the Passive Client functionality enabled on the AutoMine SSID, ARP requests are broadcast to the client.

Note: Passive clients feature is only supported when SSIDs and the WLC management interface are on different VLANs. Your network must support usage of VLANs and you must configure the WLC Management interface to be in different VLAN from where you terminate the SSID client traffic.

Note: GARP forwarding must to be enabled using the "**show advanced hotspot"** command.

FlexConnect vs Local-Mode APs

The recommendation of this solution is not to deploy APs in FlexConnect mode. All traffic is to and from the vehicle to the AutoMine system located in the Control Room and there is no vehicle-to-vehicle traffic. Due to this traffic pattern, no local traffic switching is required. Hence there is no necessity to deploy APs in FlexConnect mode. For Local-Mode APs, the wireless client traffic is transferred via a CAPWAP tunnel back to the centralized wireless lan controller.

SSO-HA Wireless Controller Redundancy

The WLC high availability architecture is box-to-box redundancy. In other words, this is a 1:1 pairing in which one WLC is in an active state and the other WLC is in a hot standby state, continuously monitoring the health of the Active WLC using a redundant port.

The redundancy port is used for configuration, operational data synchronization, and role negotiation between the primary and secondary controllers.

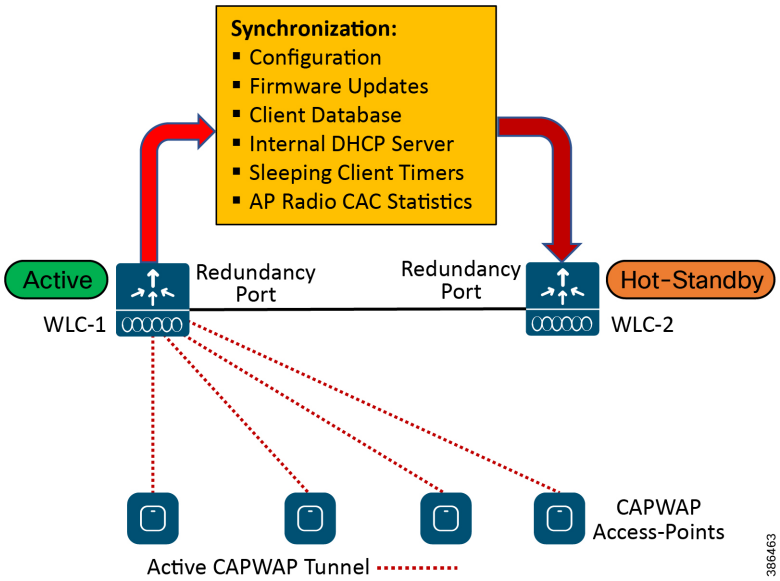
The redundancy port checks for peer reachability by sending User Datagram Protocol (UDP) keep-alive messages every 100 milliseconds (default frequency) from the standby-hot controller to the active controller. If the active controller fails, the redundancy port is used to notify the hot standby controller.

This high-availability (HA) configuration allows the access point (AP) to establish a CAPWAP tunnel with the active WLC and share a mirror copy of the AP database with the standby WLC. In the event the active WLC becomes unreachable from the network, the APs do not go into the Discovery state and the standby WLC switches over to become the active WLC.

Only one CAPWAP tunnel is maintained at a time between the APs and the WLC that is in the active state. The overall goal for the addition of AP Stateful Switch Over (SSO) support to the Cisco Unified Wireless LAN is to reduce major downtime in wireless networks as a result of failure conditions that may occur due to box failover or network failover.

Client Stateful Switch Over (Client SSO) supports seamless transition of clients and APs from the active controller to the standby controller. Client SSO will be 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 WLC when the client associates to the WLC or the client's parameters change. Fully authenticated clients, i.e. 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 no SSID outage.

Figure 24 SSO-HA Wireless Controller Redundancy

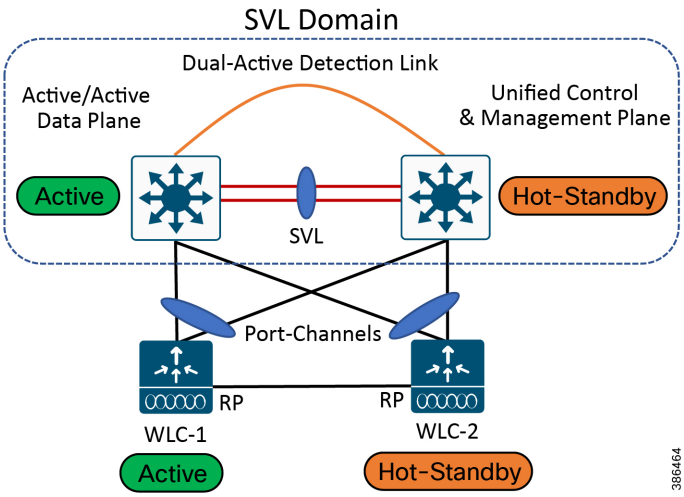


WLC SSO-HA using StackWise Switches

The topology depicted in the figure below demonstrates an SSO-HA pair of WLCs that are connected to a StackWise® pair of Cat-9300 switches and is the recommended design. This design minimizes the traffic that crosses the virtual switch link between the Catalyst-9300 switches in the StackWise® pair during normal operation, because both the active and hot-standby WLCs have ports connected to both switches. This design also avoids a switchover from the active WLC to the hot-standby WLC in the event of a switch failure within the StackWise® pair. However, in the event of a switch failure within the StackWise® pair, the number of ports connected to the active WLC would be reduced by half.

The wireless management, wireless user VLANs should be 802.1Q tagged between the Catalyst switches and the WLCs.

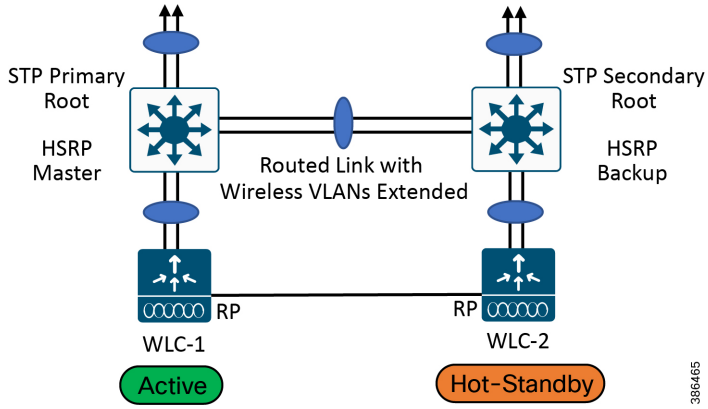
Figure 25 WLC SSO-HA using StackWise® Switches



WLC SSO-HA using HSRP

An alternative to using StackWise® Virtual at the distribution layer is to use HSRP to provide L3 redundancy. Depicted in the figure below is a WLC SSO-HA redundant deployment with HSRP implemented at the distribution layer switches.

Figure 26 WLC SSO-HA deployment with HSRP at Distribution Layer



For more information on how to configure SSO High-Availability on the controllers, please refer to the following link:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/High_Availability_DG.html#pgfId-201917

Static Channel Assignment

Disable the Dynamic Channel Assignment (DCA) feature on the Cisco WLC and statically assign the 2.4GHz channels - 1, 6, 11 on each of the APs based on the wireless and AP placement design derived from the site-survey results. This provides for a more deterministic RF environment to enable critical operations within an underground mining environment.

Manual AP Transmit Power Assignment

Disable the dynamic Transmit Power Control (TPC) feature on the Cisco WLC and statically configure the power-levels on each of the APs based on the wireless site survey results. This provides for a more deterministic RF environment to enable critical operations within an underground mining environment. For our use-case, we need to ensure that the WGB installed on the autonomous vehicles receive a signal of -55dBm or higher and a minimum SNR of 25dBm in-order to support the requirements of the Sandvik AutoMine application.

Cell Coverage Overlap

It is important to note that the actual coverage zone of an AP is from the perspective of the Wi-Fi client (in our case the vehicle WGB), and validating any planned coverage is a necessity. Further, sufficient cell coverage overlap should be provided to enable smooth roaming between APs as the autonomous vehicles move about in the underground mine tunnels. The cell coverage overlap will need to be tweaked in accordance with the maximum speed the autonomous vehicles are expected to travel at. The initial cell coverage overlap should be determined during the wireless site survey process so as to satisfy the Sandvik AutoMine application along with the desired maximum autonomous vehicle speed. This can be further fine-tuned during the post-install validation. In general, the faster the autonomous vehicle speed, the larger the cell overlap needs to be.

NTP Sync

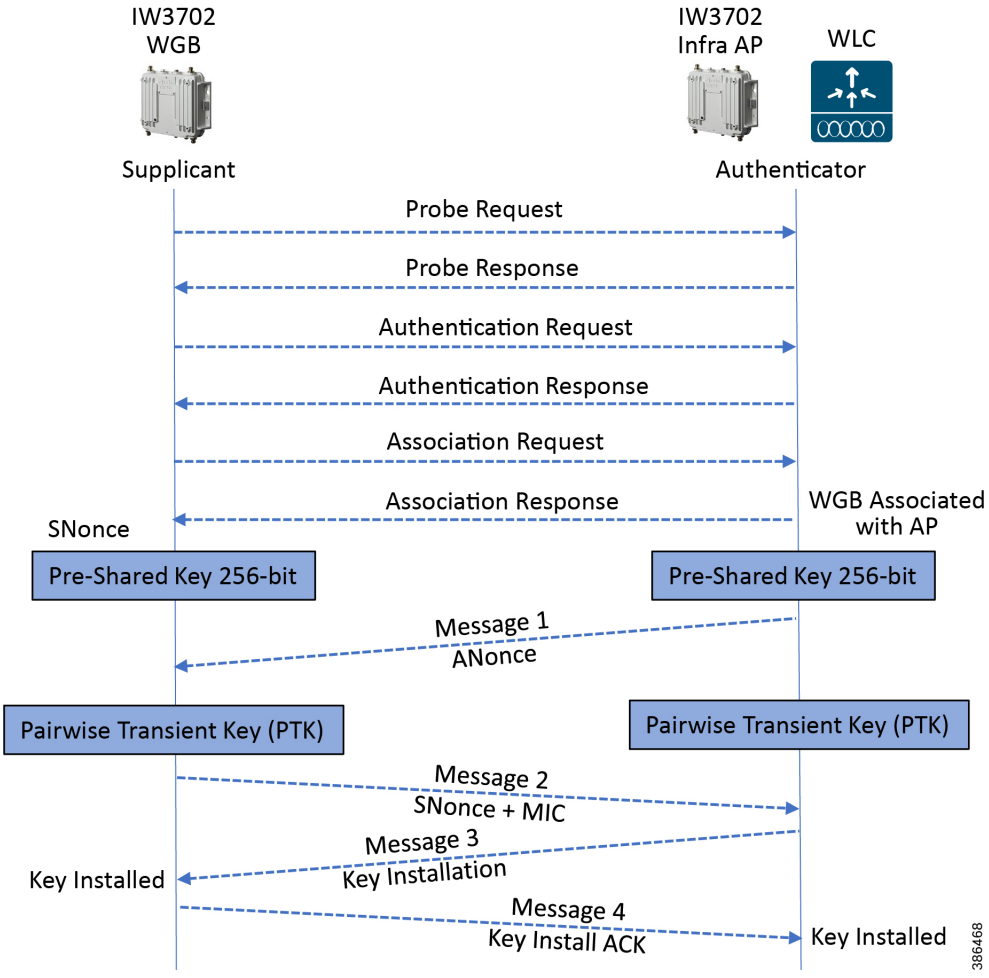
It is critical to have all your network components share the same accurate time. It is highly recommended to deploy an NTP server and sync all your network devices with it so that they all have the same synchronized time.

WLAN Security

WPA2-PSK

At a minimum, we recommend using WPA2-PSK as the authentication mechanism on the WLAN used for the Sandvik AutoMine application. A common secret pre-shared key (PSK) is configured on both the WGB and the WLC. The Cisco WGB comes pre-installed with a Manufacturer Installed Certificate (MIC). The figure below depicts the WPA2-PSK 4-way handshake used between the WGB and the AP to secure the WLAN after the WGB successfully associates with an AP.

Figure 27 WPA2-PSK 4-way handshake



Pre-Shared Key (PSK) Length

Pre-Shared Keys, at minimum, must be 8 characters long. The WLC supports a WLAN PSK between 8 and 63 characters in length. The longer and more complex your PSK is, the stronger the WLAN security is going to be and that much harder to compromise. Randomly generated PSKs using a cryptographic-strength pseudo-random number generator (PNRG)

helps prevent the PSK from being easily guessed (or subject to dictionary attacks) by a malicious user and are resistant to offline brute force attacks. The use of lower-case and upper-case letters along with numbers, and if the PSK is truly randomly generated, a twelve-character key gives you 71 bits of entropy. A 16-character PSK gives 95 bits of entropy. This should be more than sufficient security against attackers attempting to compromise the wireless network.

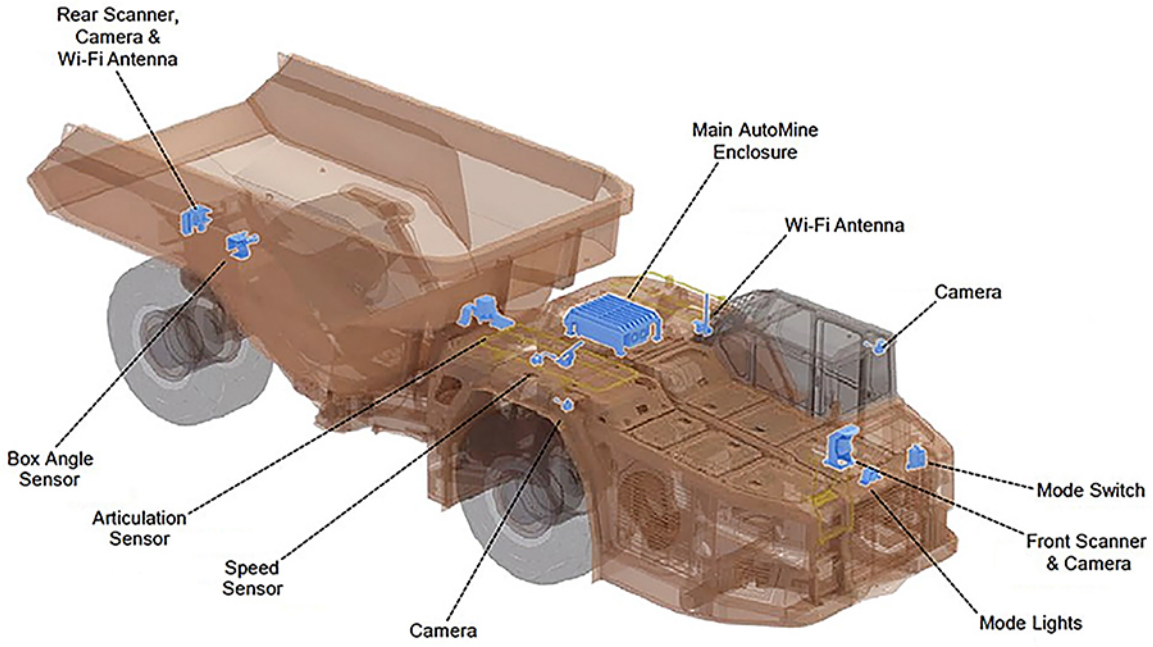
A PSK of 12 to 16 characters or longer is unlikely to be the weakest link in your wireless system and the use of extremely long keys is unnecessary and not very user friendly. You can also increase the security of your PSK by configuring the PSK-SHA2 option on the WLAN Security tab. Selecting this option uses the stronger SHA256 hashing algorithm as opposed to the default SHA1 which is used when WPA2 Personal Security is initially selected.

Cisco Work Group Bridge (WGB)

- A WGB is basically an access point (AP) configured to act as a wireless client towards an infrastructure, and to provide Layer 2 connectivity for the devices connected to its Ethernet interface.
- WGBs allow wired networks to be bridged across a wireless connection. In our scenario the wired devices behind the WGB are bridged to the Automine application network within the Control Room.
- A WGB is a special kind of client and is treat differently by the LWAP.
- WGBs use the Cisco Internet-Access Point Protocol (IAPP) to advertise their wired clients to the upstream LWAP/WLC:
  - This is a dynamic process, and the list of clients changes over time.
  - LWAPs only allow traffic to be sent to wired devices behind a WGB if they have previously been advertised via IAPP.
- For our use-case the WGB on-board the vehicle will connect to the Automine SSID advertised by the LWAP within the underground mine.

For the Sandvik AutoMine use-case, the Cisco WGB is installed on the autonomous vehicles in-order to provide network connectivity for IP-based video-cameras, I/O devices and sensors to be able to communicate with the Automine Remote Operator Station and PLC located back in the Control Room. The WGB is housed within the “Main AutoMine Enclosure” as depicted in the figure below.

Figure 28 Network connectivity for Sandvik AutoMine components on-board the autonomous vehicle



Cisco IW3702 WGB

The Cisco IW3702 WGB is deployed on-board the Sandvik Autonomous vehicle. The IW3702 WGB helps bridge the "Automine Subnet (VLAN Z)" on the vehicle with the "Automine Subnet (VLAN Z)" within the control room. This is achieved by the WGB associating with the "Automine SSID" advertised by the LWAPs distributed throughout the underground mine. The "Automine SSID" is associated with the "Automine Subnet (VLAN Z)" on the wired network.

The WGB uses its Radio-0 2.4 GHz interface to connect to the "Automine SSID". It uses pre-shared key (WPA2-PSK) authentication when associating with the "Automine SSID". AES is used as the encryption methodology over the wireless medium. Once the WGB traffic reaches the LWAP it is carried over the CAPWAP tunnel to the active WLC which then offloads it onto the "Automine Subnet (VLAN Z)" wired network.

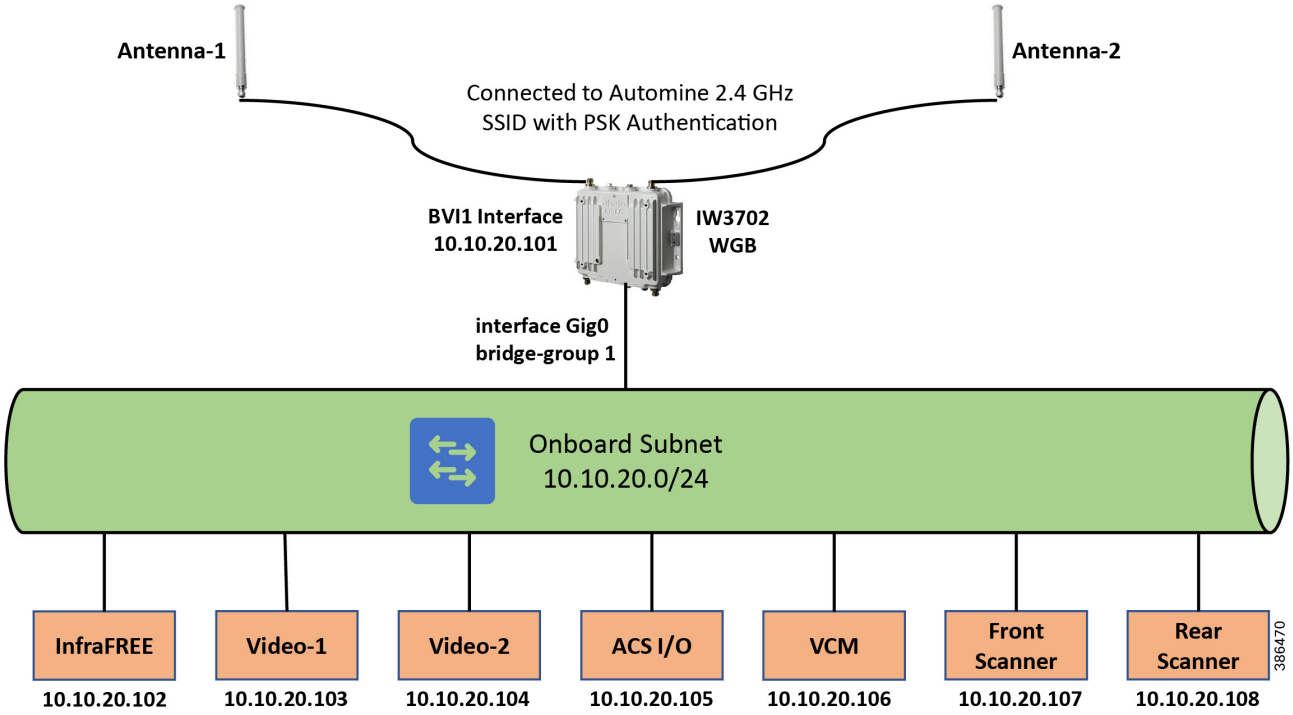
To provide wired network connectivity to multiple client devices behind the WGB a ruggedized switch is connected to the Ethernet port of the WGB. Each of the Automine components on-board the vehicle (cameras, I/O devices, sensors, scanners, etc.) are connected to an individual port on the ruggedized switch and are assigned a static IP address from within the "Automine Subnet (VLAN Z)". This means that the wired devices behind the WGB have L3 connectivity to the Sandvik AutoMine components deployed with the Control Room. All the wired devices behind the WGB belong to the same VLAN/subnet.

The Ethernet interface on the WGB is configured as part of a bridge group. There is also a corresponding Bridge Virtual Interface (BVI) interface configured on the WGB with an IP address assigned from within the "Automine Subnet (VLAN Z)".

Vehicle On-board Network

The network on-board the vehicle is a flat network with a single subnet and no VLAN segmentation. There is a switch connected to the Ethernet port of the IW3702 WGB to which all the Sandvik AutoMine vehicle components are connected each with a unique IP address assigned from within the Automine subnet.

Figure 29 Sample Vehicle On-board Networking



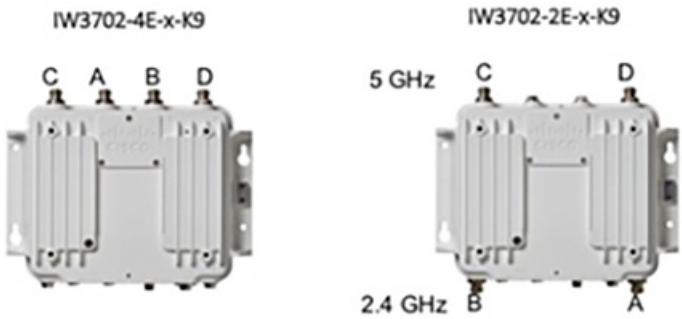
Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates using Pre-Shared Key (PSK) authentication. Therefore, it is highly recommended that the wired side of the WGB is physically secured.

There are approximately 8 IP addresses needed for each vehicle. IP addresses need to be reserved for each of the Automine and ACS servers in the control room. An IP address needs to be reserved for each of the Operator Terminals in the control room. There will an IP address needed for each of the ACS safety curtains. This means that a /24 Automine subnet we can support approximately 25 vehicles. If a larger number of vehicles need to be supported, then a subnet larger than the /24 subnet depicted here is required.

Attaching Mobile Mark 2.4GHz Antennas onto IW3702 WGB

The Mobile Mark RM3-2400 Heavy Duty vibration resistant 2.4GHz antenna should be connected to ports A and B of the IW3702 in single band mode.

Figure 30 IW3702 2.4GHz Antenna Ports – 'A' and 'B'



WGB Roaming

For a wireless device, roaming is a very critical part of its functionality. Basically, roaming provides the ability for a Wi-Fi client to transition from one AP to another where-in both APs belong to the same wireless infrastructure.

As roaming initiates a change for the Wi-Fi client from the currently serving AP to the next, there is a resultant disconnection or time without service. This disconnection time can be small. For example, less than 200ms on voice deployments or much longer, even seconds, if the security needed enforces a full authentication on each roam event.

Roaming is needed so the Wi-Fi client can find a new parent AP with hopefully a better signal, and it can continue to access the network infrastructure properly. At the same time, too many roams can cause excessive disconnections or time without service, which affects access. It is important for a Wi-Fi device, such as a WGB, to have a good roaming algorithm with sufficient configuration capabilities to adapt to different RF environments and data needs.

Elements of Roaming

- **Triggers:** Each client implementation has one or more triggers or events, that when met, causes the device to move to another parent AP. Examples: beacon loss (device does not hear anymore the regular beacons from AP), packet retries, signal level, no data received, de-authentication frame received, low data rate in use, etc. The possible triggers can be different from client implementation to another because they are not fully standardized. Simpler devices might have a poor trigger set, which causes bad (sticky clients) or unnecessary roams. The WGB supports all of the previous elements described here.
- **Scan time:** The wireless device (WGB) spends some time searching for potential parents. This normally implies going on different channels, doing active probing or passively listening for APs. As the radio has to scan, this means time that the WGB spends doing something else different from forwarding data. From this scan time, the WGB can build a valid set of parents that can be roamed to.
- **Parent selection:** After scan time, the WGB can check the potential parents, select the best one and trigger the association/authentication process. Sometimes, the decision point can be to remain on the current parent if there is not a significant benefit from a roaming event (remember that excessive roaming can be detrimental).
- **Association/Authentication:** The WGB proceeds to associate to the new AP, which normally covers both 802.11 authentication and association phases, plus completing the security policy configured on the SSID (WPA 2-PSK, CCKM, None, etc.).
- **Traffic Forwarding Restore:** The WGB updates network infrastructure of its known wired clients through IAPP updates after roaming. After this point, the traffic to/from the wired clients to the network resumes.

Security policies

One important aspect for roaming on mobile devices is what is the security policy that will be implemented on the infrastructure. There are several options, each one with good/bad points. These are the most important ones:

- **Open**—Basically no security. This is the fastest, and simpler of all policies. This has the main problem of not restricting unauthorized access to the infrastructure and no protection against attacks, which limits its usage to very specific scenarios. For example, mines where no external attacks are possible due to sheer nature of the deployment.
- **MAC address authentication**—Basically same level of security as open, as MAC address spoofing is a trivial attack. Not recommended due to the added time to complete the MAC validation, which slows down roaming.
- **WPA2-PSK**—Offers good level of encryption (AES-CCMP), but authentication security depends on the quality of the pre-shared key. For security measures, a password of minimum 12 characters and random is recommended. Similar to the pre-shared key method, as the key is used on multiple devices, if the key is compromised the password needs to be modified across all equipment. The roaming speed is acceptable, as it is performed in 6 frame exchanges, and the upper/lower time bounds for it to complete can be calculated because it does not involve any external control equipment (no RADIUS server, etc.). In general, this method is the preferred security option after balancing problems and benefits.

- **WPA2 with 802.1x**—This improves on the previous method by using a per device/user credential, which can be individually changed. The main problem is that for roaming, this method does not work properly when the device is moving fast, or short roaming times are needed. In general, this uses the same 6 frames plus the EAP exchange which can be between 4 and up. This depends on which EAP type is selected and the certificate sizes. Normally, this takes between 10 to 20 frames, plus the added delay of radius server processing.

- **WPA2+CCKM**—This mechanism offers good protection, uses 802.1x to build the initial authentication, then does a quick exchange of just 2 frames on each roam event. This offers a very quick roaming time. The main problem is that in case of a failed roam, it reverts back to 802.1x authentication. Then, starts using CCKM again after it authenticates. If the application on top of the WGB can tolerate an occasional long roaming time in case of problems, WPA2+CCKM can be employed as the best option versus WPA2-PSK.

The recommended security authentication policy to implement is WPA2-PSK with AES encryption. This means that the WGB will need to complete a 4-way handshake to authenticate its connection to the LWAP after it has successfully associated with it. Traffic to/from all the devices behind the WGB will be AES encrypted over the wireless medium.

Note: Open security gives the best handover performance, but it is not recommended. WPA2-PSK with AES encryption yields slightly longer handover times but is well within the latency requirements needed for Sandvik AutoMine application.

Disable Client MFP

- MFP can be useful from a security point of view. However, a drawback is that on roaming failure scenarios, the WGB does not accept de-auth frames from the AP parent to trigger a new roaming if the encryption key between both of them has gone wrong for any reason.

- On these rare failure scenarios, the WGB can take up to 5 seconds to trigger a new scan, if the current parent can be heard with good RF signal. There is a “catch-all” detection mechanism that WGB can trigger if no valid data frames are received during that time.

- By default, the WGB tries to use the client MFP if the SSID has WPA2 AES in use.

- It is recommended to disable client MFP if fast recovery times are needed (WGB to react to non-protected de

- -authentication frames). This is a compromise between security needs and fast recovery times. The decision depends on what is more important for the deployment scenario.

For the Sandvik AutoMine use-case because we require fast roam and recovery times it is recommended to disable client MFP.

```
dot11 ssid <ssid>
    no ids mfp client
```

IW3702 WGB Roam Time Optimization

WGB roam time is the time taken by a WGB radio to disassociate from the currently associated AP and associate to another AP which provides a better RF environment. During this interval there is no data transfer and hence the WGB roam time significantly affects application performance.

The default behavior for a WGB is to act as a normal Wi-Fi client and it will scan for a new parent AP after a continuous loss of 8 beacons. However, there are a few configurable options available to help optimize the roam process and reduce roam time.

Roaming involves two main processes:

1. Scanning
2. Re-association

Scanning

The WGB supports two main modes of roaming operations:

- **Static mode (default)** – Roaming is based on two main variables: “Packet retransmissions” or “loss of 8 consecutive beacons”.
- **Mobile Station mode** – On top of previous variables, the WGB can perform periodic analysis of signal level drops and data rate shifting.

There are four conditions that trigger the WGB to start scanning for a better AP:

- The loss of 8 consecutive beacons.
- A downward shift in data-rate.
- The maximum data retry count is exceeded (the default value being 64).
- A measured period of time of a drop in the signal strength threshold.

Only the last two items in this list are configurable and are explained here. The remainder of the values are fixed. When any of the above criteria is met, the WGB will trigger a roam process, scanning each channel for approximately 10-20ms. As a configuration optimization to reduce the roam time, the channels to be scanned during the roam process can be restricted to match only the channels used within a particular deployment. For example, a WGB radio can be configured to scan only Channels-1,6, and 11 within a 2.4GHz radio deployment.

The scanning methodology followed is termed “Active Scanning“. Instead of listening to beacons from APs, the WGB actively sends out “probe request” packets and waits for 20ms to receive a response on every channel. The AP will stop scanning after it receives the first response with a satisfying signal strength. So, scanning time may last approximately between 20-40ms in an 2.4GHz scenario and may be even shorter depending on radio hardware type deployed.

WGB Roam Optimization Parameters

There are two main methods to configure WGB roaming parameters:

- Using Packet Retries
- Using the **mobile station** command

Packet retries

Packet retries allows for a more conservative approach, where the WGB will not start a roam process until data loss is detected or 8 consecutive beacons are missed.

By default, the WGB re-transmits a frame 64 times. If it is not acknowledged (ACK) by the AP, it assumes that AP is no longer valid, and starts a scan/roaming process. See this one as an " async" roaming trigger because it can be initiated at any moment that a transmission fails.

The command to configure this, goes inside the dot11 interface, and it takes the following options:

```
interface dot11Radio0
    packet retries <1 - 128>  [drop-packet]
```

drop-packet: If not present, the WGB starts a roaming event when maximum retries are reached. When present, the WGB does not start new roaming and uses other triggers, such as beacon loss and signal.

If the WGB starts scanning because of a loss of eight consecutive beacons, the message “Too many missed beacons" is displayed on the console. In this case, the WGB is acting as a Universal Bridge Client, much like any other wireless client in its behavior.

In some situations, it is interesting to use the optional " drop" option in the packet retries, to preserve the association, even on the failure to transmit a data packet. This is useful for challenging RF environments, where the roaming can be also triggered by mobile scan command.

For the Sandvik AutoMine use-case we suggest lowering the packet retries to a value of “8” from a default value of “64” along with the ***drop-packet***. This is needed in order to meet the latency and roam-time requirements for the Sandvik AutoMine application.

RSSI Monitoring

Configuring the mobile station command will start a regular process on the WGB to perform “pre-emptive” roaming, which monitors the signal levels and data-rate speed changes and forces a roam before the currently associated AP signal strength is too low. This scan process will trigger small gaps in radio transmissions when the radio is performing the channel scan.

The **mobile station period** should be set depending on the application. The default is 20 seconds. This delay period prevents the WGB from constantly scanning for a better parent if, for example, the threshold is below the configured value. Some situations may require a faster timer; for example, autonomous vehicles.

This process takes two parameters:

- A timer, which wakes up the check process every X seconds
- RSSI threshold, which is used to trigger a roam if the current signal strength falls below it.

For example:

```
interface dot11Radio0
    mobile station period <1-1000s> threshold <1-100>
```

The time should not be lower than what the WGB takes to complete an authentication process in order to prevent a " roaming loop" in some conditions or to avoid a too aggressive roaming behavior. PSK networks may use one second. The actual period will always have one second added to the timer, product of the AP scheduler resolution for this task.

The RSSI level is expressed as a positive integer, although it is basically a normal -dBm measured level. It is recommended to use a number that is slightly above the minimum needed to satisfy the targeted data-rate.

Note: This command can also trigger a " roaming by data rate change" , which is too aggressive. It must be used together with minimum-rate for good results.

The mobile station algorithm evaluates two variables: data rate shift and signal strength and responds as follows:

- If the driver performs a long-term down shift in the transmit rate for packets to the parent, the WGB initiates a scan for a new parent (no more than once every configured period).
- If the driver detects that the RSSI from its parent is below the configured threshold, the WGB initiates a scan for a new parent (no more than once every configured period).

The threshold sets the level at which the algorithm is triggered to scan for a better parent. The default is -70 dBm. The correct threshold to configure depends on the intended data rate, versus the coverage level offered in the environment where the WGB will operate. Assuming a proper coverage level, the threshold should be configured to be a little less than the “breaking point” needed to support the data rate for the applications in use. For the Sandvik AutoMine use-case within underground mining we found the optimal roam trigger to be -55 dBm.

When these settings are enabled, the WGB scans for a new parent when it encounters poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using this criteria, a WGB configured as a mobile station searches for a new parent association and roams to the new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the WGB does not search for a new association until it loses its current association.

Minimum Data Rate

Another configurable parameter to control when the WGB should trigger a new roaming event is the “Minimum Data Rate” parameter – it triggers a roam when the current data rate falls below the configured threshold.

This is helpful to ensure a desired lower bound on data-rate is maintained in order to support video or voice applications. The recommended way is to always configure this command, whenever a mobile station period command is used:

```
int dot11Radio0
    mobile station minimum-rate 10.0
```

With this, the roam process is only triggered if the current rate is lower than the configured value. This reduces unnecessary roaming and allows one to maintain a minimum data-rate.

Note: The message " Had to lower data rate" is expected to occur even with this config, just that now it should only be seen if WGB was TX at a lower than configured speed, when the mobile station period check time was triggered.

Scan Channels

The WGB scans all " country channels" while doing a roaming event. Depending upon the radio domain, the WGB can scan channels 1 to 11 or 1 to 13 on the 2.4 GHz band. Each scanned channel takes some time. Each channel scan takes approximately 10 to 13 mSec. A good optimization is to restrict the scanned channels to use only the ones in service by the infrastructure.

There are three points to take when designing a channel plan for WGB/Roaming:

- For 2.4 GHz band, stick with channels 1/6/11 to minimize side channel interference. Any other channel plan with 4, etc., tends to be difficult to engineer properly from RF point of view, without increasing interference.
- Using a single channel setup for all APs is a good idea from scan point of view. This only makes sense if the total number of clients to support is very low, and there are not high bandwidth requirements. This eliminates the radio change time from the scan time. Be aware that few environments can benefit from this option, so use with care.

The channel plan in use for your particular deployment might need to accommodate other requirements. Follow general RF design recommendations and leading practices.

In order to configure the scan channel list:

```
int dot11Radio0
    mobile station scan 1 6 11
```

Note: The “*mobile station*” command only shows up when the radio is configured for WGB role.

Note: Make sure the WGB scan list matches the infrastructure channel list. If not, the WGB will not be able to find the infrastructure APs.

Tuning Timers

There are several timers available on the WGB to help optimize recovery time when a problem occurs. The commands are only available when the AP is in WGB mode.

```
wgb(config)#workgroup-bridge timeouts ?
    assoc-response  Association Response time-out value
    auth-response   Authentication Response time-out value
    client-add      client-add time-out value
    eap-timeout     EAP Timeout value
    iapp-refresh    IAPP Refresh time-out value
```

In the case of *assoc-response*, *auth-response*, *client-add*, these indicate how long the WGB will wait for the parent AP to answer, before considering the AP as dead the and trying the next candidate. The default values are 5 seconds, which might be too long for some applications. For the Sandvik AutoMine application the optimal values were found to be 50 msec for both *auth-response* and *assoc-response* and 800 msec for *client-add*.

For eap-timeout, the WGB sets a maximum time to wait, until the full EAP authentication process is completed. This works from a EAP supplicant point of view in order to restart the process if the EAP authenticator is not answering back. The default value is 60 seconds. Be careful to never configure a value lower than the actual time needed to complete a full 802.1x authentication. Normally, setting this to a value between 2 to 4 seconds works for most deployments. For the Sandvik AutoMine application 2 seconds was found to be an optimal value.

The IAPP protocol is used by the WGB to inform the network infrastructure of the devices that the WGB has learned on its Ethernet interface. For *iapp-refresh*, the WGB by default generates an IAPP bulk update to the parent AP after roaming in order to inform it about the known wired clients. There is a second retransmission after association around 10 seconds later. This timer allows to do a " fast retry" of the IAPP bulk after association in order to overcome the possibility that the first IAPP update was lost due to RF, or encryption keys not yet installed on the parent AP.

For the Sandvik AutoMine use-case here are the suggested and validated timer values:

```
workgroup-bridge timeouts eap-timeout 2
workgroup-bridge timeouts iapp-refresh 10
workgroup-bridge timeouts auth-response 50
workgroup-bridge timeouts assoc-response 50
workgroup-bridge timeouts client-add 800
```

These have been successfully tested on mobile WGB deployment scenarios.

Quality of Service (QoS)

Quality of Service (QoS) is the capability of a network to provide differentiated services to selective network traffic over various network technologies. Configuring QoS does not increase the bandwidth of the network; it merely enables more control over how the bandwidth is allocated to different applications on the network. It is imperative that you understand your network traffic, the protocols involved, and the sensitivity of the application to network delays.

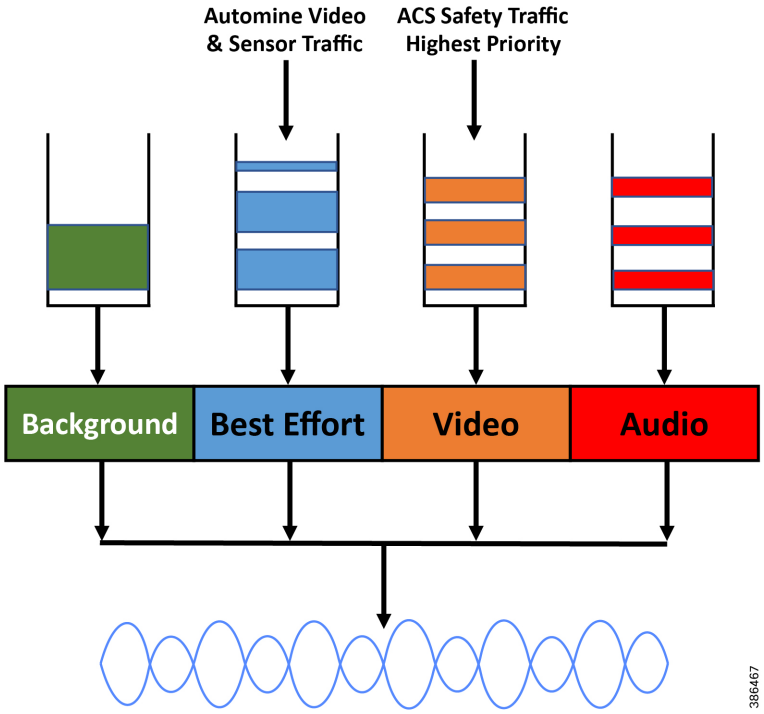
WGB QoS Policies

For the Sandvik AutoMine application, the ACS Safety traffic needs to be prioritized over all other traffic types like video traffic, sensor traffic, etc. This traffic consists of control communication going back and forth between the autonomous vehicle operations and the control room PLC. There are strict latency requirements for this traffic, typically < 250 msec.

On the Cisco WGB a combination of extended ACLs is employed to classify the safety traffic, and use a combination of class-map and policy-map to mark the safety traffic with a CoS value of “5” on the ingress of the Gigabit Ethernet port. This QoS service policy is applied inbound on the Gigabit Ethernet port of the WGB. By performing marking this way traffic is essentially mapped into the “Video Queue”.

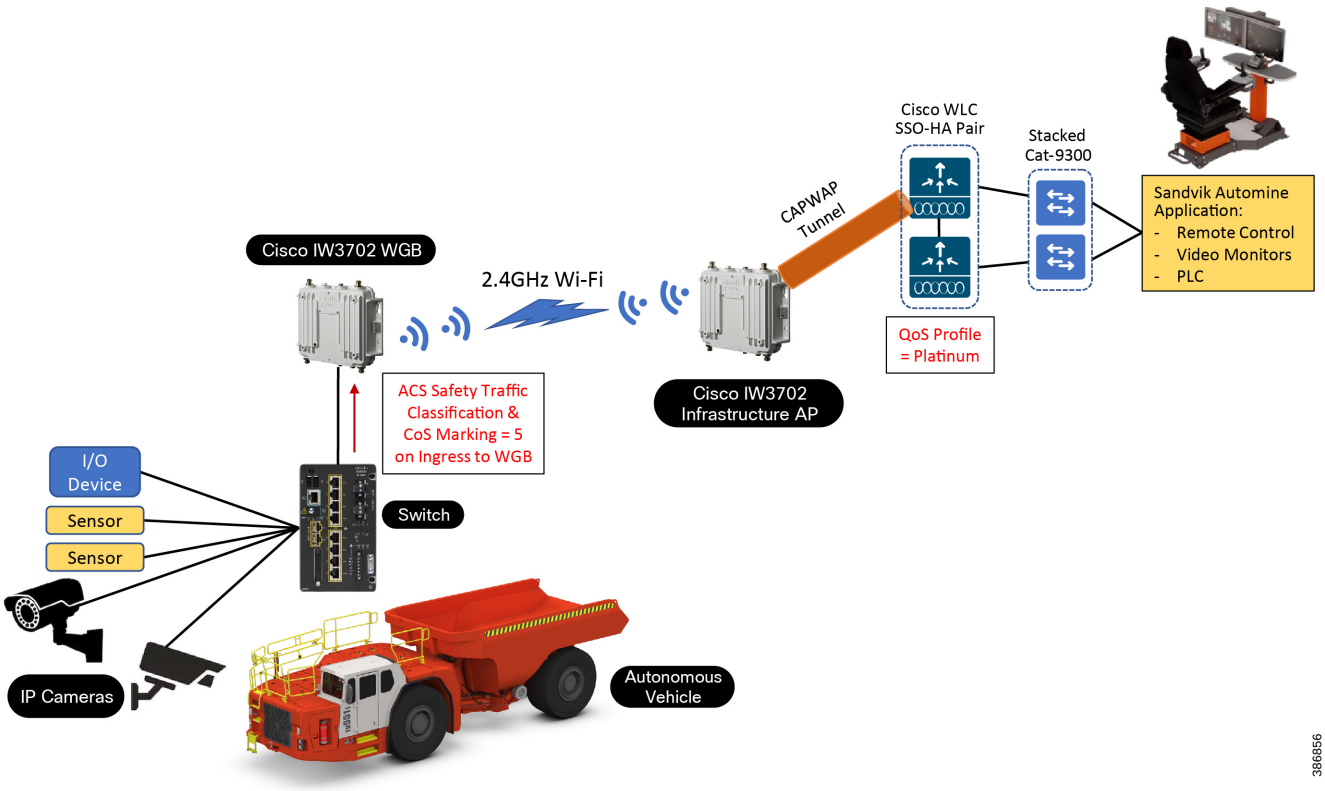
The figure below depicts the WI-FI Multimedia (WMM) queuing performed on the WGB client. There are four separate queues, one for each of the access categories. Each of these queues contends for the wireless channel. If more than one frame from different access categories collide internally, the frame marked with higher priority is sent and the lower priority frame adjusts its back-off parameters as though it had collided with a frame external to the queuing mechanism. This system is called Enhanced Distributed Channel Access (EDCA).

Figure 31 Sandvik AutoMine Traffic mapping to WMM Queues on WGB



WLC QoS Policies

Figure 32 E2E QoS for Sandvik AutoMine



WLAN data in a Unified Wireless Network is tunneled by way of CAPWAP (IP UDP packets). To maintain the QoS classification that has been applied to WLAN frames, the WLC uses a process of mapping classifications to and from DSCP and CoS. For example, when WMM classified traffic is sent by a WLAN client, it has an 802.1P classification in its frame. The AP translates this classification into a DSCP value for the CAPWAP packet carrying the frame to ensure that the packet is treated with the appropriate priority on its way to the WLC. A similar process occurs on the WLC for CAPWAP packets going towards the AP.

When the infrastructure AP receives traffic from the WGB, it encapsulates the original packet into CAPWAP and adds an outer DSCP value. This outer DSCP value corresponds to WMM user priority (UP) of the incoming frame from the client. The switchport connected to the APs must be configured to trust this DSCP value.

If the packet is sent to a trunk port, it will derive a CoS/802.1p value based on the outer DSCP value trusted at the AP connected switch port. When the packet arrives at the WLC and prior to offloading it to the wired network, the WLC will re-write the CoS value based on the capped DSCP value (or outer DSCP) of the packet received from the AP.

When the packet is offloaded from the WLC onto the wired network, the switchport where the WLC is connected must be configured to trust the CoS value set by the WLC. The switch will then derive a DSCP Value based on the CoS-DSCP table mapping on the switch.

Wi-Fi Multimedia (WMM)

Wi-Fi Multimedia (WMM) is a certification that applies to both clients and APs. The features are taken from the 802.11e draft. Using the eight IEEE-developed 802.1p QoS classifications, WMM maps the classifications into four access categories. The four access categories are mapped to the WMM queues required by a WMM certified device. The table below outlines the 802.1p to WMM mappings.

Each of the four WMM queues competes for the wireless bandwidth available on the channel. WMM uses Enhanced Distributed Coordination Function (EDCF) for handling the queue traffic. If more than one frame from different access categories collides internally, the frame with the higher priority is sent. The lower-priority frame adjusts its back-off parameters as though it had collided with a frame external to the queuing mechanism.

WMM prioritization helps minimize delays in wireless networks for time-sensitive applications such as voice and video. WMM is the default Enhanced Distribution Coordinated Access (EDCA) parameter set on the controller.

Figure 33 WMM Access Categories – EDCA

User Priority	802.1 Priority	802.1 Designation	Access Category	Designation
Lowest ↓ Highest	1	BK	AC_BK	Background
	2	-		
	0	BE	AC_BE	Best Effort
	3	EE		
	4	CL	AC_VI	Video
	5	VI		
	6	VO	AC_VO	Voice
	7	NC		

386544

WLAN QoS Profiles

QoS Profiles supported by the Cisco AireOS WLC:

- Bronze – Background (BK)
- Silver - Best effort (BE)
- Gold - Video applications (VI)
- Platinum - Voice applications (VO)

These four options correspond to the four WMM access categories shown in the previous figure.

These settings set the limit on the maximum QoS value for the CAPWAP frames and AP radio AC for the transmitted frames. Configuring a WLAN for Platinum QoS, for example, does not place every frame into the Platinum radio access category. The QoS markings on the original frame are not altered.

For the Sandvik AutoMine wireless deployment we allow a maximum QoS value of “Platinum” so as to be able to expedite the ACS safety traffic.

802.1p Markings

Since CoS is trusted on the network, 802.1p wired tagging must be enabled on the WLC to help ensure end-to-end QoS on the network. The tagged packets include CAPWAP data packets (between access points and the controller, network downstream) and packets sent toward the core network. 802.1p configurations do not affect AP to WLC traffic (network upstream).

The wired QoS profile comes into play if tagged or untagged interfaces are configured north of the controller. If the protocol type is set at the default setting of 'none', then dot1p markings for all frames are best effort regardless of the original DSCP marking.

If, however, DSCP-CoS maps are defined on the underlying Cisco AVVID infrastructure, the AVVID CoS marking corresponding to the DSCP marking is applied. This allows the controller to assign an upper QoS value on Layer 2 when it performs the mapping from Layer 3 to Layer 2. If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Note: If DSCP is trusted on the network, then the 802.1p configuration should be left at the default of **none**.

Trust DSCP Upstream

In order to ensure that frames from Wi-Fi clients are properly encapsulated based on the DSCP marking, Trust DSCP Upstream should be enabled under the QoS Map feature on the WLC. Enabling this feature tells the AP to use the DSCP marking on the client frame to determine the outer CAPWAP frame DSCP value.

This feature is especially useful when Wi-Fi client supplicant or application is incorrectly marking the 802.11e UP value when sending traffic to the AP.

Although Trust DSCP Upstream is under the QoS Map feature on the WLC GUI and CLI, this feature is wholly independent from the QoS Map. The Trust DSCP Upstream feature without making any changes to the QoS Map configuration, i.e. enabling or disabling QoS Map.

Note: Trusting DSCP Upstream is a global configuration and once enabled will apply to all APs and WLANs.

Chapter 4: Wireless Site Survey

Wireless Site Survey Overview

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

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

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

The purpose of this section is to outline the steps and key requirements for deploying a network in support of an underground mining operation.

Pre-Survey Data Collection

Prior to conducting a site survey, it is imperative the RF engineer investigates the customer requirements. This step ensures the applications and use cases that ultimately need to be supported by the wireless deployment are well understood. Integrating these requirements into the survey process ensures that the resultant design accommodates proposed performance criteria, as stated by the customer's equipment and application vendors. A thorough analysis of the requirements might reveal further exceptions and atypical needs that may impact a site survey, such as the need to support legacy 802.11b endpoints and corresponding data-rates.

Requirements Gathering Process:

- Application Requirements (Real-Time vs Non-RT)
- Bandwidth requirements for the applications
- Concentration of users/endpoints requiring wireless connectivity

As an example of a requirement that may be found in an underground mining operation, consider vehicle remote control or tele-operations. This is a real-time application, which also relies on several on-board video cameras to remotely operate a vehicle. Considering the resulting per vehicle bandwidth requirements, due to the on-board video cameras, a site survey would likely reveal a dense AP deployment in order to support the necessary data rates to sustain acceptable application behavior. While other steps and considerations may be necessary to fully optimize the wireless network to support tele-operations, this application and its requirements are very different from needing to support tablets or other handheld devices for inspection and maintenance activities.

Other customer requirements could consist of the following:

- Specific areas that require WLAN coverage to support specific applications, as well as areas that do not require coverage

- Contiguous RF coverage to facilitate fast client/endpoint roam times to support real-time applications
- Convergence of OT and IT applications/users
- Concurrent access and concentration of users/endpoints
- Identify
- WLAN requirements for client devices and applications such as, but not limited to:
  - Application bandwidth and throughput requirements
  - Endpoint/application transmission characteristics (constant bit rate vs. traffic bursts)
  - Supported data rates; with a desire to disable lower/legacy data rates
  - Transmit Power
  - Minimum RSSI
  - Signal-to-Noise
  - Ratio (SNR)
  - Packet Error Rate (PER)
  - Retransmissions
  - Latency and Jitter
  - Channel separation
- Designated high throughput rates for maximum network performance per AP
- High density coverage areas such as training rooms, cafeterias, and equipment docking stations
- IEEE 802.11a/g/n/ac Wave-1/ac Wave-2/ax
- Support for legacy 802.11b client devices
- Minimize coverage bleed out into undesired coverage areas (security consideration)
- Support for future applications (excess capacity and performance)

RF Site Survey

A thorough RF site survey comprises of multiple activities in order to yield the desired outcome. One, as mentioned previously, is the actual site survey activity, which involves the placement of APs in different locations within a defined area, in order to understand RF coverage and potential performance characteristics. Another is an RF spectrum analysis. While it is imperative to validate that the wireless design and the resultant deployment are capable of meeting the application requirements, it is equally important to understand what other RF devices might be operating in close proximity that can end up adversely impacting the wireless deployment.

RF Spectrum Analysis

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

Note: When considering OT and IT convergence, particularly within an underground mine, in order to avoid potential challenges with interference, it is strongly recommended to deploy a single converged wireless network capable of supporting both OT and IT wireless requirements. Deploying 2 independently managed radio systems will not only increase the probability for interference but could also result in excessively high channel utilization levels.

The principle goals of a spectral analysis are to search for and locate potential sources of RF interference. Based on the awareness of potential interferers, it is possible to somewhat reduce the effects to other equipment and end user applications, if the RFI sources cannot be completely eliminated. Although comparatively rare in everyday life, RFI opportunities increase proportionally with the increased density of wireless devices. Therefore, given the reliance on mobile assets/endpoints and application needs, areas such as medical, military, industrial, and commercial environments are more prone to the effects of RFI due to wireless equipment being more commonplace. 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 and locate 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 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-in to the area.

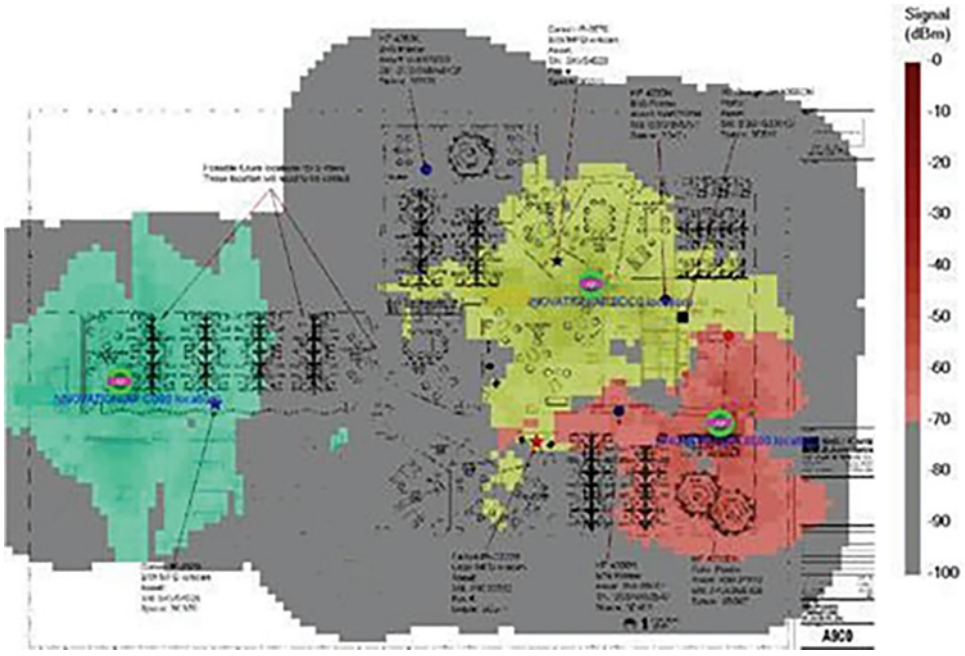
Wireless Site-Survey Tools

There are a growing number of survey and test tools addressing WLAN and Voice over WLAN (VoWLAN) deployments. 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 but are not recommended for use 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. Site-survey products from AirMagnet and Ekahau are commonly used.
- Premium RF site survey products allow field engineers to collect live information on signals, packets, and spectrum data during site surveys. This information may be collected while in active or passive modes. Active mode surveys reveal more detailed information while passive modes enable faster survey.

These products 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 as shown in the sample survey shown in the following figure. The figure below depicts indoor survey data with colors enhanced to show channelization.

Figure 34 Sample Indoor Survey Data



Site Survey Techniques

General site survey techniques vary among engineers based on experience and training which may result in wide ranging results for the same environment. Assuming each of the surveys are performed with the requirements and use cases in mind, each of the resulting different designs may be sufficient. However, this lack of uniform methodology and design principles can leave a customer or end user questioning the outcomes and facets of the technology. Topics in this section include Baseline Propagation Assessments, Active Site Survey, Passive Site Survey, and 2D Site Surveys. These principles can be applied to underground mining environments.

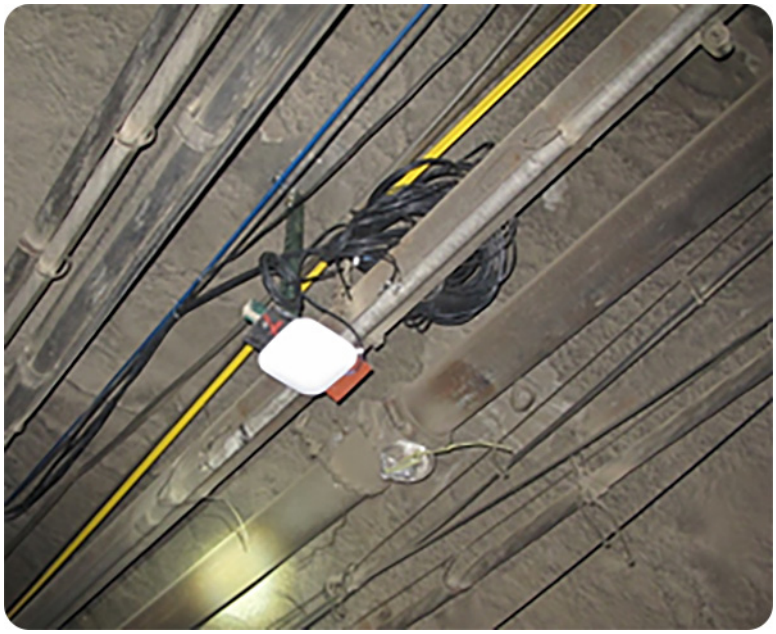
Baseline Testing Methodology

The purpose of a baseline assessment is to better understand propagation within an environment to establish general guidelines and a repeatable methodology that can help guide the remainder of the survey process. Guidelines to consider are obstructions and potential mounting locations, required clearances for vehicles and other traffic, client devices and mounting locations on mobile equipment, acceptable antenna types, maximum or minimal AP power settings, and general separation between APs to maintain as low of a noise floor as possible. Establishing a baseline survey methodology in an underground mining environment is critical, as there are several factors within the environment that can impact the propagation of RF signals. In addition, each mine presents its own fair share of challenges and unique characteristics, requiring a new baseline and survey methodology to be established per mine. Therefore, it is critical to uncover and understand these factors early on, for each environment, allowing for them to be accounted for and addressed as survey activities progress.

As an example, mounting radios and antennas in the “best” or preferred location within a mine is not always an option. Sometimes concessions need to be made. It may not be possible to always mount radios down the centreline of a tunnel. Equipment clearance heights, existing pipes and equipment, availability of power, physical form factor, are all considerations that need to be factored in when determining where a radio/antenna can be mounted. Once a candidate mounting location has been identified, based on a visual survey of the environment and available viable location options, it is necessary to perform a survey to understand signal propagation. Initial testing and placement will set the precedence for the remainder of the survey, as preliminary results will indicate how environmental challenges should be dealt with. The survey will reveal if objects in the vicinity of the AP have an impact on RF transmission by creating “blind spots” or

shadows. It will also reveal what kind of RF propagation characteristics a drift may have, such as whether the walls and tunnel material absorb RF energy, or if they have reflective properties and acts as more of a waveguide. Both examples can influence where subsequent APs may be placed, locations that should be avoided, as well as the acceptable spacing between consecutive APs.

Figure 35 Sample AP placement



The following is a list of factors to consider while establishing a baseline site-survey methodology:

- Tunnel shape, geometry and potential equipment mounting locations
- Inclines/declines and bends/turns in the tunnel
- RF absorption vs. reflection characteristics of the tunnel
- Mounting options/potential shadowing
- Types of client devices connecting and position
- Availability of power and resources to support the equipment
- Opportunity to repeat similar placements

While determining the mounting and positioning for the infrastructure APs is critical, it is also essential to consider the position and orientation of the client devices in relation to the infrastructure APs. Are they tablets or other handheld devices, are they radios mounted on mobile assets, are the antennas mounted on the vehicles limited to one side or section of the vehicle? When possible, actual or similar client devices should be leveraged to aid in the survey process, to include mounting the radios in the manner in which they will be used. As an example, while it might not be possible to use a revenue generating mobile asset, a truck can be leveraged with the equipment temporarily mounted.

Baseline Execution

If the network is to support 5 GHz and 2.4 GHz, then these tests should be conducted with both frequency bands, taking into account local RF regulatory domain restrictions. If both technologies would be used, then it is best practices to first conduct these tests with 5 GHz, determine the best power settings, and then do 2.4 GHz and alter power settings for those frequencies to match coverage area to that of the 5 GHz coverage cells. This matched coverage cell architecture will ease overall design and deployment issues. In order to achieve the desired results, the following steps should be followed:

1. Set up one AP in one area of the location being surveyed. Set Power level on the 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 environment 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, with the specific power setting and antenna configuration while recording the data.
4. If 5GHz and 2.4GHz are to be used for this location, then at this point configure AP power for 2.4 GHz while standing at the edge of the 5 GHz coverage cell to match the cell sizes. After this, the baseline power levels for both 5GHz and 2.4 GHz is set. This step is omitted when using outdoor mesh equipment where the 5GHz radio is only used for backhauling communications and not supporting client connectivity.
5. Once this baseline is established, then re-do the site survey process in the same area for that same AP location for 2.4 GHz 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

Implementation Considerations

As already mentioned, many factors should be considered when designing and deploying a wireless network. Each of the topics listed below has a unique ability to impact wireless communications and must be considered or uncovered during the site survey and installation process. Ultimately, these considerations and their handling need to harmonize with the overall solution requirements. This will provide more assurances both the design and subsequent resulting deployment, will be able to meet service level expectations and application requirements.

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 remote or tele-operations, or location appliances services that rely on RSSI trilateration to determine approximate locations of a client device. In an oil and gas processing area or underground mining, the elevated operational spaces may only require a singular AP position locations to provide the needed coverage or connectivity. A suitable location on infrastructure like a vessel or stack may not exist. It may not be suitable or practical to install APs to support RSSI trilateration for location services. 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 a client devices passes by a near-field micro-area such as a doorway or another known point.

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 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.

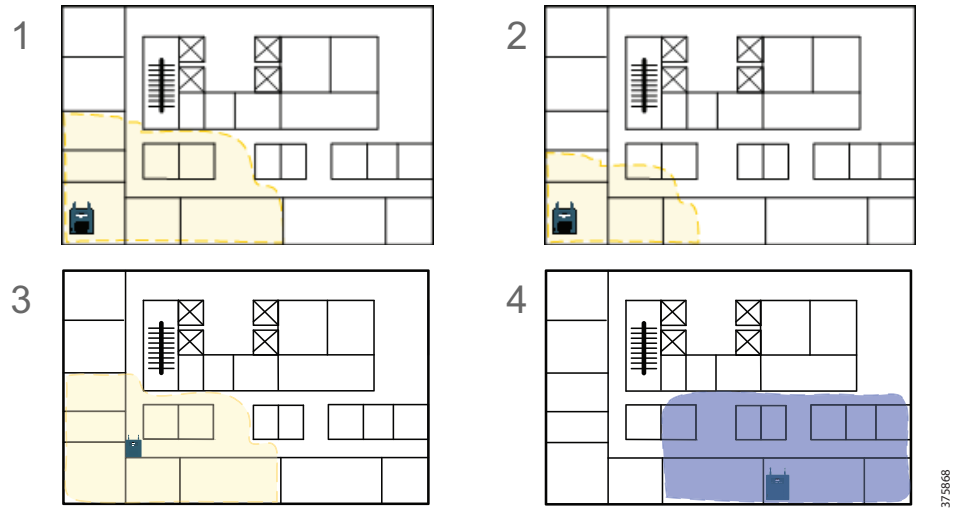
3. With the AP moved into its first official test location, the site survey will yield the anticipated controlled results. Depending on the desired results, it may be best to leave an AP in remote rooms for more cellular isolation that directly relates to the density of APs required to support coverage. 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.

The following figure demonstrates some example AP placements to begin the corner out 2D RF site survey methodology.

Figure 36 2D Site Survey



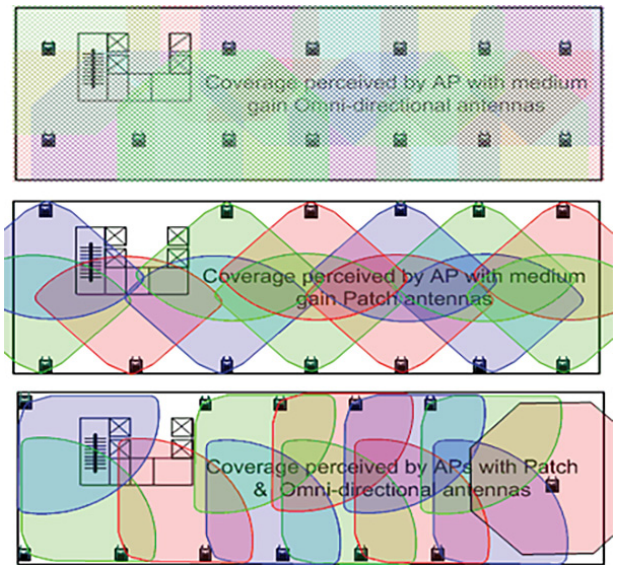
Omni versus Directional Energy Surveys

The 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 and 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 37 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.

Post Installation: RF Tuning and Optimization

While the output from the survey work is critical for the planning and design phase of a project, there is still additional work that needs to be performed, post-deployment and installation. In order to validate the installed solution aligns with the specifications of the design, and meets application requirements, it is necessary to conduct another survey once the wireless equipment has been deployed within the mine. This validation may be done over time in phases, which aligns with a phased construction and implementation schedule. However, the fundamental purpose is to conduct an RF survey, using previously described tools and techniques, to tune and optimize the wireless system, ensuring it provides the necessary coverage and meets the design requirements.

Additional Considerations

Work Safety

Safety is the first priority when working in any environment, especially within hazardous locations. Several levels of safety training and certifications that may include regional, national 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
- Respirator
- Helicopter transport to offshore (dunk tank crash survival training)
- Lockout/tagout/try out

A best practice for safety and security is ensuring that a local site escort be present 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. Examples of 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)
- Respirator
- 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 used in environments for which it is rated. Cisco industrial APs are rated for Class 1 Div 2 / ATEX Zone 2 environments. It is important to note that these devices must be externally powered, so be sure to use a safe and compliant method for temporarily powering up the APs. Laptops and tablets that are planned to be used to collect site-survey data must also be rated for the environments in which they will be used.

The Figure below shows a Cisco Technical Solutions Architect (TSA) working at a mine.

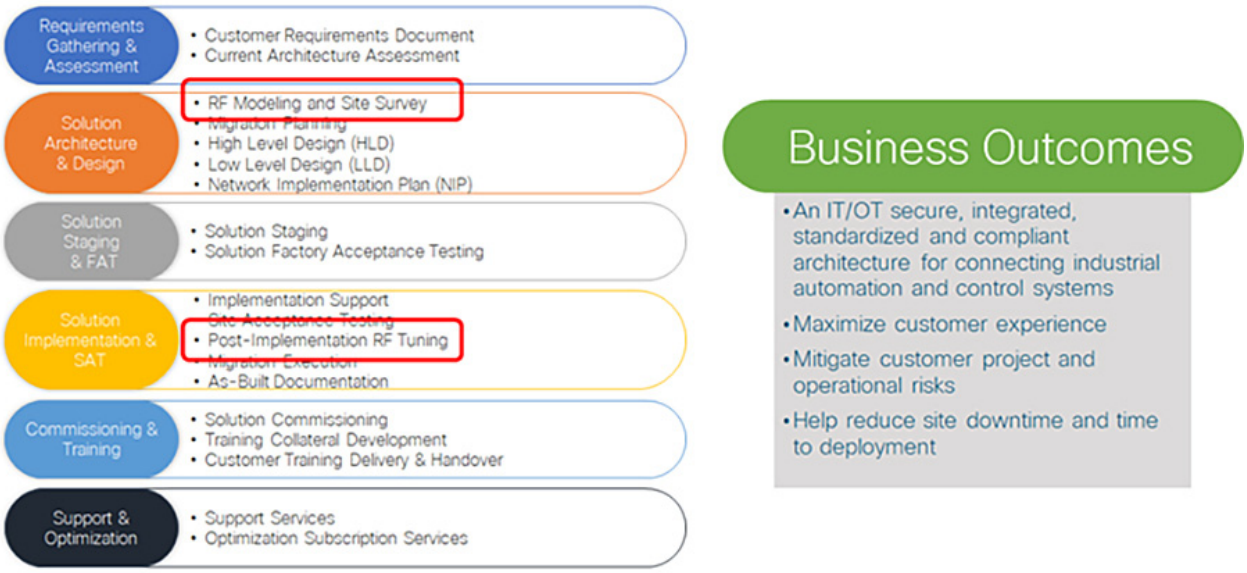
Figure 38 Field Engineer Performing Survey Work

Cisco Customer Experience (CX)

Thanks to a unique architectural based approach, Cisco® CX Industrial Networking and Security services help mining operators to accelerate 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 an 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 39 Cisco CX Service Offerings



Cisco CX 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 meeting the evolving demands of the business.

In line with the wireless services outlined in this section, Cisco CX with support from key partners, provides professional services to help underground mining customers with RF planning and design, as well as post-implementation RF tuning and optimization.

Note: For industrial wireless (particularly outdoor) deployments, it is critical to perform both predictive modeling, as well as an on-site survey, as part of the planning and design process. The amount of time spent on each of these tasks depends on the environment for which the wireless solution is being targeted for; specifically, are we dealing with a new greenfield deployment, or will the wireless solution be deployed within an existing brownfield environment.

Chapter 5: Underground Mining Wireless Network Implementation Guide

Test and Validation Methodology Overview

Cisco took a two-pronged approach to test and validate the use-case:

1. Cisco Outdoor Test and Validation within a parking lot
2. Test and Validation at the Sandvik Test Mine with Sandvik AutoMine, Sandvik ACS and Sandvik Autonomous Vehicles

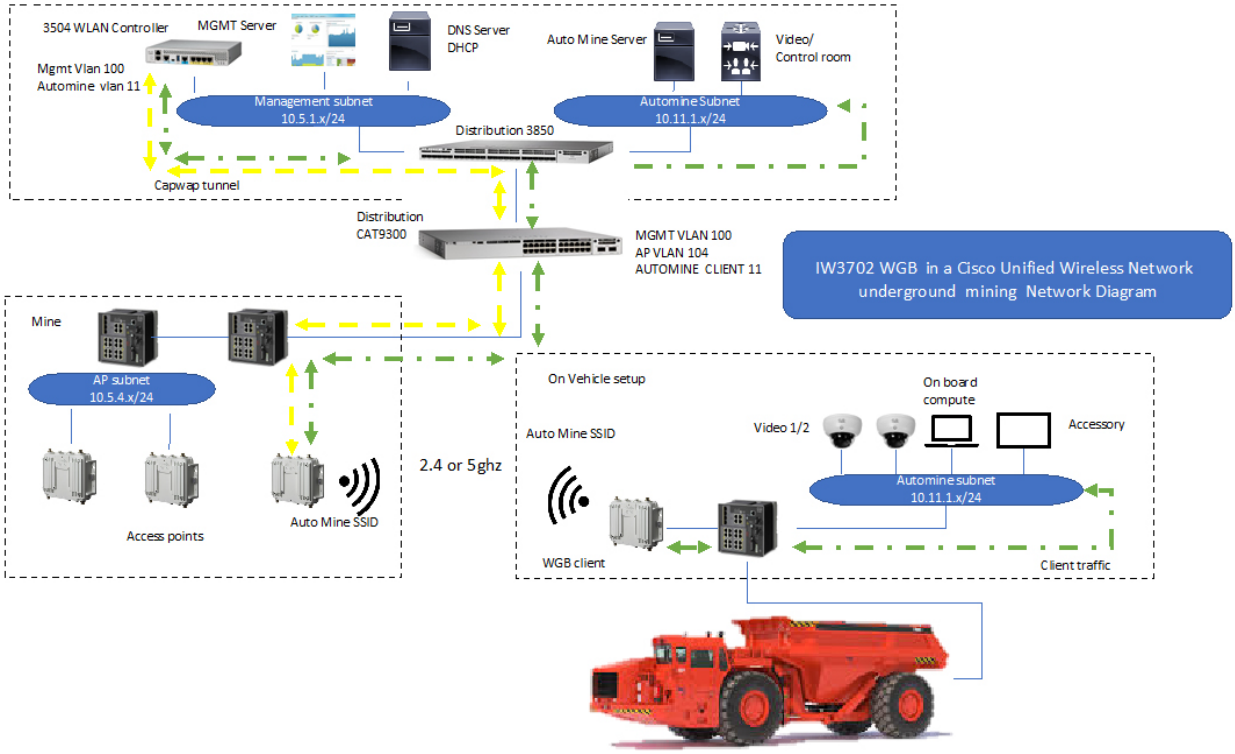
Note: The implementation guidance and configuration settings validated and mentioned here only apply to having a Cisco WGB installed on the vehicle. If using a non-Cisco WGB on the vehicle please adjust the settings needed accordingly.

Cisco Outdoor Test and Validation

The Cisco outdoor landscape was designed to present similar challenges to that found within a mining environment. Some of the types of challenges presented in these environments that have an adverse effect to Radio frequency are terrains and obstructions, antenna placement, transmitter power, cable attenuation losses, and other sources of RFI. Therefore, before any type of WLAN deployment it is recommended that a wireless site survey be completed to help ensure design requirements (coverage area, data-rate, roam latency, packet loss rate, etc.) are met for the network.

As part of the Cisco outdoor test effort, the following reference topology was used to help validate the autonomous vehicle use-case.

Figure 40 Reference Topology



WGB Installation

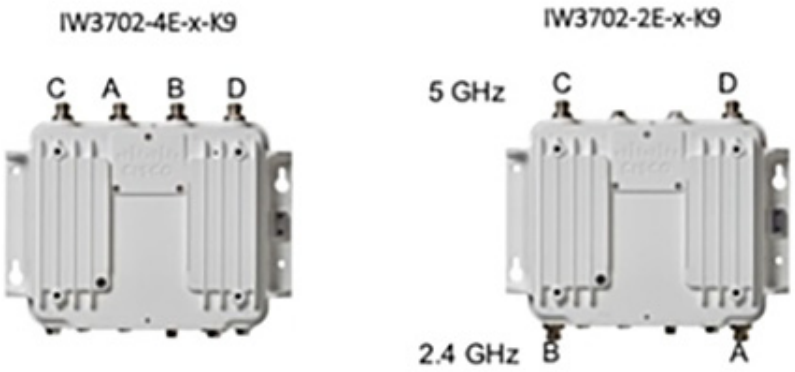
In the Cisco outdoor validation environment, the IW3702 WGB was installed in the rear of a test vehicle at a height between 10-11 ft. PoE was provided from a Cisco IE-3400 switch which also provided connectivity to wired devices such as IP cameras, on board PC (used for log collection during validation testing, etc.). An un-interrupted power supply (UPS) was used to power-up the IE-3400 switch and the IW3702 WGB.

Within the Sandvik Test Mine validation environment, the Cisco IW3702 WGB, a ruggedized switch and any additional electronic equipment were housed on the autonomous vehicle within a purpose-built industrial rated enclosure. Such an enclosure helps ensure that the components are safe from possible damage caused by falling debris, toxic chemicals and fumes, etc. while the vehicle traverses through the underground mine.

Attaching Mobile Mark 2.4GHz Antennas onto IW3702 WGB

The Mobile Mark RM3-2400 Heavy Duty vibration resistant 2.4GHz antenna should be connected to ports A and B of the IW3702 in single band mode.

Figure 41 IW3702 2.4GHz Antenna Ports - 'A' and 'B'



IW3702 Flexible Antenna Port

- Supports either dual-band or single band antennas on the same platform.
- Configurable via a CLI command.
- In single band mode, 2.4GHz radio uses antenna ports A and B, and 5GHz radio uses antenna ports C and D.

Configuring Antenna Band Mode for Mobile Mark antennas in autonomous mode:

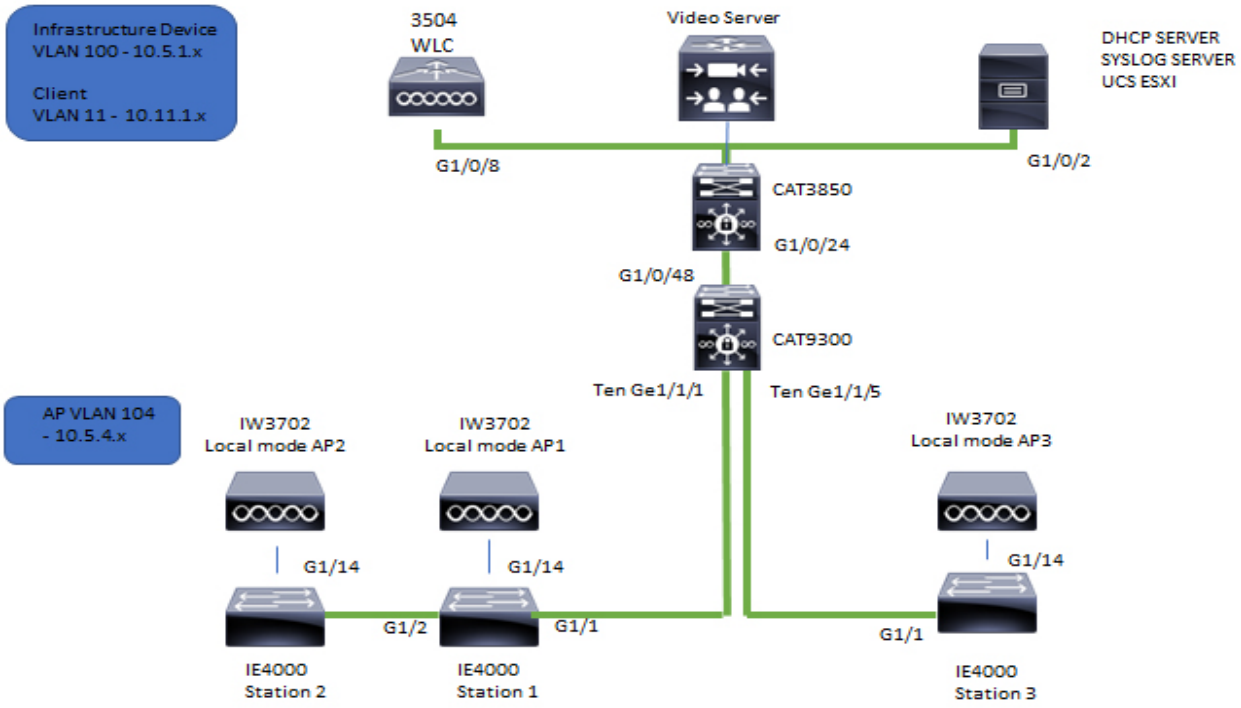
- IW3702-WGB-1(config)# dot11 ant-band-mode (dual | single)
- IW3702-WGB-1(config)# dot11 ant-band-mode ***single***

Table 6 Network Components used during validation

Components	Role	Version
Cisco 3504	AireOS Wireless LAN Controller (WLC)	AireOS 8.10.122
Cisco 1572	Mine Infrastructure AP (EoS 11/20 – Supported for existing Brownfield Deployments)	AireOS 8.10.122

Cisco IW3702	Mine Infrastructure AP	AireOS 8.10.122
Cisco AIR-ANT2568VG-N	Cisco 1572 Dual-band Omni-directional Antenna. 4 antennas recommended per AP for maximum omni performance.	N/A
Cisco IW3702	Autonomous Vehicle Work Group Bridge (WGB)	Autonomous AP Software 15.3.3 - JK2
Mobile Mark RM3-2400 Antenna	2.4 GHz Vibration Resistant Antenna for Cisco WGB on Autonomous Vehicle	N/A
Cisco IE-3400	Ruggedized Access Switch used behind WGB onboard vehicle	Cisco IOS XE 16.12.01
Cisco IE 4000	Mine Infrastructure Switch with Fiber ports	Cisco IOS 15.2(4)EA9, Release software (fc2)
Catalyst 9300	Control Room Distribution Layer Switch	Cisco IOS-XE 17.1.1

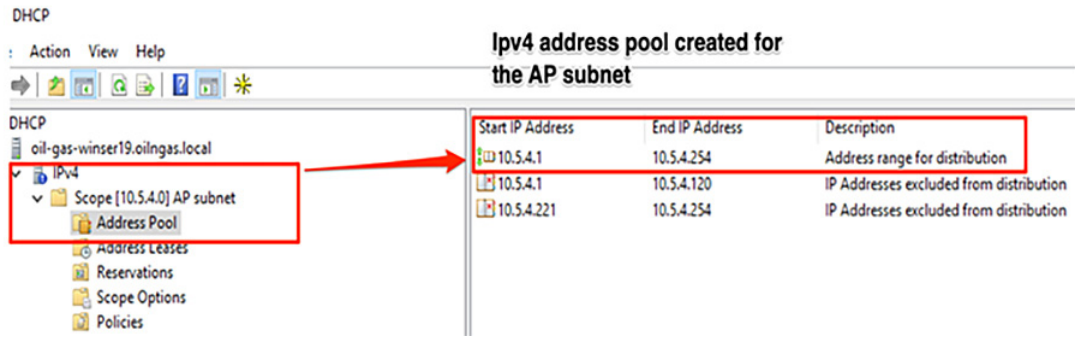
Figure 42 Validation Testbed Layout



IP Addressing and DHCP

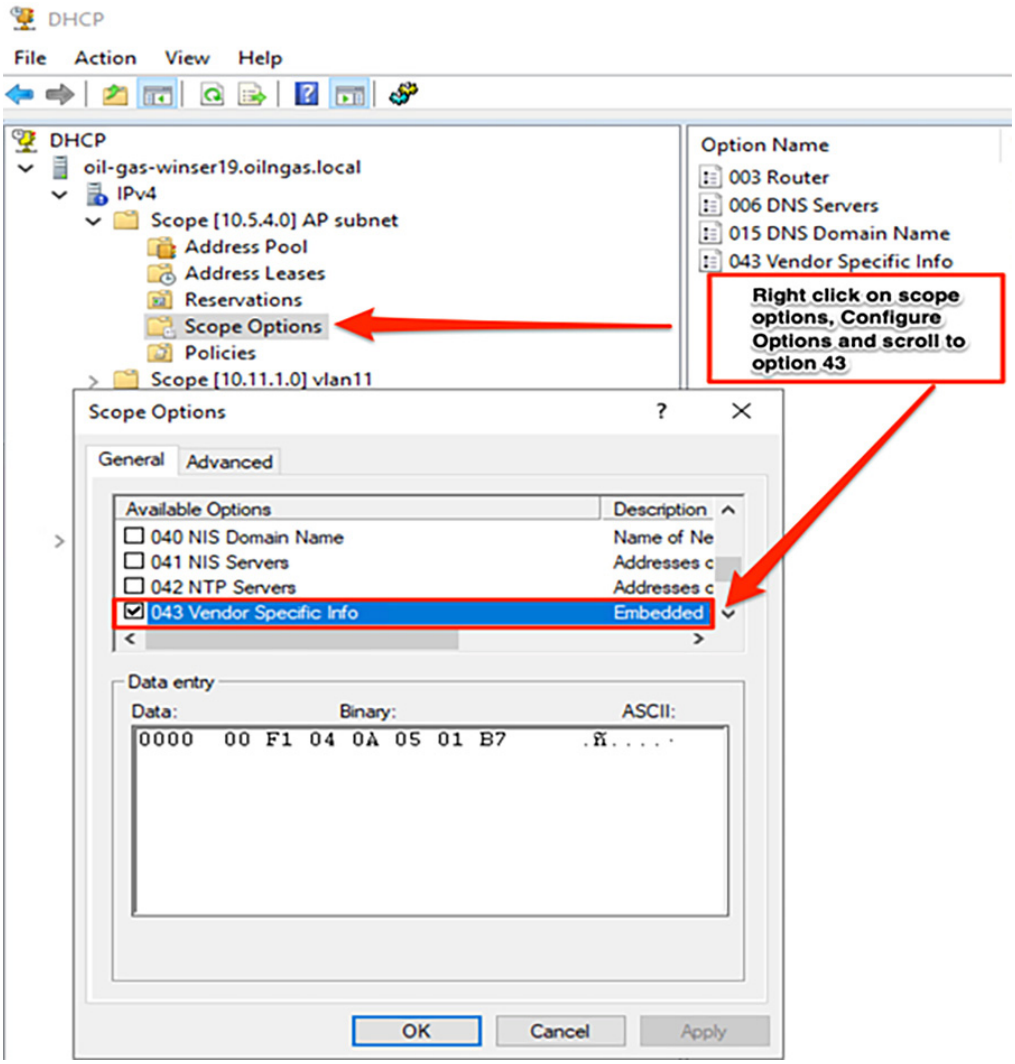
In preparation to on-board the infrastructure APs, a DHCP pool needs to be created corresponding to the AP management subnet within your DHCP server. Within the lab environment, a Microsoft Active Directory based DHCP Server (Windows Server 2019 Edition) was deployed. The DHCP pool was configured with an Option-43 value pointing to the WLC IP. The infrastructure APs use DHCP Option 43 for WLAN Controller Discovery when the WLC is in a different subnet than the AP.

Figure 43 AP Subnet dhcp pool



The following references the option 43 parameter added for the 10.5.4.0 subnet.

Figure 44 DHCP option 43 for AP subnet



Note: TLV values for the Option 43 sub-option: Type + Length + Value. Type is always the sub-option code 0xf1. Length is the number of controller management IP addresses times 4 in hex. Value is the IP address of the controller listed sequentially in hex. In this reference topology the controller management IP address is 10.5.4.183. The type is 0xf1. The length is 1 * 4 = 4 = 0x04. The IP address translates to 0a0501b7, therefore when the string is assembled, it yields f1040a0501b7

Note: This guide does not cover adding the DHCP server role and creating DHCP pools on the Microsoft Windows Server. For examples on adding the DHCP server role to your AD Server please refer to the relevant Microsoft documentation.

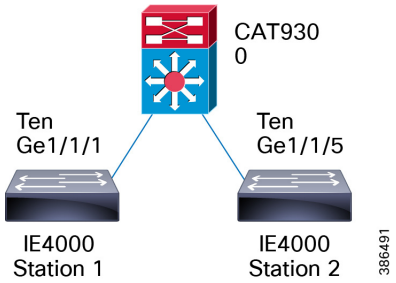
Switch Configurations

The Cisco IE 4000 switch provides highly secure access and industry-leading convergence ring protocols to support a resilient and scalable network access layer adhering to industrial compliance requirements. In the reference figure the IE4000 is used to provide wired network connectivity to the Mine Aggregation switch and provide POE+ in-line power to the Cisco IW3702 infrastructure access points. The access points utilize the Layer-2 CDP feature to negotiate the power draw from the IE 4000 switchport.

Configure Trunks between switches

A trunk is a point-to-point link two switches. Trunks carry traffic for multiple VLANs over a single link and allows one to extend VLANs across an entire network. To correctly deliver traffic to a trunk port with several VLANs, the device uses the IEEE 802.1Q encapsulation (tagging) method that uses a tag that is inserted into the frame header. This tag carries information about the specific VLAN to which the frame belongs. This allows for traffic from several different VLANs to traverse the same link while maintain Layer-2 segmentation of traffic across the trunk link.

Figure 45 Access Layer Switch to Distribution Layer Switch Trunk



Cat-9300 configuration towards the IE 4000 Switches

Configuration below depicts the trunk configuration for the Cat-9300 switch to the IE 4000 switches.

```
9300-mine-switch#
!
interface TenGigabitEthernet1/1/1
  description Connected to IE4K-1
  switchport trunk allowed vlan 100,104
  switchport mode trunk
!
interface TenGigabitEthernet1/1/5
  description Connected to IE4K-2
  switchport trunk allowed vlan 100,104
  switchport mode trunk
!
```

IE 4000 configuration towards Cat-9300

Configuration below depicts the trunk from the IE 4000 switch to the Cat-9300 switch.

```
IE 4000-1#
!
interface GigabitEthernet1/1
  description Connected to 9300-mine-switch
  switchport trunk allowed vlan,100,104
  switchport mode trunk
!
```

IE 4000 switchport configuration for Infrastructure APs:

The IE 4000 port connected to the infrastructure AP can be as configured as an access port within the AP management VLAN. Since the AP forms a CAPWAP tunnel with the controller all client (VLAN-tagged) traffic traverses the CAPWAP tunnel and hence there is no need to configure the switchport as a trunk.

IE 4000 port configuration towards the Infrastructure AP:

```
!
interface GigabitEthernet1/14
  description Connected to IW3702-Infra-AP-1
  switchport access vlan 104
  switchport mode access
!
```

The above needs to be configured on each IE 4000 port which has an infrastructure AP connected to it.

Distribution Switch (Cat-9300) Configuration

VLANs divide broadcast domains in a LAN environment. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. On Catalyst switches it is accomplished by the creation of Layer 3 Switched Virtual Interfaces (SVIs). In the reference topology the catalyst 9300 is the Layer-3 mine aggregation switch responsible for inter-vlan routing (or Layer-3 routing).

Enabling IP Routing on Mine Aggregation Switch:

```
9300-mine-switch#
!
! IP routing must be enabled to route traffic between Vlans
ip routing
!
```

Creating Client VLAN-11 on Mine Aggregation Switch:

```
9300-mine-switch#
!
vlan 11
  name client-vlan-11
!
```

Creating required VLANs and SVIs on Cat-9300

```
9300-mine-switch#
! OOB Management Network
interface Vlan1
  ip address 192.168.251.175 255.255.0.0
!
! SVI for Wireless Client subnet
interface Vlan11
  ip address 10.11.1.1 255.255.255.0
!
! Inband Mgmt vlan for network devices (wlc, dhcp, etc)
interface Vlan100
```

```
 ip address 10.5.1.1 255.255.255.0
!
! SVI for AP Management Subnet. APs getting their IP from the DHCP Server, hence need to
configure the ip-helper address command to point to the DHCP server. IP helper can address
can be useful as it forwards UDP broadcasts, including bootp and dhcp. It can be helpful
when the dhcp server is not on the same layer 2 subnet. In this scenario the helper is the
dhcp server address.
interface Vlan104
  ip address 10.5.4.1 255.255.255.0
  ip helper-address 10.5.1.185
```

Cat-9300 Configuration towards Cat-3850

```
9300-mine-switch#
!
interface TenGigabitEthernet1/0/48
description connected to 3850-mine-dc
switchport mode trunk
auto qos trust dscp
spanning-tree portfast trunk
!
```

Cat-3850 Configuration towards Cat-9300

```
3850-mine-dc#
!
interface GigabitEthernet1/0/24
  description connected to 9300-mine-switch
  switchport trunk allowed vlan 11,100,104
  switchport mode trunk
  auto qos trust dscp
  spanning-tree portfast trunk
!
```

WLC switchport configuration on Cat-3850

Each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. If you configure an interface to use the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the controller to be untagged.

```
3850-mine-dc#
!
interface GigabitEthernet1/0/8
 description connected to wlc
 switchport trunk native vlan 100
 switchport trunk allowed vlan 11,100,104
 auto qos trust dscp
switchport mode trunk
!
```

Quality of Service (QoS)

In environments such as underground mines, different types of applications are in use: some of which may require special prioritization in regard to the traffic requirements. In such scenarios voice, safety, video traffic flowing in the ingress/egress direction may need to be classified in accordance to the site guidelines.

Auto-QoS was used in this topology to simply the deployment of QoS Features. Auto-QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows. The switch employs the MQC model. This means that instead of using certain global configurations, auto-QoS applied to any interface on a switch configures several global class maps and policy maps.

Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue. For an in-depth overview of configuration please see the following QoS Configuration Guide.

To help ensure optimum QoS performance, you should configure QoS on all devices in your network. In this validation, the following configuration was used as a reference.

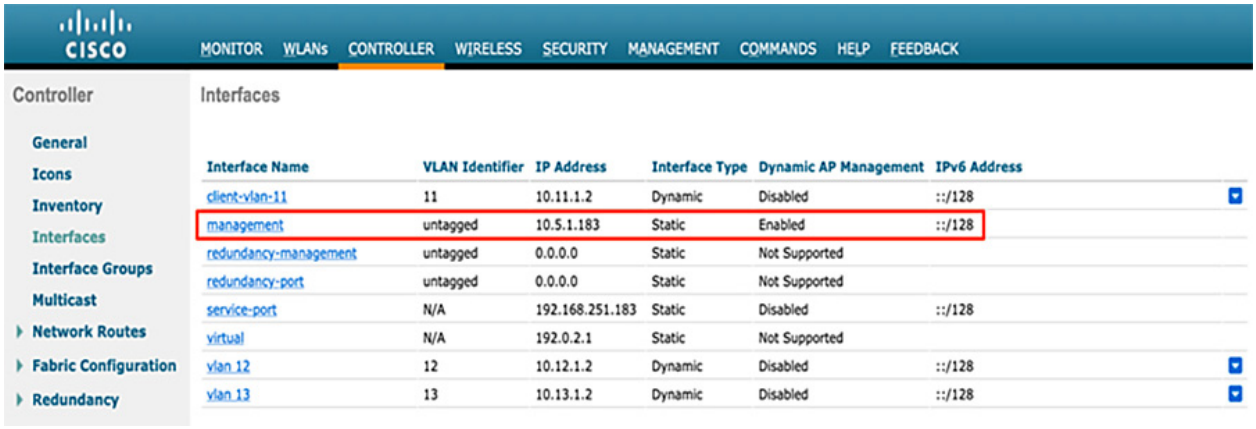
```
9300-mine-switch#
!
interface TenGigabitEthernet1/0/48
 description connected to 3850-mine-dc
 switchport mode trunk
 auto qos trust dscp
 spanning-tree portfast trunk
!
```

WLC Configuration

WLC Interfaces

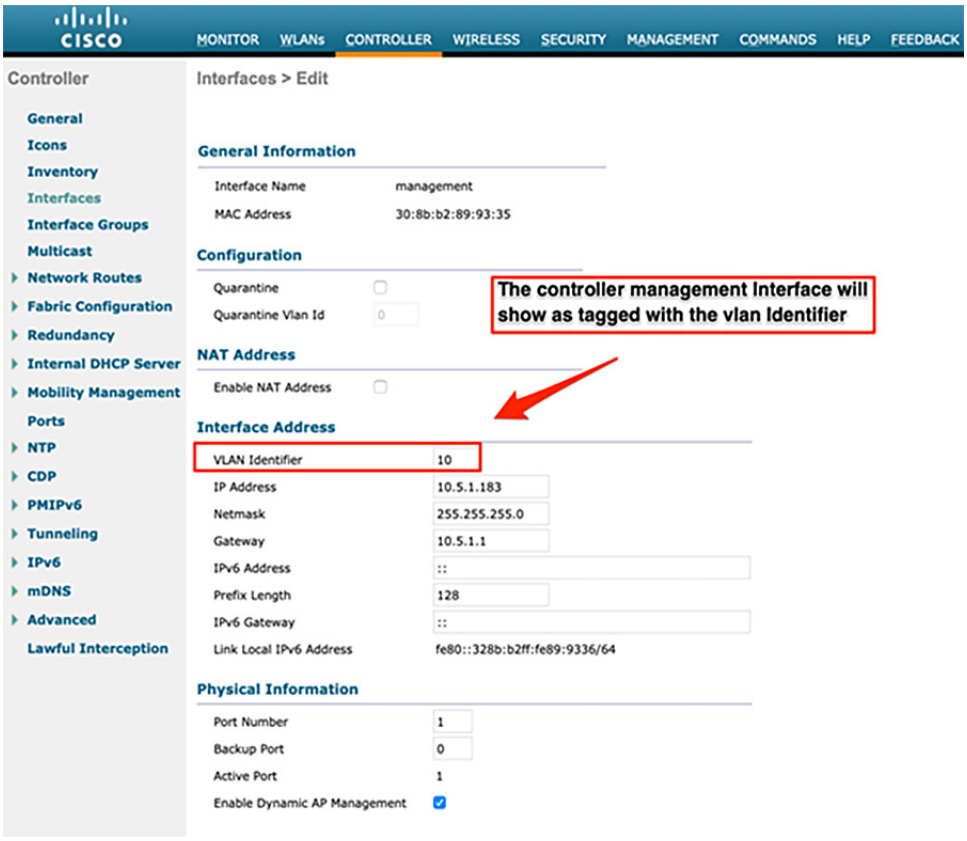
The management Interface is the Interface that the APs will use to join the WLC. The APs do not need to be in the management VLAN to join the WLC.

Figure 46 WLC Untagged Interface Configuration



Note: Figure 5 shows the management interface as untagged in this topology as the switchport configuration is tagged with a native vlan of 100 as shown in the previous example. However, Cisco recommends tagged management interfaces and the switch port configuration will need to be configured as a trunk but without the native vlan ID.

Figure 47 Tagged Management Interface Configuration

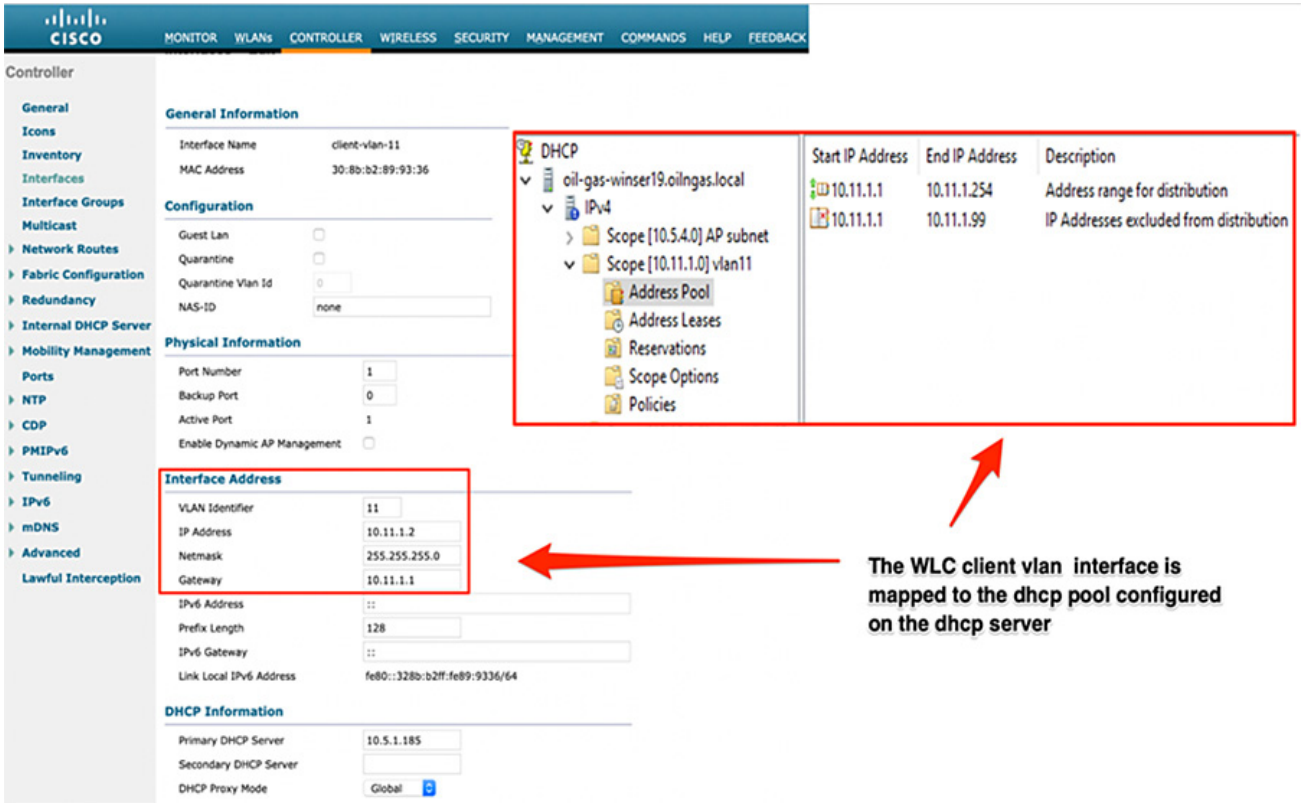


WLC Client VLAN Interface and DHCP Scope

Next, an interface needs to be created on the WLC and associated with the client VLAN/subnet. This is achieved by navigating to **Controller > Interfaces**.

If certain clients within this subnet expect to receive an IP address using DHCP, a corresponding DHCP scope needs to be created on the DHCP server. Make sure to exclude a range of IP addresses from the pool to use for static IP address assignment.

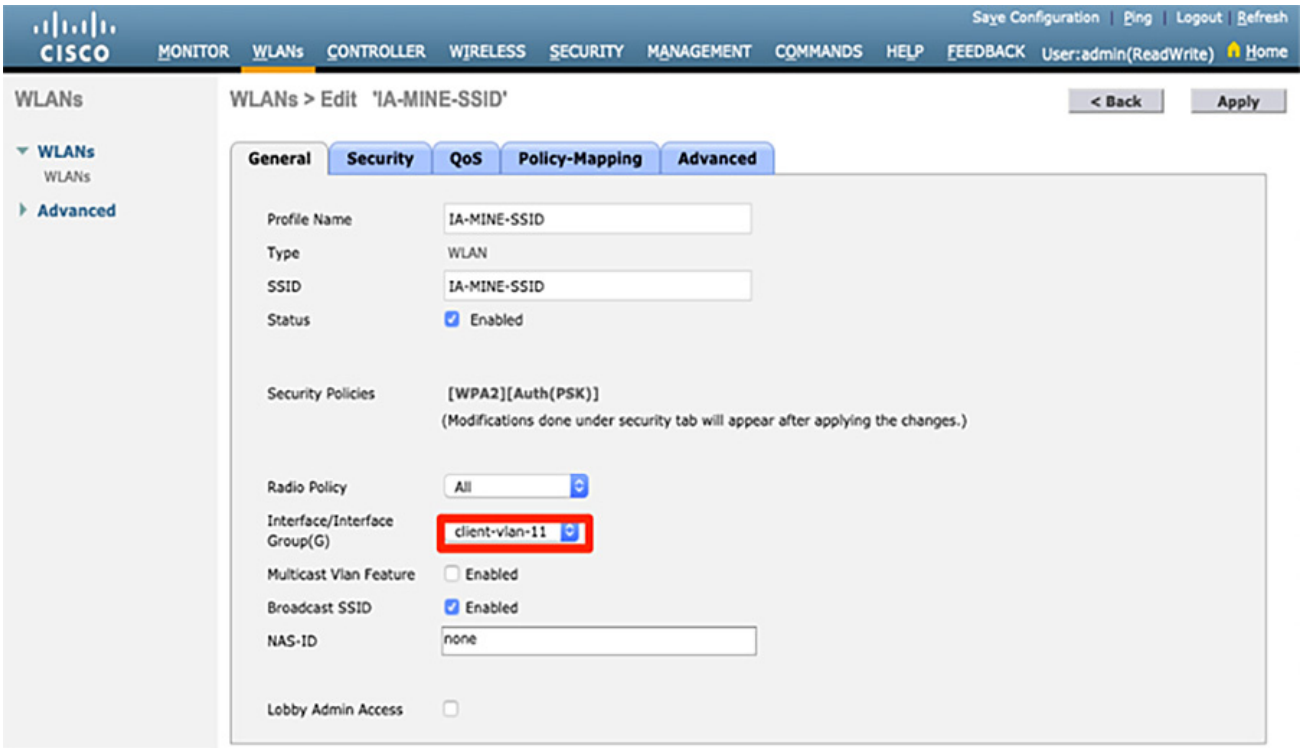
Figure 48 WLC Client Interface and corresponding DHCP Scope configuration



Automine WLAN General Settings

Next we need to create our WLAN SSID (“IA-Mine-SSID”) for the autonomous vehicle WGB to connect to. This is achieved by navigating to WLANs > WLANs. Make sure to “Enable” this SSID once correctly configured. This SSID needs to be mapped to the client VLAN interface “client-vlan-11” created above. Next, we need to broadcast this SSID so that it is advertised within the underground mine.

Figure 49 WLC WLAN General Configuration



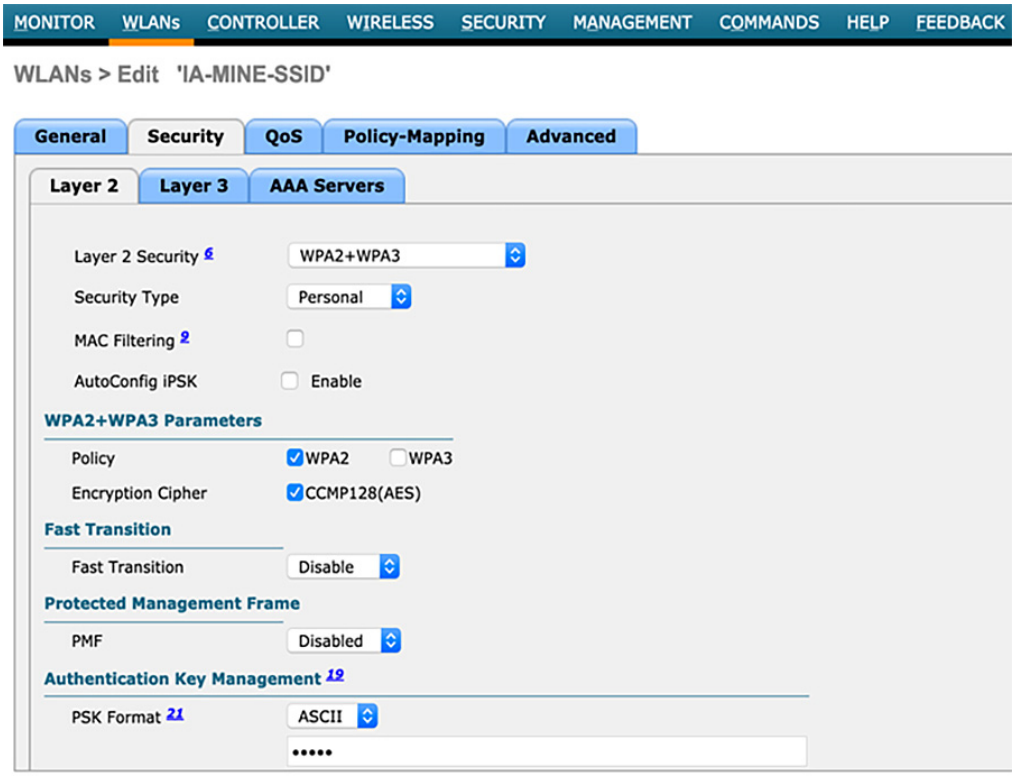
Automine WLAN Security Settings

The Layer 2 Security for the "IA-MINE-SSID" WLAN is configured to use pre-shared key (WPA2-PSK) authentication. Layer 2 Security is set to WPA2+WPA3. Security Type is configured as Personal. WPA2+WPA3 Parameters use WPA2 as the Policy and the Encryption Cypher is CCMP128 (AES). Fast Transition is set to Disabled, since it is not supported by the WGB. Protected Management Frame is set to Disabled. Configure the desired PSK string of at least 8 characters to a maximum of 63 characters and enable the PSK setting.

To get to the L2 Security settings, navigate to WLANs > WLANs > Select "IA-MINE-SSID" > Security > Layer 2.

Note: When configuring the PSK on the WGB, make sure to match what is configured on the WLC. If not, the authentication between the WGB and the infrastructure will fail resulting in the WGB not being able to gain wireless network access.

Figure 50 WLC WLAN Security Layer 2 Configuration

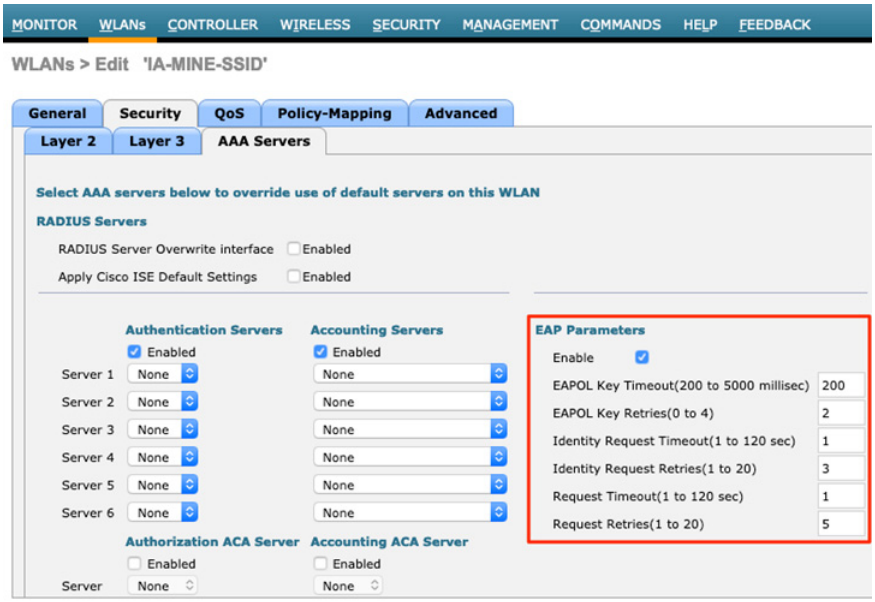


WLAN EAP Settings

The following EAP parameters need to be configured to optimize roam-times for the WGB on the autonomous vehicles. An EAPOL key timeout of 250ms is recommended to help ensure proper key exchange between the WLC and the WGB client.

Note: The same parameter options are also found under the **Security> Advanced EAP** tab, however, if there are no WLAN specific EAP parameters applied then the global settings will be used.

Figure 51 WLAN EAP Settings



EAPOL Key Retries – Currently using the default value of 2, the AP will attempt to send the key to the client 2 times before de-authentication if there is no response. A max value could cause a prolonged de-authentication message which delays the 802.1x process.

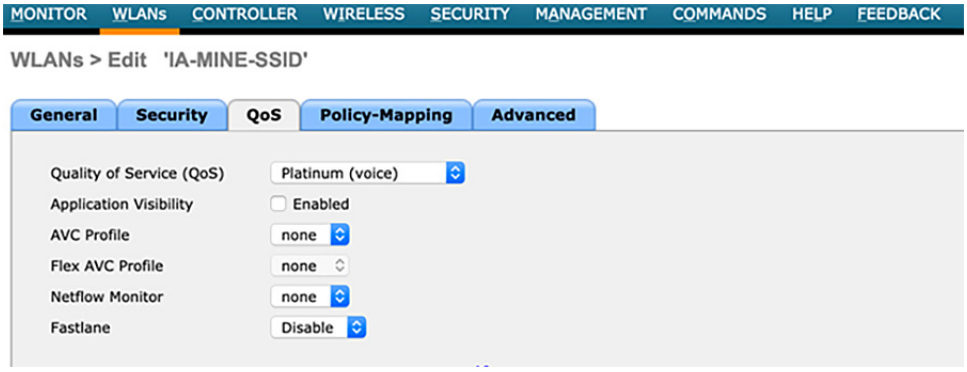
Identity Request Timeout – This affects how long we wait between EAP identity requests. Currently the value of 1 is being used, which means the controller will wait 1 second between requests. his affects new connections and roaming.

Identity Request Retries – This is the number of times the WLC will send the Identity Request to the client, before removing its entry from the MSCB. Once the Max Retries is reached, the WLC sends a de-authentication frame to the client, forcing them to restart the EAP process.

Automine WLAN QoS Settings

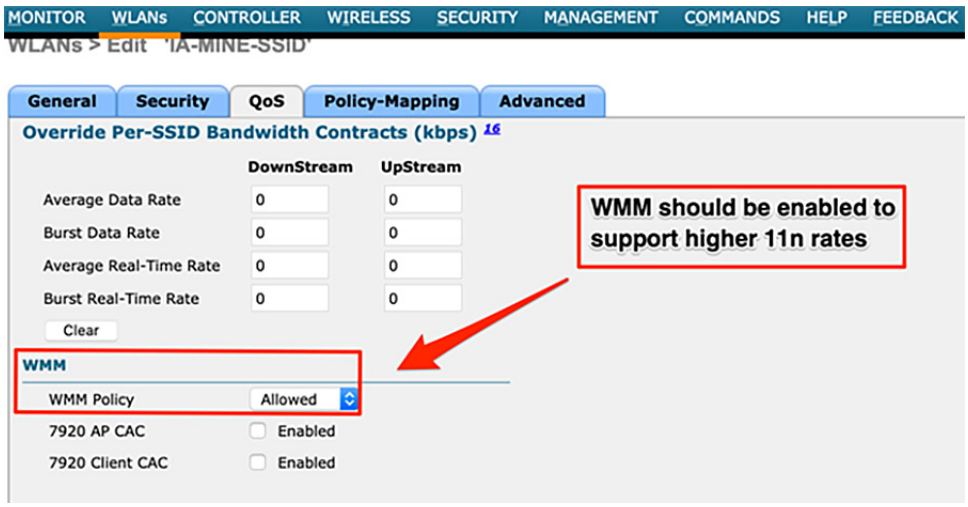
Set the Quality of Service (QoS) to Platinum (voice).

Figure 52 WLC WLAN QoS Configuration



Set WMM Policy to Allowed.

Figure 53 WLC WLAN QoS Configuration



Automine WLAN Advanced Settings

Under the WLAN Advanced tab configure the following settings.

- Enable Session Timeout is Disabled.
- Aironet IE is Enabled.
- P2P Blocking Action is Disabled.
- Client Load Balancing is Disabled.
- Client Band Select is Disabled.
- Passive Client is Enabled.
- Scan Defer Priority is Enabled for 0, 1, 2, 3, 4, 5, 6, & 7.
- Scan Defer Time (msecs) is set to 10000.

Figure 54 WLC WLAN Advanced Configuration

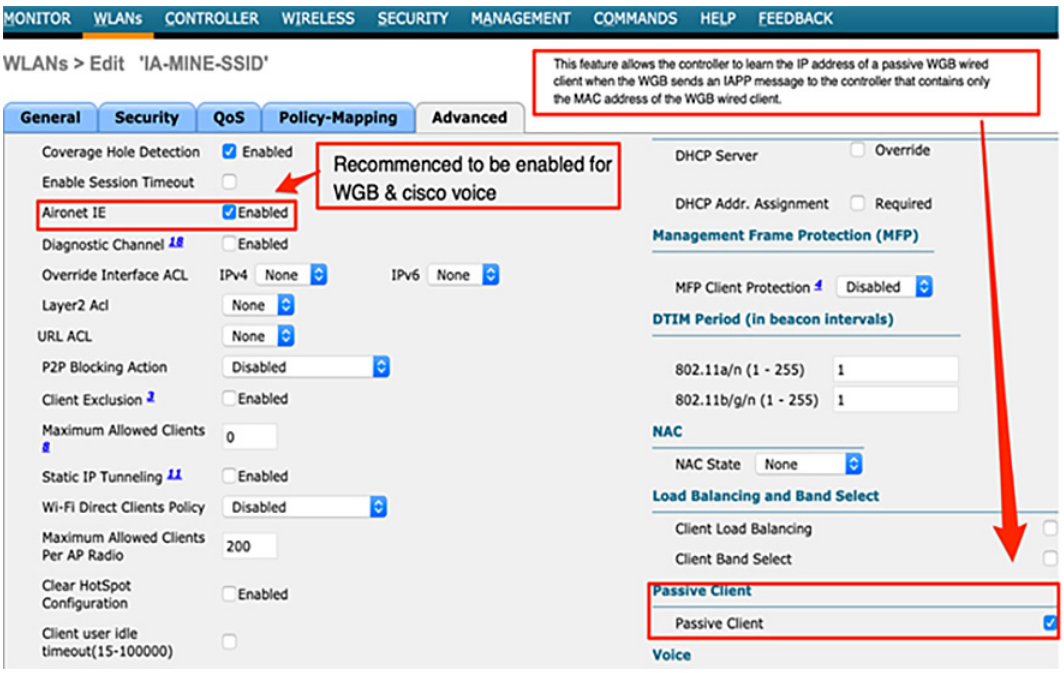
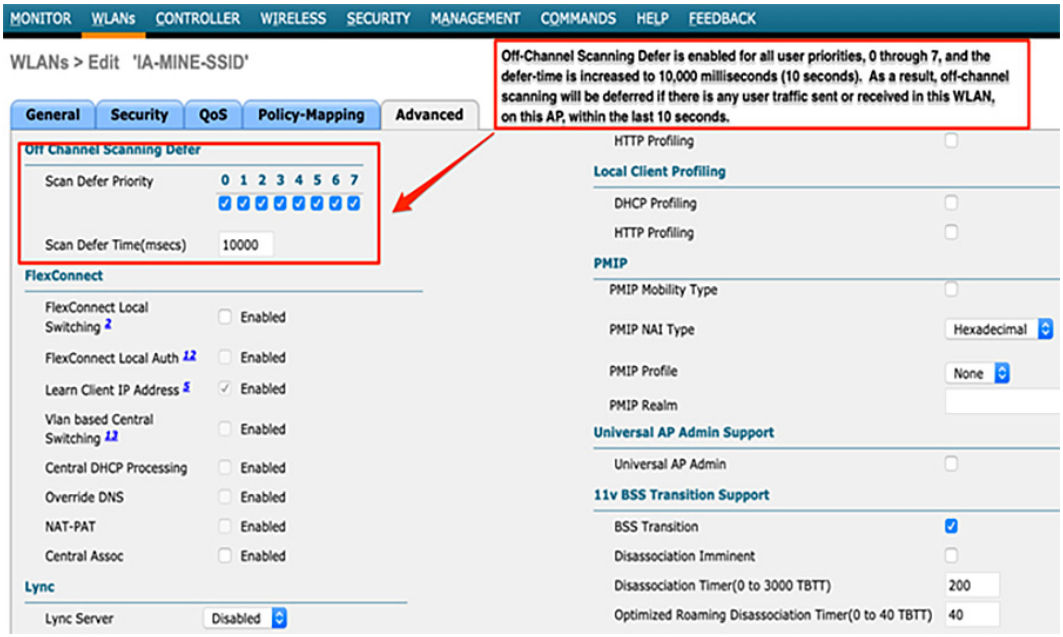
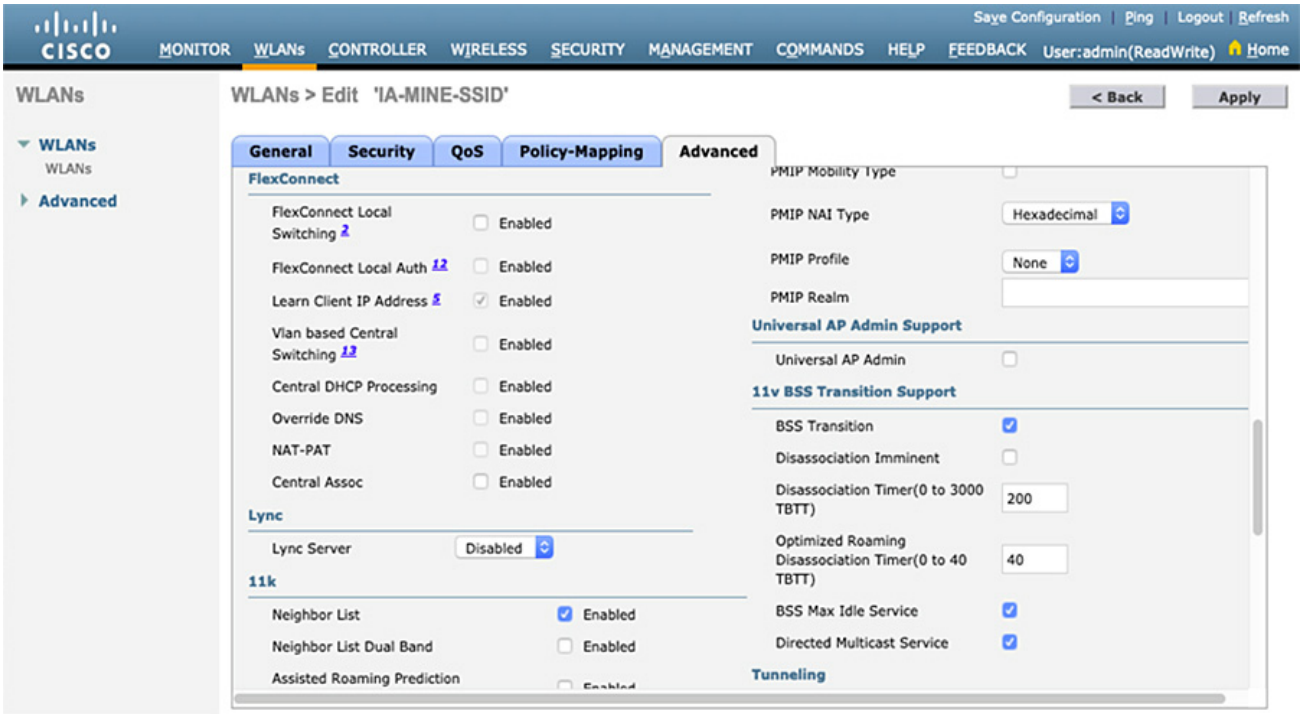


Figure 55 WLC WLAN Advanced Configuration



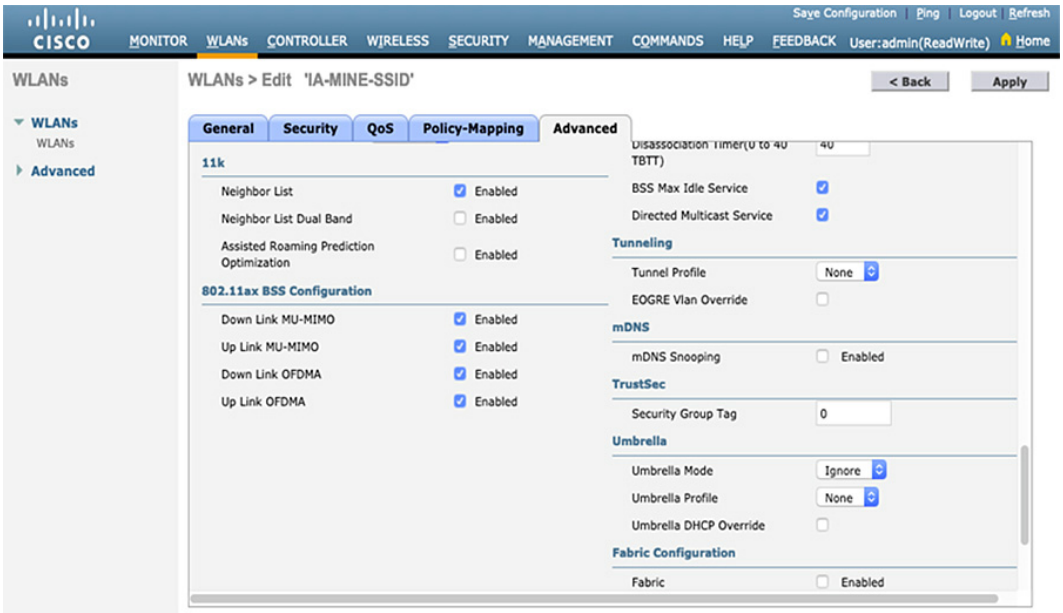
It is recommended to configure the scan defer time to a value large enough to allow minimum loss of critical packets, like Sandvik ACS safety traffic between the autonomous vehicle to the control room and from the control room to the ACS safety curtains.

Figure 56 WLC WLAN Advanced Configuration continued



Note: Some settings such as Neighbor list (802.11K), BSS Transition support (802.11V), Coverage hole Detections are enabled by default.

Figure 57 WLC WLAN Advanced Configuration continued



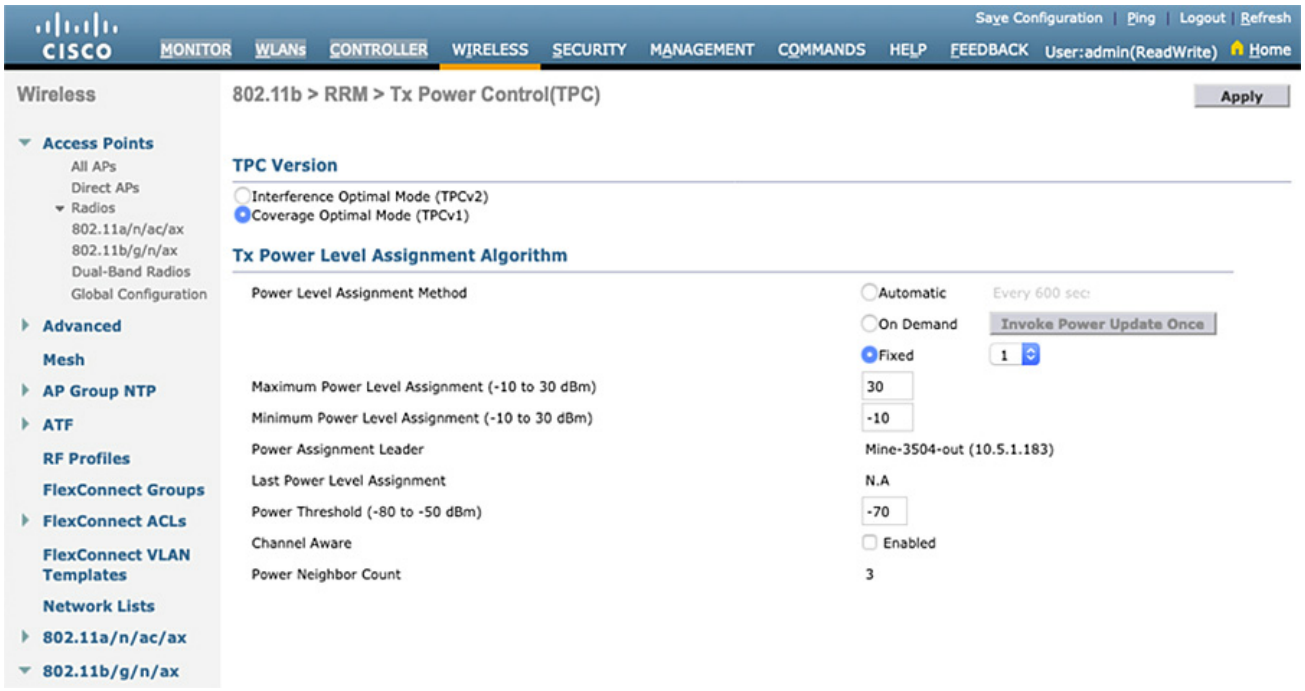
Cisco CleanAir

Cisco CleanAir event-driven radio resource management (RRM) is not recommended for use in this scenario. Not deploying it results in a more deterministic wireless environment by using manual static channel assignments and power-control settings.

Transmit Power Control

Transmit Power Control (TPC) is recommended to be turned off and to use manually selected fixed transmit power. Each AP should have their power level configured to a static value to provide deterministic coverage. The transmit power-level that needs to be configured for each AP should be based on the analysis of the results obtained from the RF site-survey for your underground mine.

Figure 58 WLC Global Tx Power Control (TPC) Settings

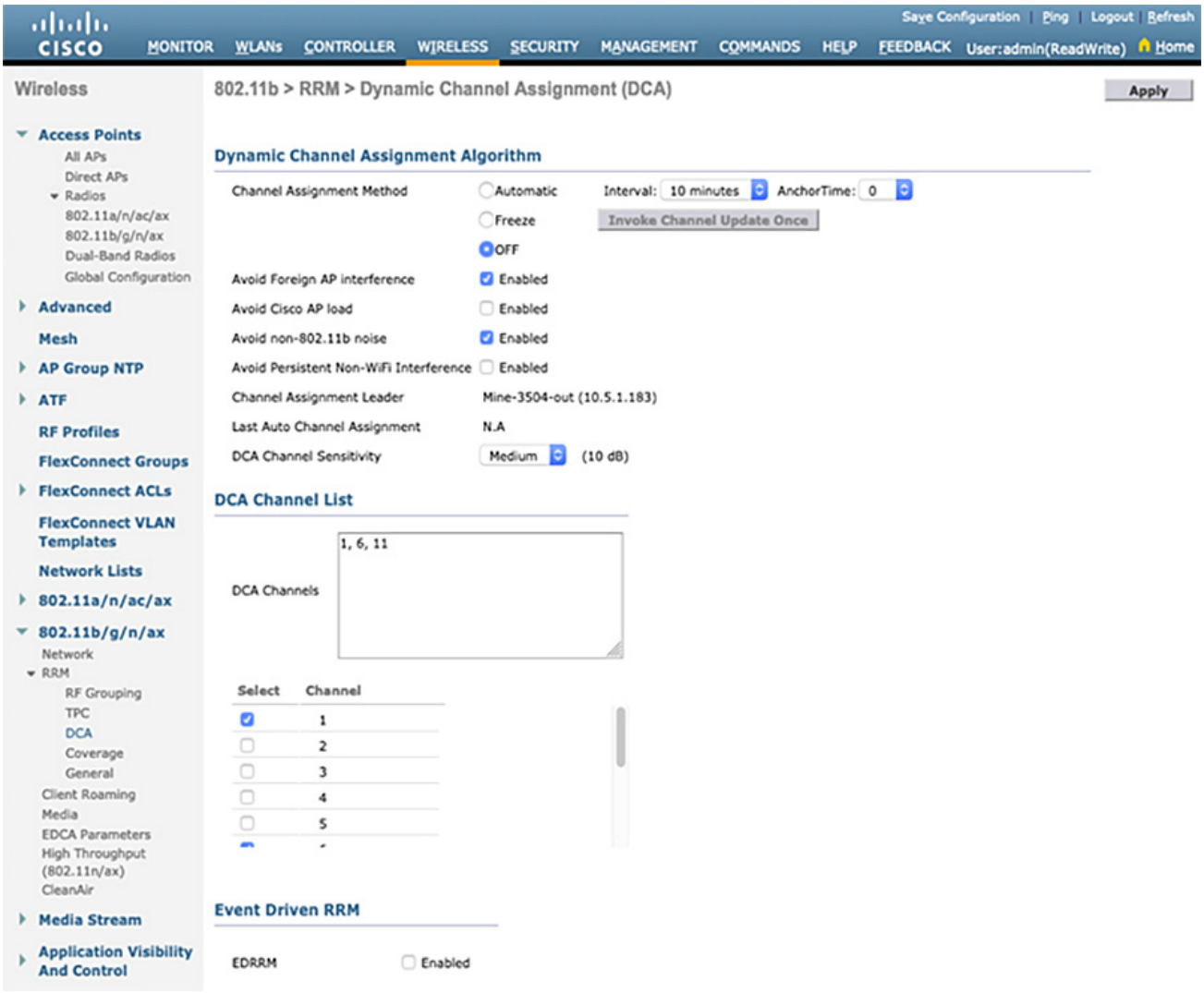


Static Channel Assignment

The Dynamic Channel assignment is recommended to be turned off and all APs should be set to use manual channel assignment according to the network plan (Channels 1,6,11 should be used within the 2.4GHz frequency band). Each AP should have their channel assignment configured statically. The channel that needs to be configured for each AP should be based on the analysis of the results obtained from the RF site-survey for your underground mine.

As depicted in the figure below, disable DCA by navigating to Wireless > 802.11b/g/n/ax > RRM > DCA. Configure the “Channel Assignment Method” to “OFF”. This will disable the Dynamic Channel Assignment and allow one to statically assign a specific channel to each of the infrastructure APs within the underground mine.

Figure 59 WLC – Disabling DCA

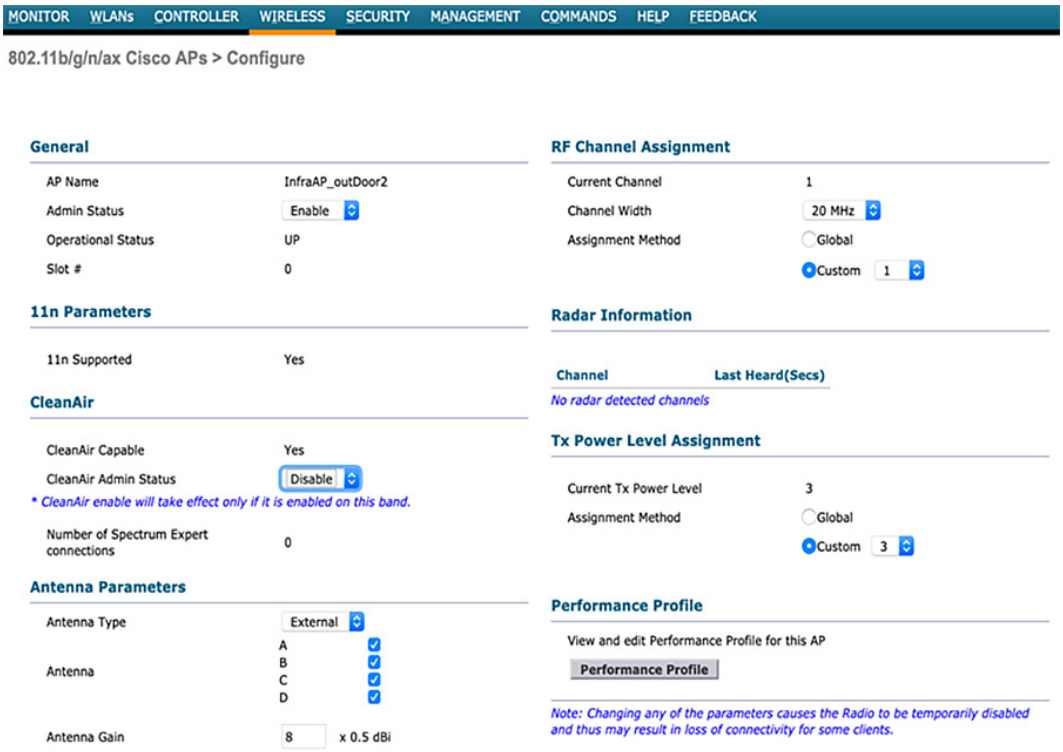


AP 2.4 GHz RF Settings

Configure each AP with a static transmit power and channel assignment of either 1,6, or 11 within the 2.4GHz frequency band based on analysis of the RF site survey results. To configure static channel assignment leverage the Custom Assignment Method within the RF Channel Assignment tab for a particular AP, and configure the needed channel for the AP. Similarly, in order to configure a static Tx Power Level for the radio, leverage the Custom Assignment Method and set an appropriate power level.

As depicted in the figure below, this particular AP has been assigned a static 2.4GHz channel of “1” and a Tx Power Level of “3”.

Figure 60 2.4 GHz Infrastructure AP Radio Configuration



802.11b/g Global Parameters

Beacon Period

According to the IEEE 802.11 standard, every compliant Access Point (AP) periodically sends out management frames called beacon frames. The purpose of beacon frames is to advertise the presence of an AP in an area, its SSID, capabilities, and some configuration and security information to the client devices. The time interval between two consecutive beacon frames is called the beacon interval. The beacon interval is measured in Time Units (TUs), where each TU equals 1024 microseconds, so the default period between beacons is approximately 100 milliseconds. Beacon interval is a configurable parameter on Cisco APs.

Within challenging RF environments, the WGB could potentially miss the AP beacon message(s) when it moves to a specific location. This can result in unexpected roaming. If the WGB can't see consecutive beacons for several hundred milli-seconds, the WGB assumes that it can't receive data packets and it should roam. In order to avoid un-expected roams within a challenging RF environment, we highly recommend to increase the beacon interval period from the default value of 100 mSec in order to decrease the possibility of consecutive missing BEACON packets and thus avoiding unexpected roaming.

During testing we found that a Beacon Period value of 1000 mSec is optimal.

Note: The beacon interval period can be adjusted to a lower value depending on the RF characteristics of the mine in which the solution is being deployed.

Data Rates

Mandatory/supported data-rates are based on application requirements. For Sandvik AutoMine each WGB client installed on an autonomous vehicle requires a minimum data-rate of 10Mbps. Keeping this in mind we need to disable some of the lower data-rates below 10Mbps to satisfy the Automine application requirements.

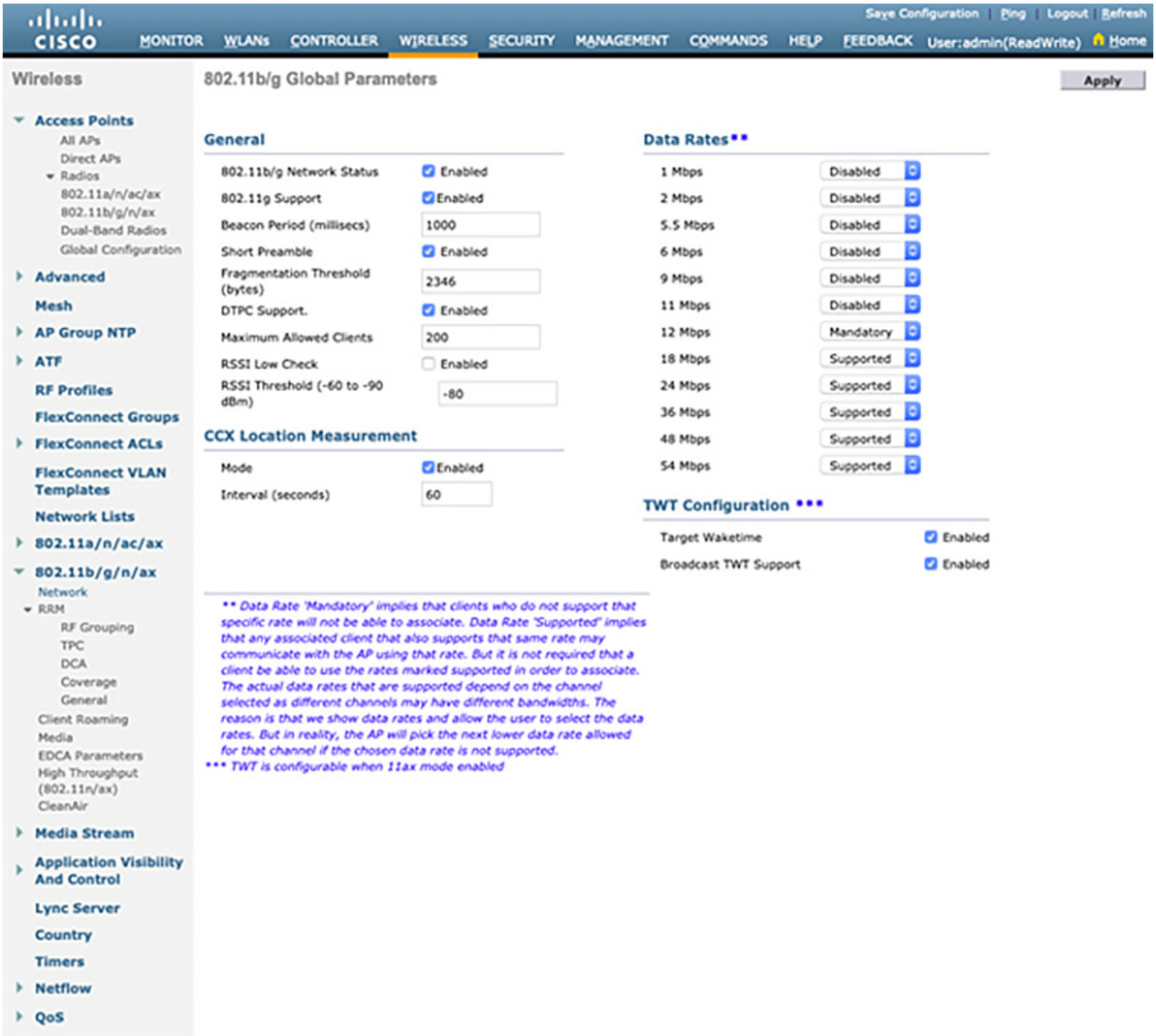
- **Mandatory Data Rates** - Clients must support this data rate in order to associate to an access point on the controller.

- **Supported Data Rates** – Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.

The 802.11b/g Data Rates of 1, 2, 5.5, 6, 9, & 11Mbps should be disabled. Data Rate of 12Mbps should be set to Mandatory since this is the lowest data-rate at which we want the WGBs to communicate. Data Rates of 18, 24, 36, 48, 54 Mbps should be set to Supported. This can be configured under the Data Rates section under Wireless > 802.11b/g/n/ax > Network > 802.11b/g Global Parameters.

Note: A note about mandatory data rates: The lowest mandatory data rate is used to transmit management frames. The highest mandatory data rate is used to transmit multicast/broadcast frames. In order to be able to associate with the infrastructure AP, the client must have the ability to support at least the mandatory data rates.

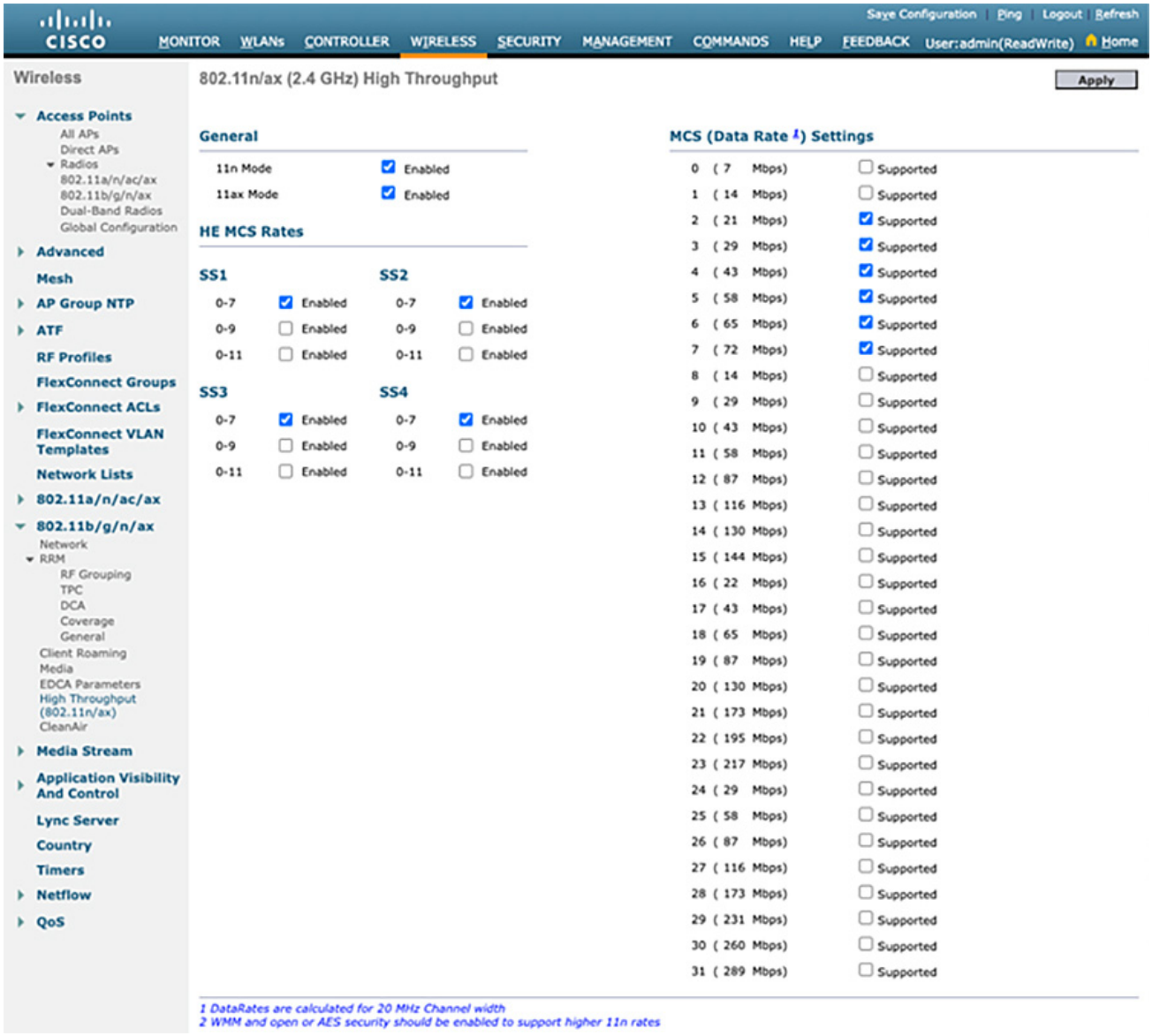
Figure 61 WLC 2.4GHz Data Rates



802.11n/ax (2.4 GHz) High Throughput

Set the MCS Data Rates 2, 3, 4, 5, 6, 7, and 54 Mbps to “Supported”. All other MCS Data Rates should not be set to “Supported”. MCS-0 and MCS-1 are disabled on the WGB.

Figure 62 WLC 2.4GHz Spatial Streams and MCS Data Rates



WGB Global Configuration

The snippet below depicts the WGB Global configuration.

The ***dot11 pause-time*** global configuration command is used to set TX pause duration after consecutive TX failure. The default, and also the maximum, value is 100 ms. The minimum is 10 ms. For our use-case we set this value to the lowest value of 10 mSec which makes the radio recover faster when multiple retries fail.

Next configure a static IP address for the BVI interface. The static IP address is assigned from the Client VLAN-11.

If a wired client behind the WGB does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid traffic loss, prevent the wired clients that are part of bridge-group "1" from being removed from the bridge table by configuring an extended aging-out timer of **1000000** seconds. It is recommended configuring the seconds parameter to a value greater than the wired client's idle period.

Next configure the NTP server with a source interface of the BVI interface.

```
! When multiple retries fail, the radio pauses for a certain time. Default time is
100 msec.
! Configuring it to 10 msecs will make the radio recover quicker from that situation.
dot11 pause-time 10
!
! Static IP address assignment for WGB BVI interface from Client VLAN/subnet.
interface BVI1
 ip address 10.11.1.93 255.255.255.0
 arp timeout 6000
!
! Large aging-out timer value for WGB wired clients
bridge 1 aging-time 100000
!
! NTP configuration
sntp server 10.11.1.1
sntp source-interface BVI1
!
```

WGB 5GHz Radio Configuration

The below snippet depicts the configuration needed for the 5GHz radio.

```
! Places the 5 GHz radio in station-role root and disables it. This allows for the 2.4GHz radio to then

! be put in workgroup-bridge mode.
interface Dot11Radio1
  station-role root
  shutdown
!
```

WGB 2.4 GHz Radio Configuration

The snippet below depicts the configuration for the 2.4 GHz radio in workgroup bridge mode with the relevant parameters.

For Sandvik AutoMine it is highly recommend using a roam-threshold value of -55dBm.

```
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 load-interval 30
 no shutdown
 !
 !


! Please configure the appropriate antenna gain value based on the antenna type and site survey   !
results analysis.
 antenna gain 9
 antenna ab-antenna
 stbc
! Disables packet aggregation for the Video Queue
```

```
 no ampdu transmit priority 4
 no ampdu transmit priority 5
 no amsdu transmit priority 4
 no amsdu transmit priority 5
! Long guard interval lowers the throughput but resists against the RF environment variation
 guard-interval long
 speed  basic-12.0 24.0 m2. m3. m4. m5. m6. m7.
!  The idea here is to configure a proper retry value (drop the packet as soon as the packet
!  retry reaches this value). This helps minimize consecutive packet loss.
 packet retries 8 drop-packet
! station role workgroup-bridge converts the radio to workgroup bridge mode.
 station-role workgroup-bridge
 mobile station scan 1 6 11
! A proper threshold could avoid unnecessary roaming, this is related to coverage.
 mobile station period 1 threshold 55
!
```

WGB Security using WPA2-PSK

Configure the WGB to use WPA2-PSK authentication and AES-CCM cipher-based encryption.

Note: Make sure to exactly match the pre-shared key that was configured on the WLC if not the WGB will fail authentication and will not be able to associate with the wireless infrastructure.

```
!
interface Dot11Radio0
  encryption mode ciphers aes-ccm
  ssid IA-MINE-SSID
!
dot11 ssid IA-MINE-SSID
   authentication open
   authentication key-management wpa version 2
! The below ascii PSK should be replaced with your PSK
   wpa-psk ascii 7 070E34584104100B1211021F0725
! It is recommended to disable client MFP if fast recovery times are needed (WGB to react to
non-protected de-authentication frames). This is a compromise between security needs and fast recovery
times. The decision depends on what is more important for the deployment scenario.
   no ids mfp client
```

WGB QoS Configuration

For the Sandvik AutoMine use-case the requirement is to assign the ACS safety traffic with the highest priority . To achieve this classify and mark ACS Safety traffic on UDP/6010 with Cos value of 5. An extended access-list is used to match UDP traffic on port 6010 and then a combination of class-map and policy-map is used to set a Cos value of 5 for the ACS safety traffic. The QoS service-policy is applied on the ingress to the WGB wired interface.

```
!
class-map match-all ACS_Safety_Traffic_Class_Map
 match access-group name ACS_Safety_Traffic
!
policy-map ACS_Safety_Policy_Map
 class _class_ACS_Safety_Traffic_Class_Map
  set cos 5
!
ip access-list extended ACS_Safety_Traffic
  permit udp any any eq 6010
!
interface GigabitEthernet0
 service-policy input ACS_Safety_Policy_Map
!
```

WGB Timer Configurations

To avoid a long EAP process timeout the eap-timeout timer needs to be set to a value of '2' seconds.

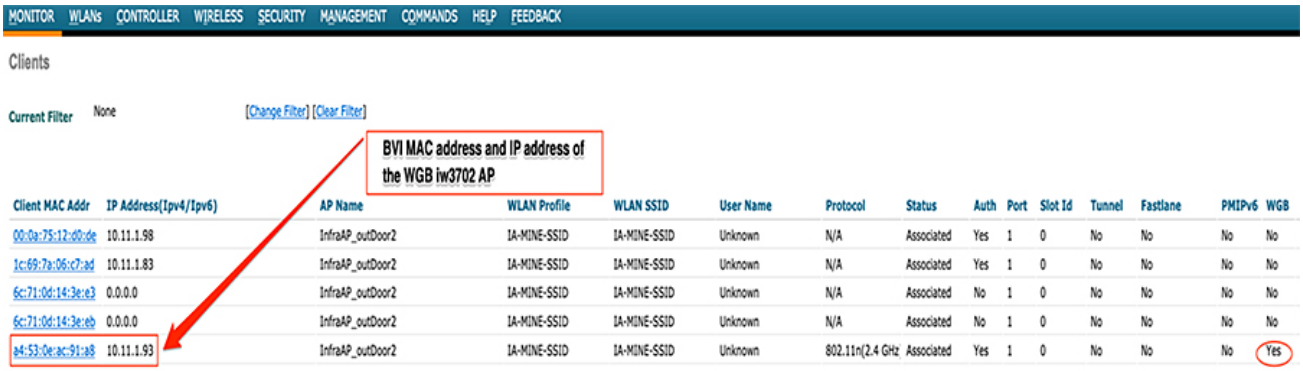
```
workgroup-bridge no_reset
workgroup-bridge unified-vlan-client
workgroup-bridge timeouts eap-timeout 2
workgroup-bridge timeouts iapp-refresh 10
workgroup-bridge timeouts auth-response 50
workgroup-bridge timeouts assoc-response 50
workgroup-bridge timeouts client-add 800
```

Verification Notes

Once the WGB and the WLC/APs have been configured appropriately, the WGB on the autonomous vehicle associates to the LWAP as a client. The status of the WGB(s) on the network can be viewed from the WLC UI.

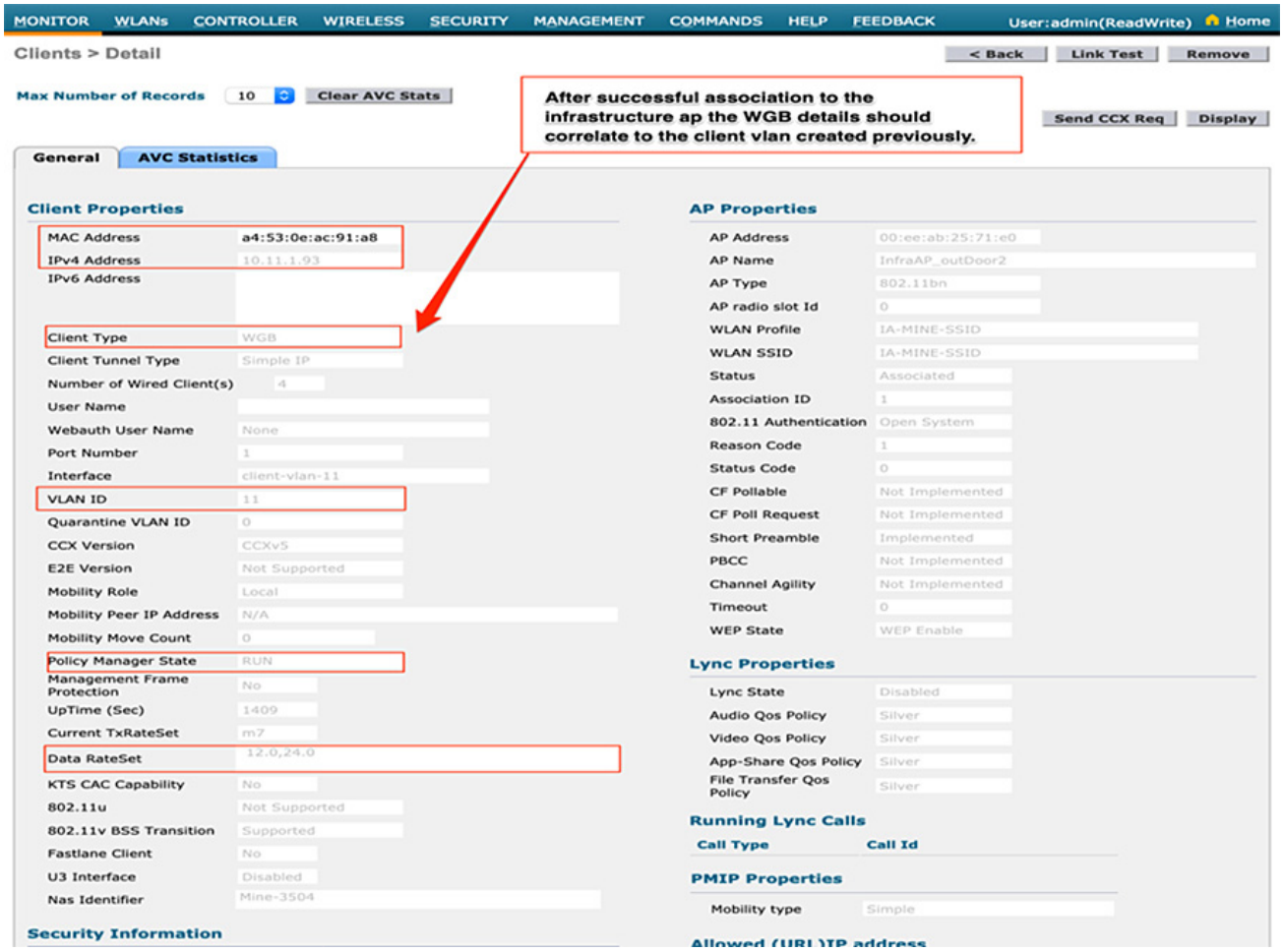
From the WLC UI, navigate to **Monitor > Clients** in order to view the wireless Clients. The WGB field on the right side of the page indicates whether any of the clients on the network are WGBs.

Figure 63 WGB as a client



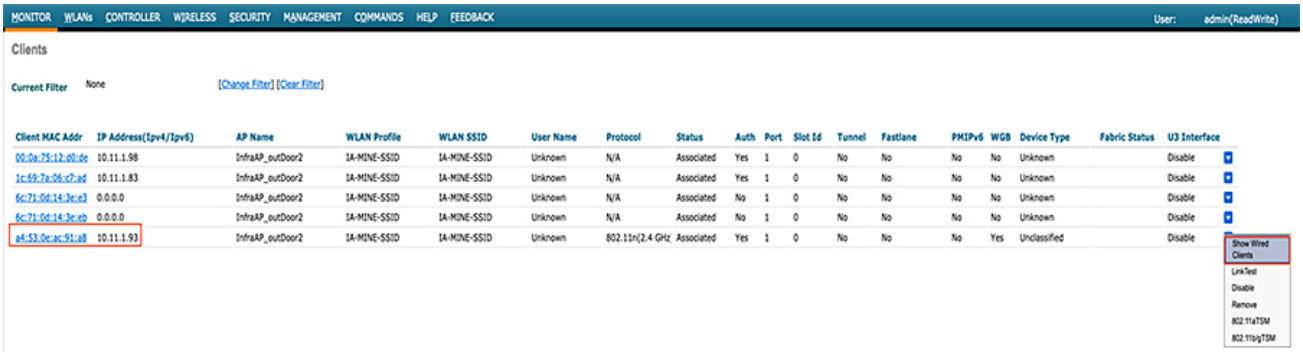
Click the WGB MAC address to view detailed information.

Figure 64 Client Detail for WGB



In order to view details for any of the wired clients that are connected behind a particular WGB, navigate back to the Clients page, hover your cursor over the blue drop-down arrow for the desired WGB, and select Show Wired Clients. The WGB Wired Clients page appears.

Figure 65 Viewing wired clients behind a particular WGB



Using the WLC CLI the “**show wgb summary**” command can be used to view the WGB(s) associated with the wireless network.

```
(Cisco Controller) > show wgb summary
```

```
WGB Vlan Client Support..................................... Enabled
Number of WGBs.............................................. 2

MAC Address       IP Address      AP Name                   Status    WLAN   Auth       Protocol
Clients
-----------------          --------------- -----------------                 ---------   --------
-------      ------------           ---------
a4:53:0e:ac:91:a8  10.11.1.93      InfraAP_outDoor2   Assoc        1        Yes    802.11n(2.4 GHz)
4
```

To view the connected wired clients behind a particular WGB use the WLC CLI "**show wgb detail <wgb_mac>**".

```
(Cisco Controller) > show wgb detail a4:53:0e:ac:91:a8

Number of wired client(s): 4

MAC Address IP Address            AP Name            Mobility   WLAN  Auth
------------------           ---------------    ----------------------     ----------     ------
-----
6c:71:0d:14:3e:e3   Unknown       InfraAP_outDoor2     Local         1         No
00:0a:75:12:d0:de  10.11.1.98      InfraAP_outDoor2     Local         1         Yes
1c:69:7a:06:c7:ad   10.11.1.83      InfraAP_outDoor2     Local         1         Yes
6c:71:0d:14:3e:eb   Unknown       InfraAP_outDoor2     Local         1         No
```

To view the list of active clients on a WGB, issue the "***show bridge***" CLI command.

```
WGB3# show bridge

Total of 300 station blocks, 291 free
Codes: P - permanent, S - self

Bridge Group 1:

    Address       Action   Interface       Age   RX count   TX count
000a.7512.d0de   forward   Gi0              P    28679258      21034
1c69.7a06.c2db   forward   Vi0             37          12          0
1c69.7a06.c7ad   forward   Gi0              0        2910       1199
f078.16fd.fe88   forward   Vi0              0        1451       1451
0024.9b2d.77f6   forward   Vi0              0       20773   28678879
308b.b289.9335   forward   Vi0              0        1684          0
0c75.bd89.9754   forward   Vi0             15          59         63
6c71.0d14.3eeb   forward   Gi0              0          19          0
6c71.0d14.3ee3   forward   Gi0              0       16991          0
```

To view the parent AP that a particular WGB is associated with issue the WGB CLI command "**show dot11 associations**".

```
WGB3# show dot11 associations

802.11 Client Stations on Dot11Radio1:

SSID [IA-MINE-SSID] :

MAC Address       IP address      IPV6 address                              Device
Name               Parent         State
00ee.ab25.71e0 10.5.1.183           ::                                        LWAPP-Parent
InfraAP_outDoor2         -             Assoc
```

Troubleshooting Notes

There is a common problem that has been observed mainly within Cisco IOS-Based workgroup bridge. When a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if the traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. In order to help avoid the traffic loss and removal of the wired client from the bridge table, use the following command in order to configure the aging-out timer on the WGB to a large value:

```
WGB3(config)#bridge 1 aging-time ?
  <10-1000000>  Seconds

WGB3(config)#bridge 1 aging-time 1000000
```

where bridge-group-number is a value between 1 and 255 and seconds is a value between 10 and 1,000,000 seconds. Cisco recommends configuring the seconds parameter to a value greater than the idle period of the wired client.

The "**debug dot11 dot11radio 0 trace print uplink txfail rcv**" debug command is useful to use on the WGB. This command takes you through the join process of a WGB, from scanning (if there are multiple parents), selection process for the parent, association and dot1x/PSK authentication (if configured) in phases.

```
WGB3# term mon
WGB3# debug dot11 dot11radio 0 trace print uplink txfail rcv
```

Appendix A: Wireless Mesh Deployment for Underground Mining

Wireless Mesh Considerations

For autonomous fleet management wireless mesh is not used. However, there are occasions within an underground mining environment where-in a mesh topology can be used the mine to extend network connectivity into areas which currently lack any sort of network connectivity. This section will cover these use cases.

Note: Wireless Mesh deployment has not been validated as part of this CVD effort and will be considered in a future version.

Two broad use cases are covered here:

- Use-Case 1: Expansion of the mine face or new tunnel drifts are created, and no infrastructure is in place and when there is a wired network failure.

  During a face expansion, several customers and partners have made self-contained mobile access points with batteries and other network devices to allow for temporary network connectivity until infrastructure can be expanded to the new area. The overall process is to configure the closest infrastructure Access Point(s) which has connectivity into the wired network into mesh mode with a role of Root Access Point (RAP) and configure the mobile as a Mesh Access Point (MAP) which wirelessly connects back to the RAP. In most cases the 5 GHz radio is used to connect the MAP to another MAP or to a RAP and the 2.4 GHz is used to service wireless clients at the mine face.

  Depending on the geographical terrain of the mine, directional antennas can be deployed for the RAP and MAP 5 GHz back-haul radios to help increase the wireless link Signal-to-Noise Ratio (SNR) between them, which in-turn helps increase the throughput and reliability of the wireless network extension.

- Use-Case 2: Multi-Hop Mesh deployment might be needed for temporary connectivity during a wired network failure with no direct line of sight (LoS) to a mesh Root Access Point (RAP).

  Due to no wireless LOS availability, sometimes a multi-hop mesh deployment is required to provide network connectivity to the affected area. A few RF considerations need to be factored in for this deployment:

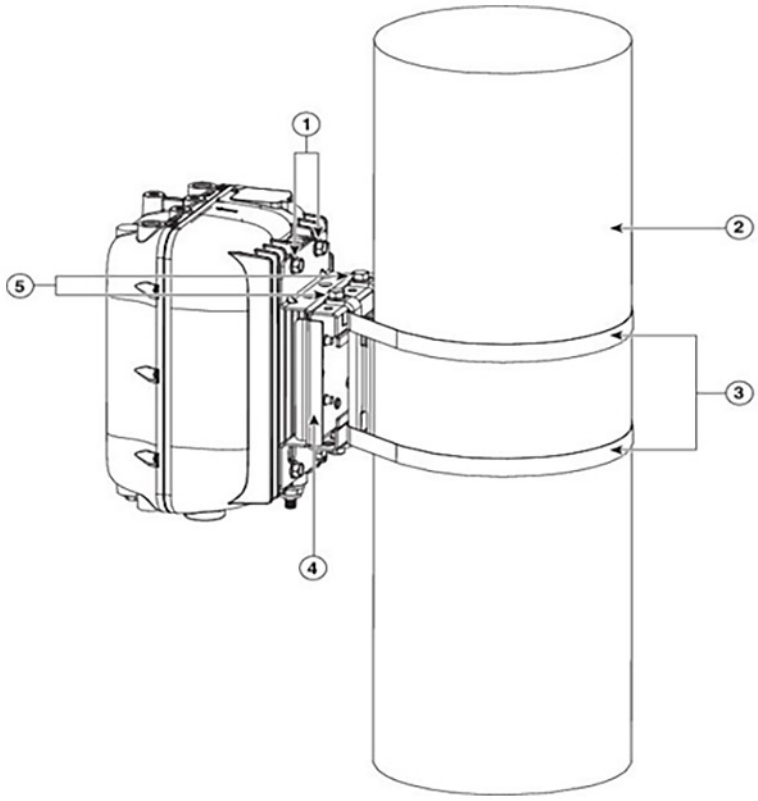
  - For every extra hop that is used the overall throughput of the system will be reduced.
  - Directional antennas cannot be used on the MAPs in the middle of the linear RF chain because the MAPs downstream will not be able to connect.
  - Placement of multiple units in the drifts could be an issue with equipment movement.

  Having limited network connectivity to allow for continued mining operations until the wired infrastructure can be repaired is better than having to stop all mining operations in the area affected.

Appendix B: Infrastructure AP Installation

The infrastructure APs used within the Cisco outdoor testing included the 1572 (1572EAC) along with the Cisco IW3702 with antenna models AIR-ANT2568VG-N and AIR-ANT2547 installed at a height of 15 feet. Installation included the use of pole mount kit 2 [AIR-ACCPMK1570-2=] for vertical installation on poles ranging in diameter of 2 to 16 inches. Mounting tools used can vary based on the deployment needs. See the following figure for reference.

Figure 66 Pole mounting option



In deployments such as mining where pole mounts may not be optimal the access point can be mounted on hard ceilings and walls using the built-in mounting flanges.

Using the Integrated Flange Mounts

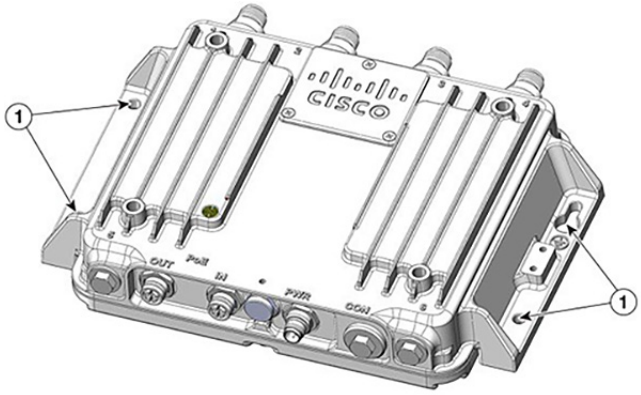
Direct mounting using the integrated flange mounts is typically for confined spaces or deployments that experience severe shock and vibration.

To mount the access point using the integrated flange mounts:

Step 1: Choose the access point location that can safely support the weight of the access point.

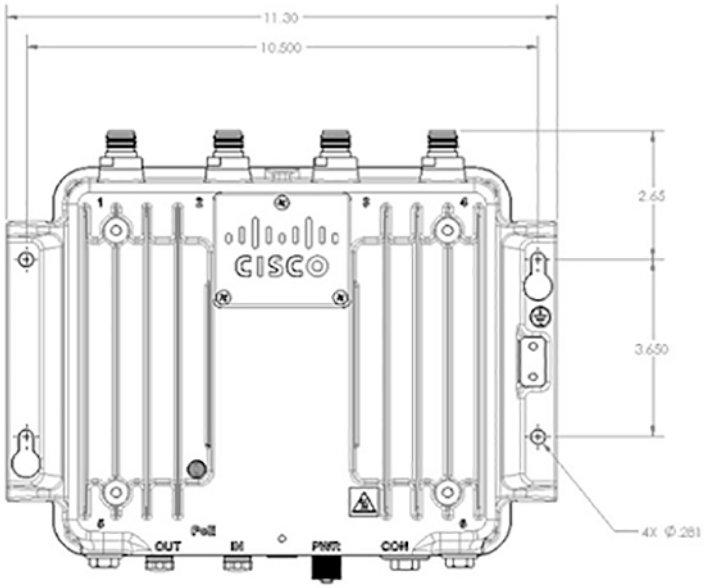
Step 2: Use the access point mounting holes as a template and mark them at the mounting location.

Figure 67 0.28 in (7.12 mm) mounting holes



Step 3: Drill holes on the mounting surface for plastic wall anchors to suit 1/4-20 or M6 bolts and add the appropriate anchors. The following figure shows the hole locations.

Figure 68 Mounting hole location



Step 4: Align the access point mounting holes with the suspended ceiling mounting holes.

Step 5: Insert a mounting screw in each of the four mounting holes and tighten.

Step 6: You can use the keyholes for “hands-free” installation.

Figure 69 Wall mounted IW3702 within the test Mine

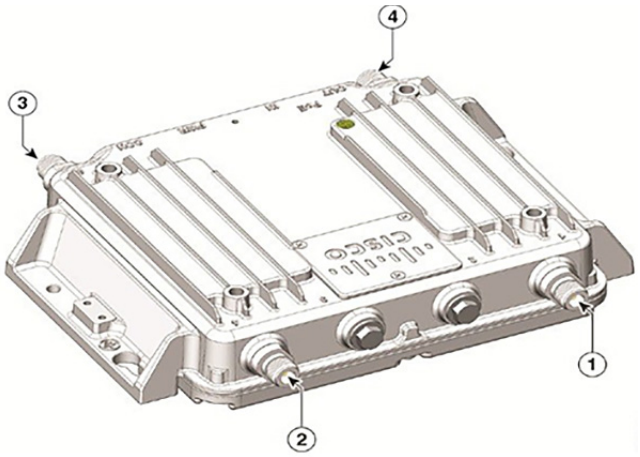
All versions of the 1570 and IW3702 series access points contain a 4x4:3 2.4 GHz radio and a 4x4:3 5 GHz radio, which are connected to physical antennas/antenna ports numbered 1, 2, 3, and 4.

These radios can be configured for both dual-band (both 2.4 GHz and 5 GHz signals coming from the same antenna ports) and single band (2.4 GHz and 5 GHz signals coming from different antennas / antenna ports). The 2.4 and 5 GHz radios connected to these antennas/antenna ports are user configurable as follows:

Table 7 Allowable configurations for the 2.4 GHz radio

Mode	Active Antennas / Ports			
	1	2	3	4
2x2 Single Band	Yes	Yes		
2x2 Dual Band	Yes	Yes		
3x3 Dual Band	Yes	Yes	Yes	
4x4 Dual Band	Yes	Yes	Yes	Yes

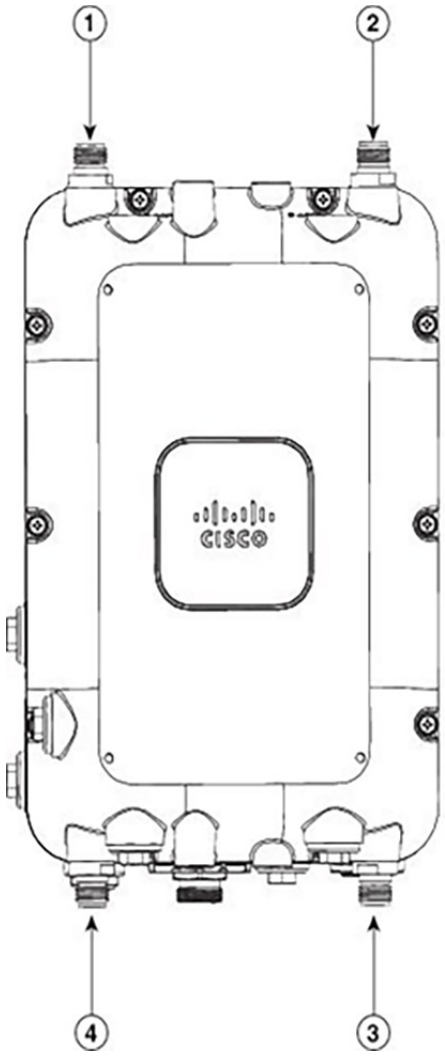
Figure 70 Top Panel View of Cisco IW3702-2E-x-K9



Antenna ports and references are shown below.

1	Antenna port C	3	Antenna port A
2	Antenna port D	4	Antenna port B

Figure 71 AIR-CAP1572EAC-X-K9



Due to the challenging RF environments within an underground mining environment we recommend deploying 4 x Dual Band Antennas on the APs to provide antenna diversity. With the 5GHz radio disabled all of the 4 x Dual Band Antennas will be used for the 2.4GHz radio.

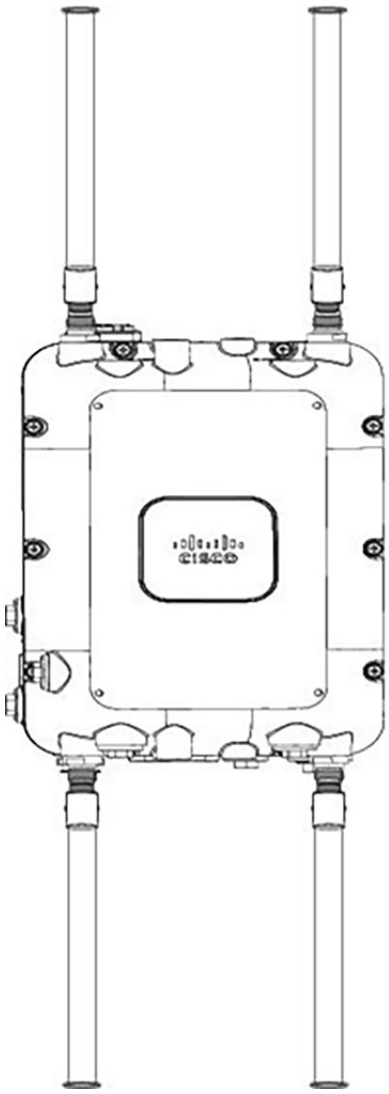
3702 N-Type Antenna Connectors

The IW3702 access points use N-type connectors. Depending on the model type the location of the connectors can be on the top or bottom of the AP. Please refer to the following IW3702 antenna install guide for further details: https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw3702/hardware/install/guide/b_iw3702_gsg.html#con_1155340

1572 N-Type Antenna Connectors

The AP1572E access point version has two N-type antenna connectors located on the base and two N-type antenna connectors on the head of the access point. The N-type connectors support variety of the Cisco Aironet antennas. For detailed information about installation of these antennas, refer to https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1570/installation/guide/1570hig/1570_chinstallaccs.html#79962.

Figure 72 AIR-CAP1572EAC-X-K9 with AIR-ANT2568VG-N



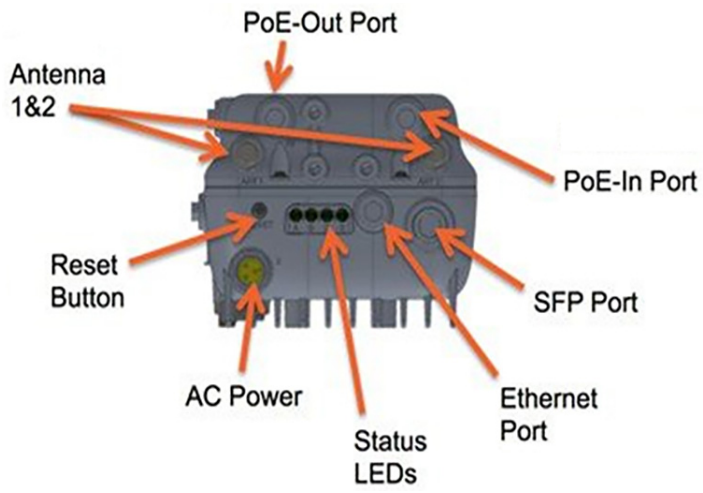
PoE-Input

AC powered versions of AP1572EAC can be powered by UPOE compliant power sourcing equipment.

In addition to being powered by UPOE sources, the access point can also be powered by the AIR-PWRINJ1500-2 power injector.

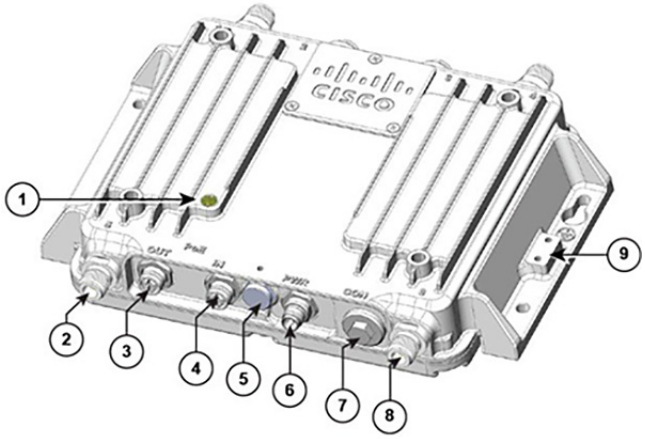
The access point also supports an Ethernet uplink port (PoE-In). The access point Ethernet uplink port uses an RJ-45 connector (with weatherproofing) to link the access point to the 10BASE-T, 100BASE-T or 1000BASE-T network. The Ethernet cable is used to send and receive Ethernet data and to optionally supply inline power from the power injector or a suitably powered switch port.

Figure 73 Cisco 1572 Port Layout



The IW3702-2E-x-K9 has four antenna connectors, 2 on the top and 2 on the bottom.

Figure 74 Cisco IW3702-2E-x-K9 Port Layout

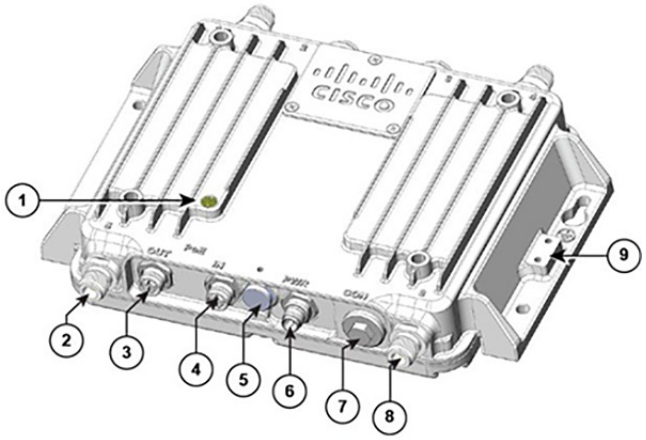


The Cisco IW3702-2E-x-K9 Port reference and descriptions are shown below.

1	Status LED	6	Power(PWR) connector
2	Antenna port B	7	Console (Con) port
3	PoE OUT port	8	Antenna port A
4	PoE in port	9	Ground Connection
5	Protective vent/Reset button (covered)		

There are four antenna ports on the Cisco IW3702-4E-x-K9 model, all four connectors are on the top side.

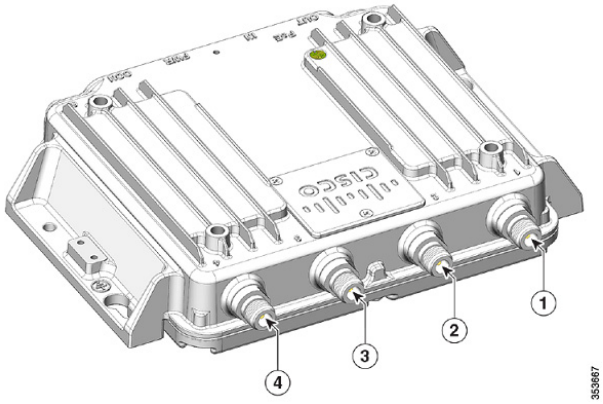
Figure 75 Cisco IW3702-4E-x-K9 Bottom Panel View



The Cisco IW3702-4E-x-K9 Bottom Panel references are shown below.

1	Status LED	5	Power (PWR) connector
2	PoE OUT port	6	Console (CON) port
3	PoE IN port	7	Ground connection
4	Protective vent port / Reset button (covered)		

Figure 76 Cisco IW3702-4E-x-K9 Top Panel View



The Cisco IW3702-4E-x-K9 Top Panel antenna ports are referenced below.

1	Antenna port C	3	Antenna port B
2	Antenna port A	4	Antenna port D

The figure below depicts the Cisco IW3702-2E-x-K9 infrastructure AP mounted on one of the walls of a mine tunnel, with 4 x AIR-ANT-2547 antennas attached to it.

Figure 77 AIR-ANT-2547

The figure below depicts a Cisco IE 4000 switch along with its power supply located within a purpose built ruggedized enclosure mounted on one of the walls of a mine tunnel.

Figure 78 Pre- Fabricated Mine Enclosure for Cisco IE switch and components

Appendix C: FTP Integrated Monitoring System

The Integrated Monitoring System (FTP IMS) is the first Wi-Fi Mesh or any 802.15.4 variant network monitoring application to bridge the gap between operational technology and information technology world. IMS has a unique database design that allows for the business to report and visualize all parts of the operation in near real time. With IMS you have the choice to overlay or replace existing systems and reporting methods, either way IMS removes the siloed point solutions that have helped to create the separation between IT and OT. IMS is a disruptive technology application, however, due to the overlay deployment capability each business unit can control end user visibility to help minimize impact. IMS is suited to both greenfield and brownfield sites, small or large, local or remote. Our application has the ability to visualize all of your data no matter how complex, from real-time location data to business intelligence and financial modeling.

IMS has the ability to extract new and existing information from all systems, giving you the flexibility to create your own customized reports with the click of a button.

The IMS tool can be used to identify and root cause wireless network events before they become incidents.

Advantages of IMS:

- Improve network wide situational awareness.
- Easy to understand representations of complex problems to aid in decision making and reduce MTTR.
- Optimize operational performance through up to the second issue tracking.
- Increase knowledge and understanding of production networks through simple historical interrogation of networking data.
- Benchmark performance and monitor SLAs, hold vendors accountable for system availability.
- Reduce operational downtime, increase profitability.
- Efficiently direct onsite resources to the root cause of issues.

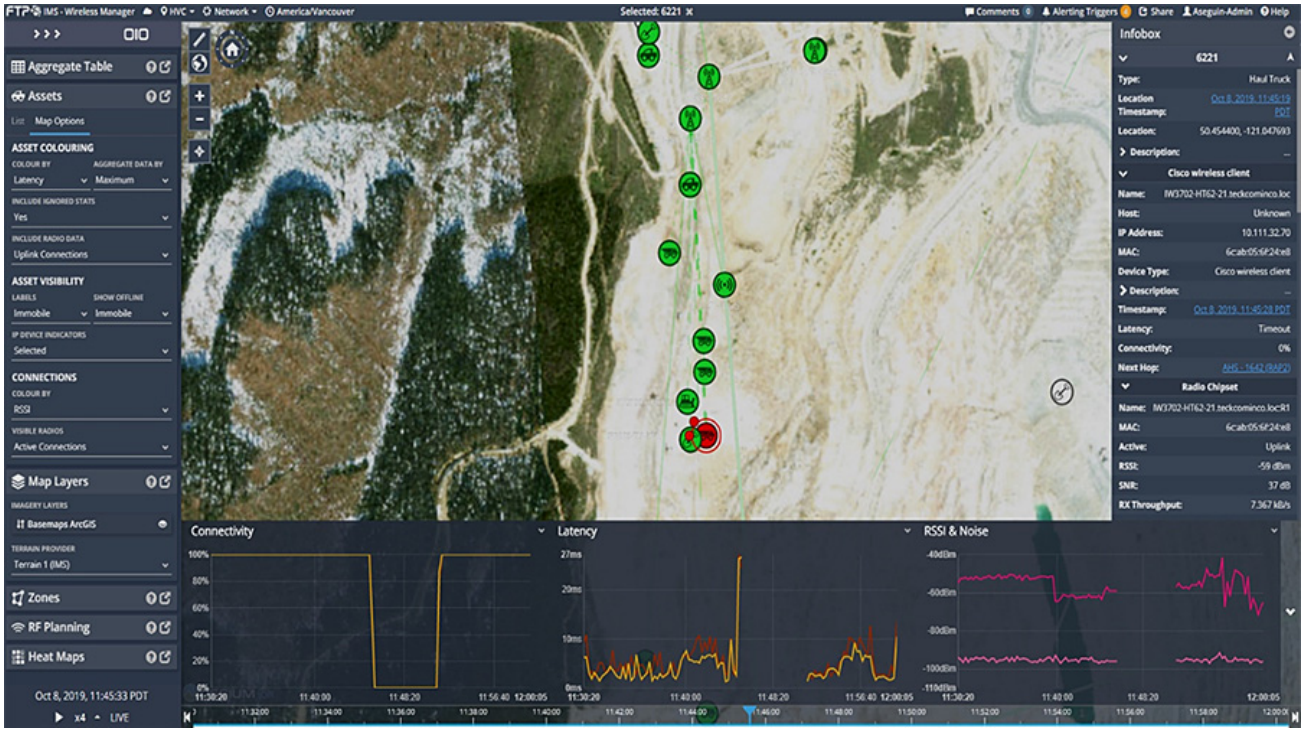
The FTP IMS tool has the real time Wi-Fi Mesh Network visualization capability for the following functionality.

- Wireless Network Infrastructure
- Wired Network Infrastructure
- In-pit Infrastructure
- Personnel Movements
- IoT Infrastructure
- Incident Investigation and Management

Sample Snapshots and illustration from a real-world Cisco Wi-Fi Mesh deployment.

- The green colored legend below depicts the vehicles which are roaming without losing Wi-Fi Network connectivity.
- Red color legend below shows the vehicles for which WIFI Network connectivity is lost.

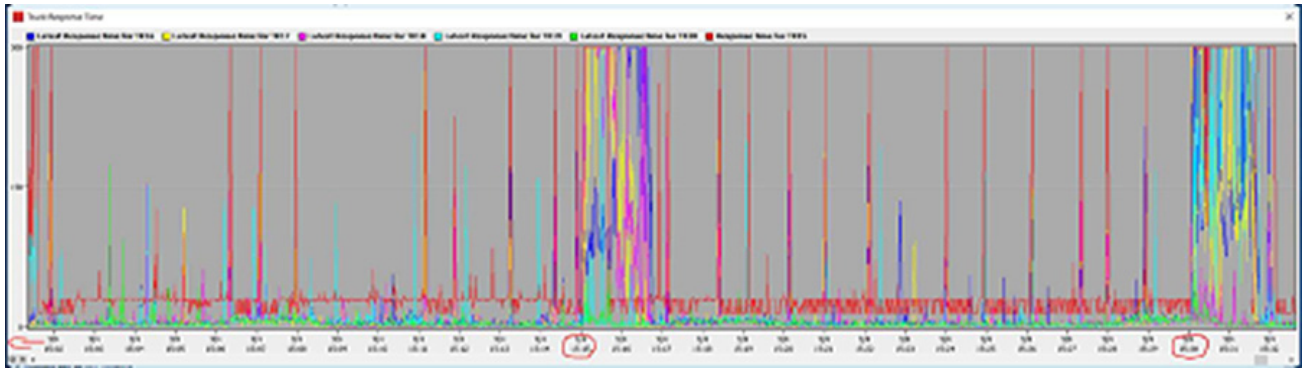
Figure 79 FTP IMS Wireless Manager Network View



Here is an event at 1530 on Sept 5 that triggered a disconnect on TK15. This pattern 15 minute latency spikes can be seen consistently for months.

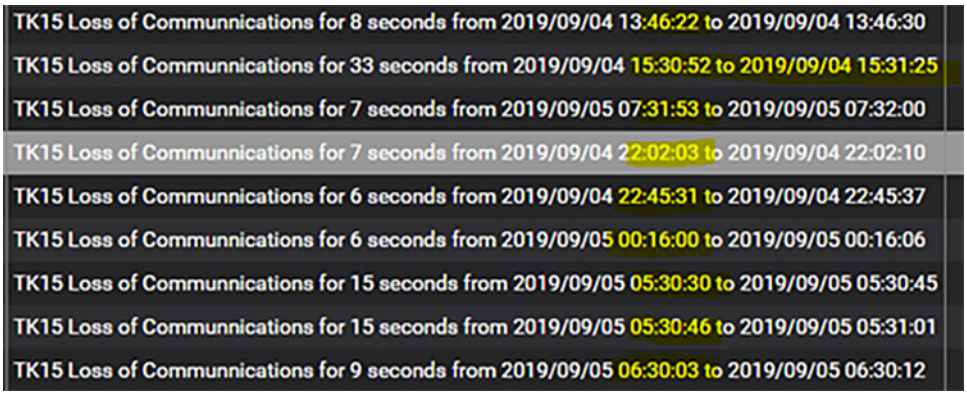
Note that TK15 overall worse performance has been likely attributed to it missing the beam-forming disabling configuration.

Figure 80 FTP IMS Truck Response Time Chart depicting an issue



Below is a record showing a pattern of disconnects occurring as the trucks were doing or shortly after they completed a log dump.

Figure 81 FTP IMS Event Log

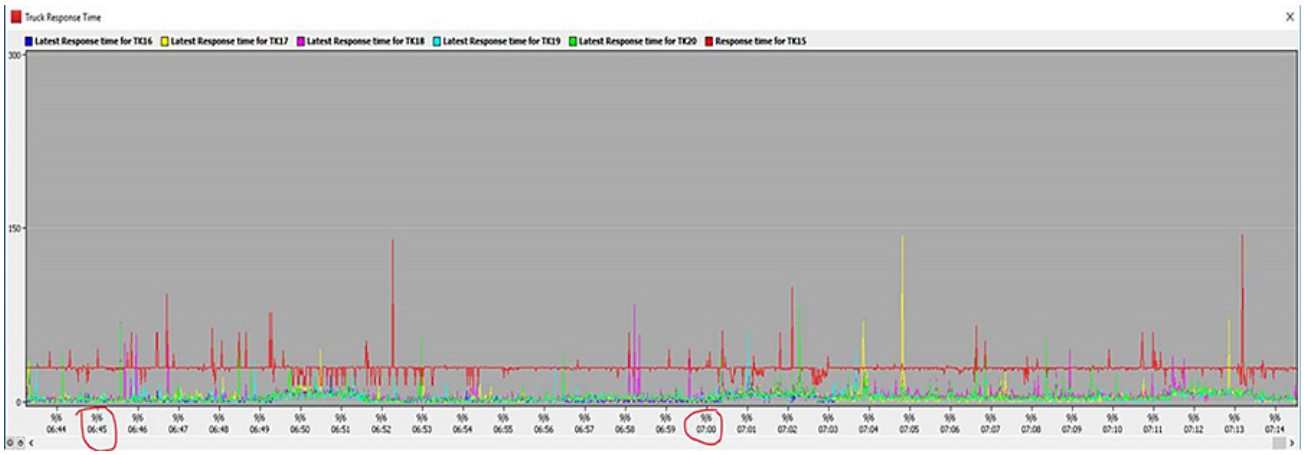


As can be seen since disabling the OTA log dumps, there has been a noticeable improvement on all of the reporting tools.

The 15-minute interval latency spikes seem to have disappeared.

Note that TK15 overall worse performance has been likely attributed to it missing the beamforming disabling configuration.

Figure 82 FTP IMS Truck Response Time Chart after issue resolved



There have been no loss of communication or broadcast since the OTA dumps have been disabled.

In analyzing IMS data, the TK20 suddenly loses RF signal due to a passing truck but takes five minutes to reconnect after the truck has passed and good RF signal is achieved.

Figure 83 FTP IMS Wireless Manager depicting an issue

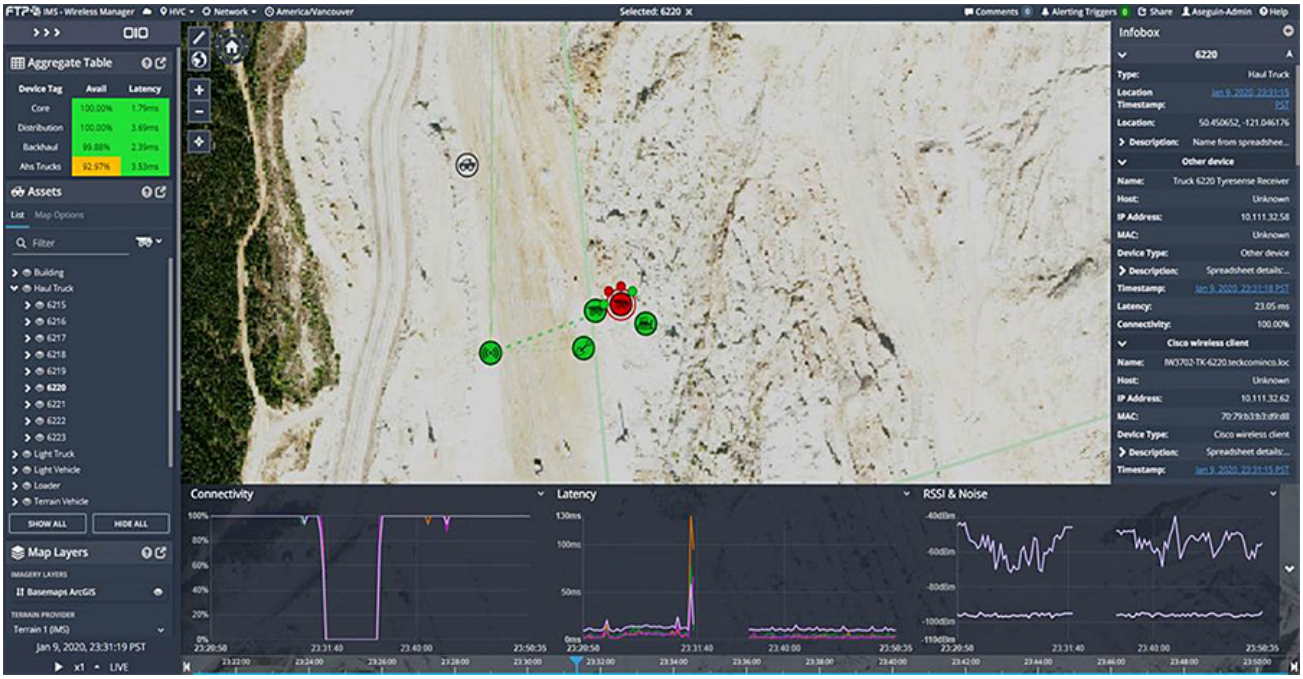
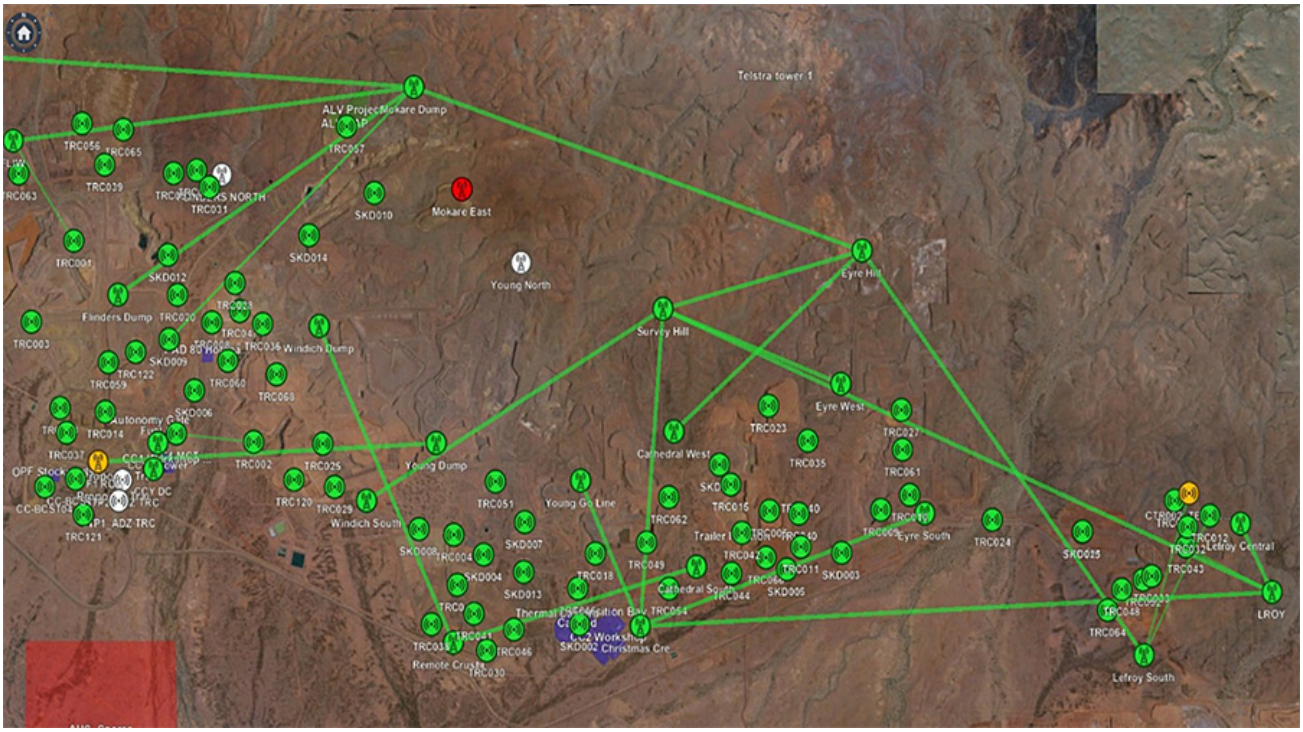
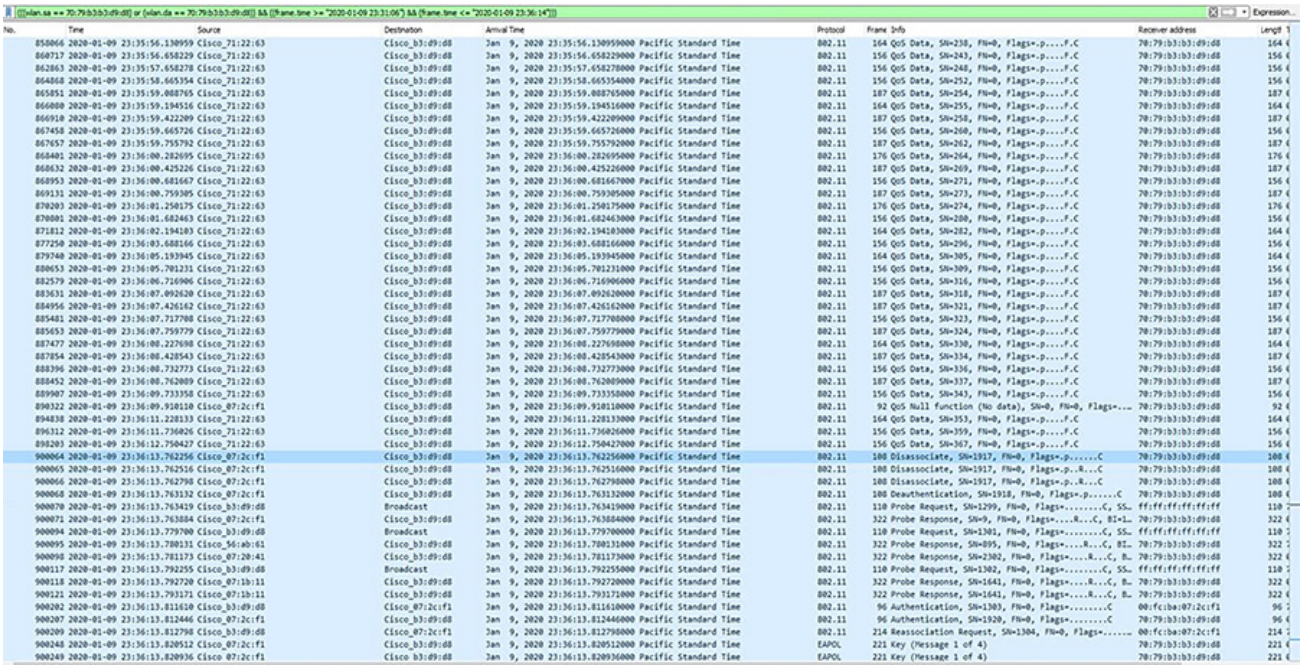


Figure 84 FTP IMS expanded terrain view



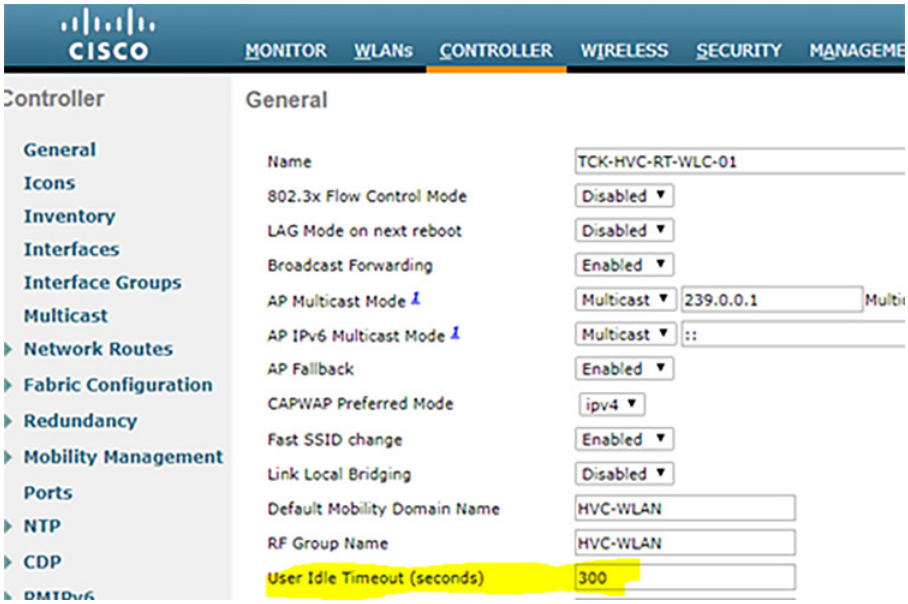
PCAP analysis reveals that the truck does not transmit any frames until a **Disassociate** frame is sent by the MAP.

Figure 85 PCAP analysis using Wireshark



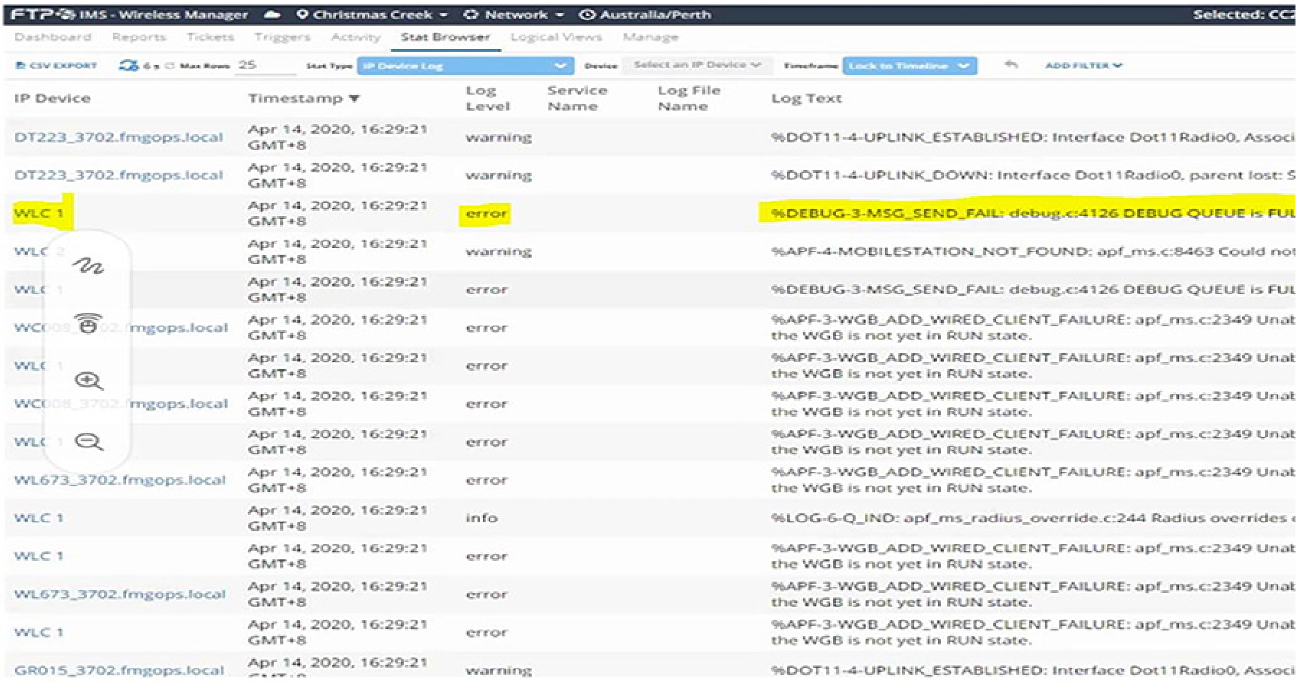
The time stuck, so check if the WLC is set to delete idle clients after 5 minutes.

Figure 86 WLC User Idle Timeout setting



The FTP IMS Logs Browser depicts an error captured via SNMP messages coming in from WLC.

Figure 87 FTP IMS Logs Browser depicts an error captured via SNMP messages coming in from WLC



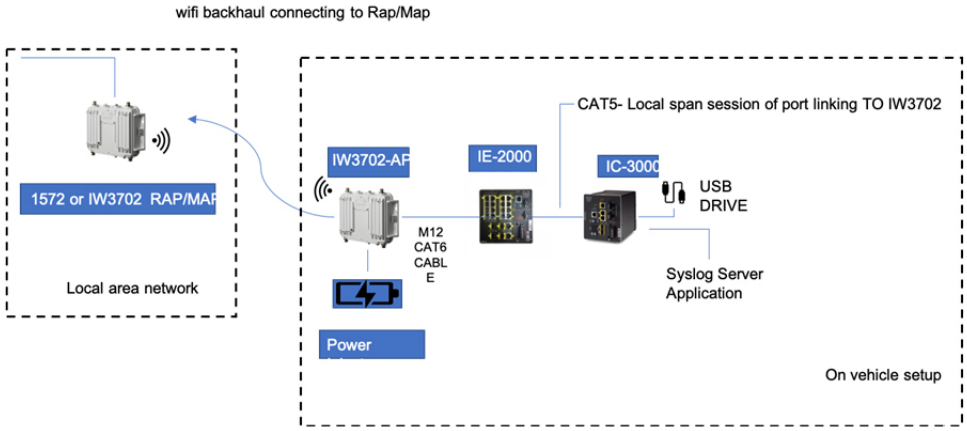
IP Device	Timestamp ▼	Log Level	Service Name	Log File Name	Log Text
DT223_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	warning			%DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associ
DT223_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	warning			%DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: S
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%DEBUG-3-MSG_SEND_FAIL: debug.c:4126 DEBUG QUEUE is FUL
WLC 2	Apr 14, 2020, 16:29:21 GMT+8	warning			%APF-4-MOBILESTATION_NOT_FOUND: apf_ms.c:8463 Could not
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%DEBUG-3-MSG_SEND_FAIL: debug.c:4126 DEBUG QUEUE is FUL
WC008_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WC008_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WL673_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	info			%LOG-6-Q_IND: apf_ms_radius_override.c:244 Radius overrides
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WL673_3702.fmgops.local	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
WLC 1	Apr 14, 2020, 16:29:21 GMT+8	error			%APF-3-WGB_ADD_WIRED_CLIENT_FAILURE: apf_ms.c:2349 Unat the WGB is not yet in RUN state.
GR015_3702.fmgops.local	Apr 14, 2020, 16:29:21	warning			%DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0, Associ

Appendix D: Using Cisco IC-3000 Ruggedized Compute as a Syslog Server to collect WGB Logs

This setup can be used for the pre-deployment process while performing the initial wireless install, for fine-tuning the RF characteristics, tuning the roam-times by using a Cisco IC-3K ruggedized compute to collect and analyze WGB logs.

The following steps detail the workflow for syslog collection and packaged application deployment using the IC-3000 behind the work group bridge. The reference in Figure 1 details the wireless backhauls through a RAP/MAP within a mesh scenario, however this should still apply within a CUWN with local mode APs.

Figure 88 Reference topology with IC-3000 behind WGB



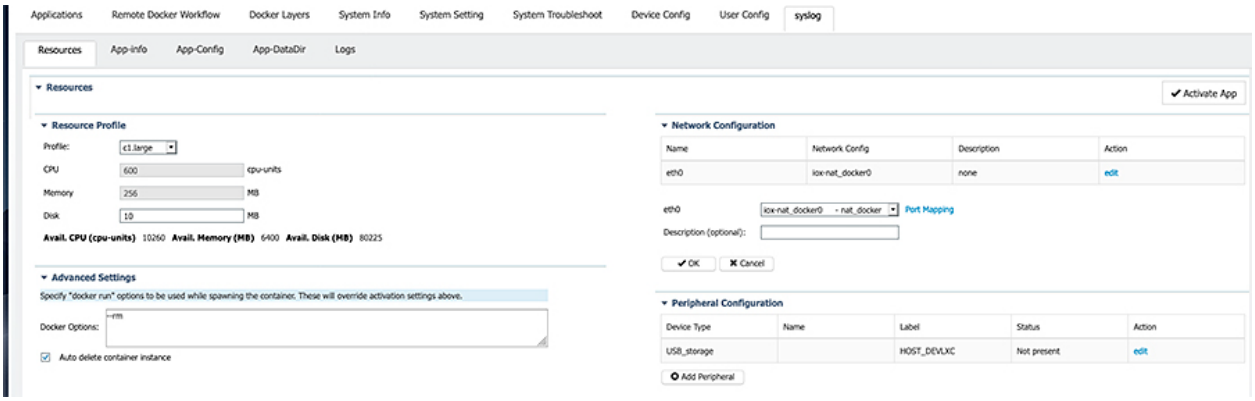
Note: Link Local Interface (LLI) can be used to manage IC-3K in Standalone/developer Mode for making changes. IP Subnet https://169.254.128.2:8443/ and by default the Local Manager (LM) UI is mapped to an IP address of 169.254.128.2

- Ensure the Laptop Wired NIC is assigned with an IP in the same subnet 169.254.128.x and then ping the LM IP Address IOX_CAF LM UI Credentials: developer/cisco123#
- Ensure that the USB is connected to IC-3K on port 1 of the USB Slot.

Deploying the Packaged Application in other IC-3000s

1. For detailed steps on how to access the Local Manager UI with Link Local Interface (LLI) access refer to Cisco IC3000 Industrial Compute Gateway Deployment Guide.
2. Add the application by typing the + key, and then map the proper Network interface. The application can be downloaded at the following link: https://ciscoshare.cisco.com/alfext/ext/download/workspace/SpacesStore/0c7c49ee-479b-4772-9fde-2b712f312f1b/Syslog_Package.tar?a=true

Figure 89 Cisco IOx Local Manger

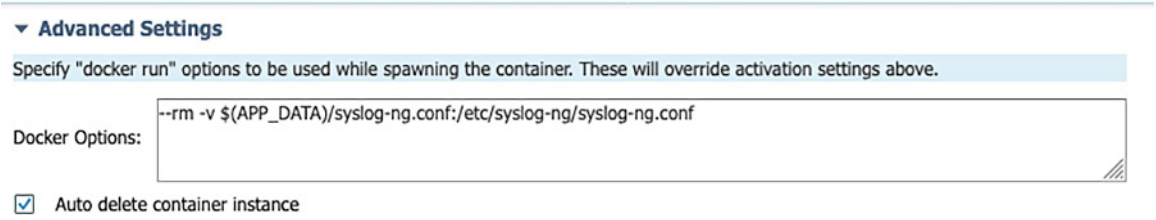


3. In Application, under Resources > Advanced Settings add this line:

```
--rm -v $(APP_DATA)/syslog-ng.conf:/etc/syslog-ng/syslog-ng.conf
```

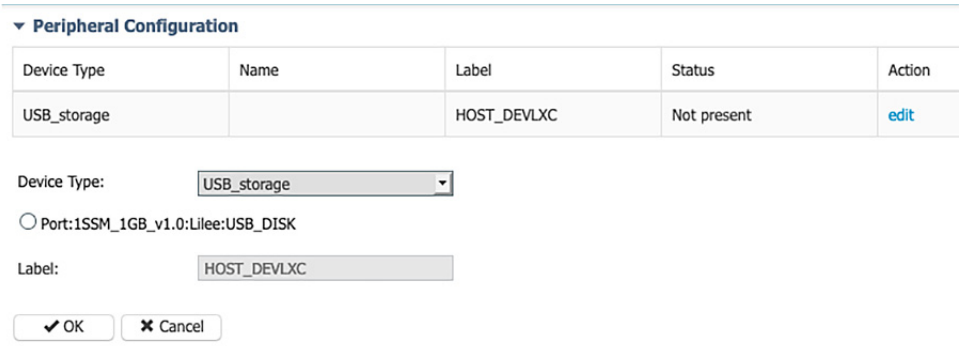
in the Tab as shown in the figure below, save it, and then import the file (syslog-ng.conf).

Figure 90 Advanced Settings



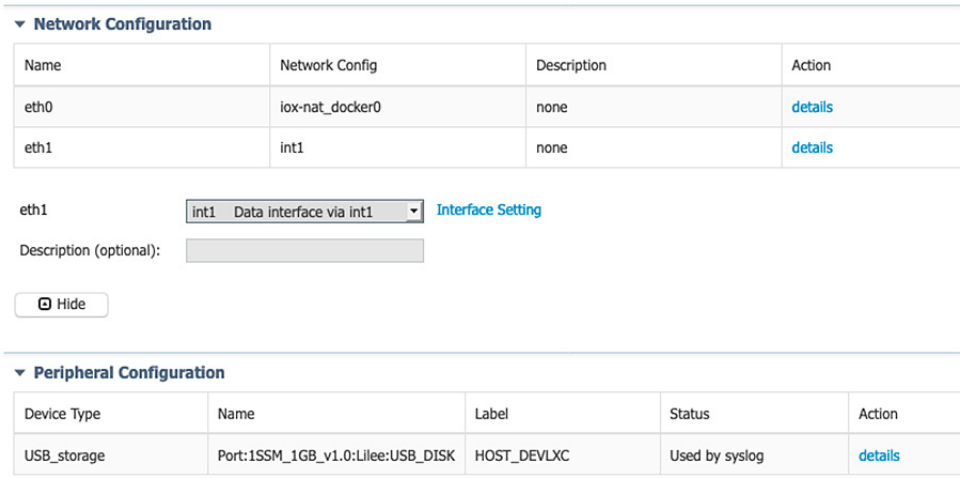
4. Under Peripheral, click on edit and select radio button to add the USB to the Application and then hit OK.

Figure 91 Peripheral Configuration



5. On Specific Application, under Resources > Network Configurations, add another ethernet port and map that to the interface that is connected to IE2K and click Interface Setting.

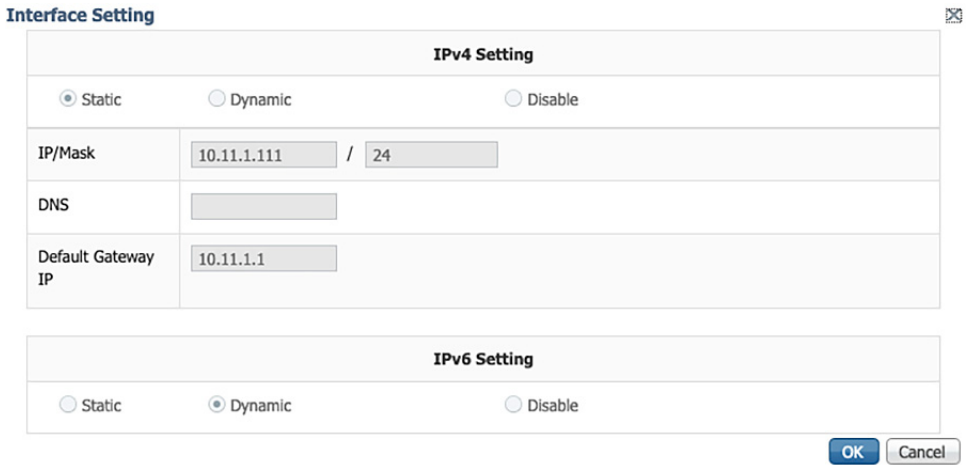
Figure 92 Adding Interface in Application



6. Assign a static IP address to the interface under IPV4 setting and leave IPV6 as default and hit OK and then Activate the Application.

   Note: The static IP address should be in the same subnet of IE2K and the BVI interface of the WGB.

Figure 93 Assigning Static IP address

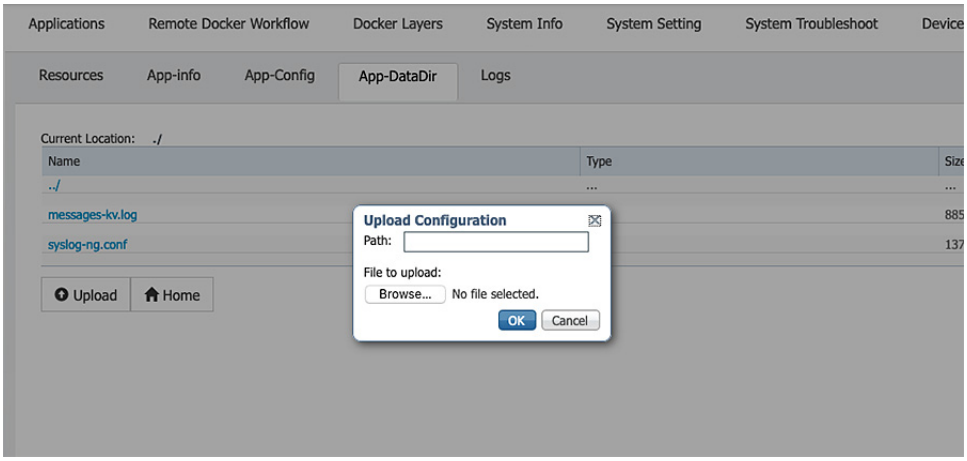


7. After Activating the Application, go to App-DataDir in Application and hit Upload button to upload the syslog-ng.conf. syslog-ng.conf file can be downloaded from the following link:

   https://ciscoshare.cisco.com/alfext/ext/download/workspace/SpacesStore/9782f254-9fb4-4520-b406-591b5951a56a/syslog-ng.conf?a=true

   Note: You will need to provide your Cisco CCO credentials to access the file.

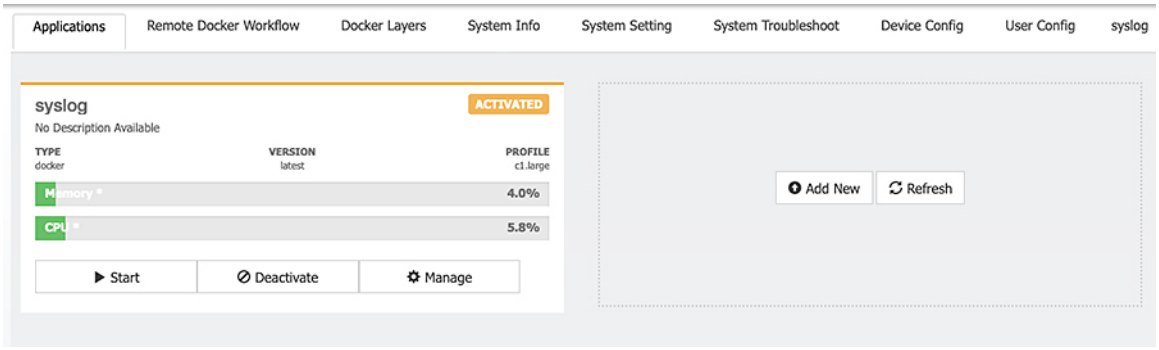
Figure 94 Upload the file



Note: It is mandatory to upload the .conf file corresponding to that application.

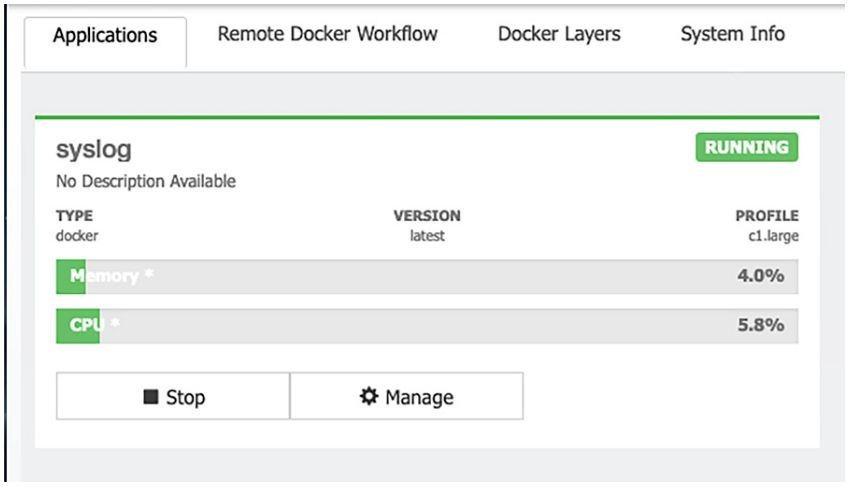
8. For Path type syslog-ng.conf. After uploading, go to Applications tab and hit start on the specific application.

Figure 95 Activated Application



9. Check to see if the state turns Green (running status for the application).

Figure 96 Running Application



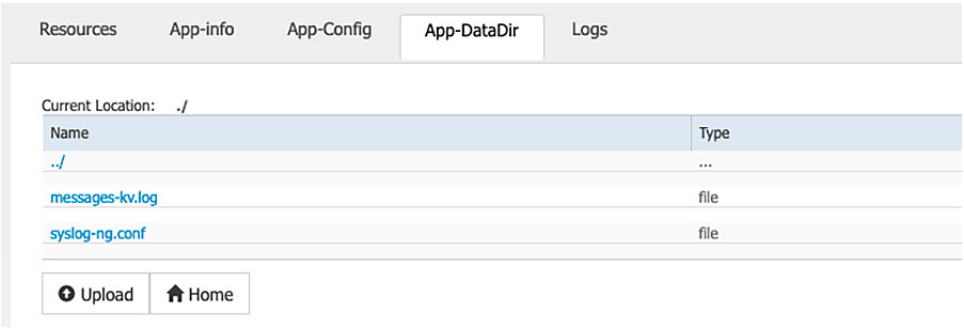
10. For the logs to show up on the syslog server running on the IC-3K, on WGB configure logging redirect to the IP address that was configured previously in **step 6.**

    Configuration on WGB to direct syslog messages to syslog server running on the IC-3K:

```
WGB(config)#logging host 10.11.1.111
WGB(config)#logging trap debugging
```

11. Navigate to the App-DataDir tab on the Application to see messages-kv.log being populated with the logs from the WGB.

Figure 97 Log Collection



12. A copy of the logs is also stored on the USB Drive attached to the IC-3K for later offline analysis.